

Oracle® Key Vault

Developer's Guide



Release 21.8

F88240-02

April 2024



Oracle Key Vault Developer's Guide, Release 21.8

F88240-02

Copyright © 2014, 2024, Oracle and/or its affiliates.

Primary Author: Monika Sharma

Contributors: Mark Doran, Rahil Mir, Min-Hank Ho, Swapna Jawarikapisha, Shirley Kumamoto, Michael Leong, Sunil Pulla, Sindhu Ravichandran, Saikat Saha, Vipin Samar, Dongwon park, Swati Doddabalapur Vijaya Bhaskar, Alex Abell

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	xiv
Documentation Accessibility	xiv
Diversity and Inclusion	xiv
Related Documents	xv
Conventions	xv

Part I Introduction to the Oracle Key Vault Client SDK

1 Changes in This Release

1.1 Changes for Oracle Key Vault Client SDK Release 21.6	1-1
1.1.1 Support for Sign and Signature Verify Operations	1-1
1.1.2 Ability to Control the Extraction of Private Keys from Oracle Key Vault	1-2
1.2 Changes for Oracle Key Vault Client SDK Release 21.5	1-3
1.3 Changes for Oracle Key Vault Client SDK Release 21.4	1-3
1.3.1 C and Java SDK APIs for Cryptographic Operations	1-3
1.3.2 Client Endpoint File Updated When A KMIP Server Operation Is Executed Using SDK	1-5
1.3.3 Ability to Control the Extraction of Symmetric Encryption Keys from Oracle Key Vault	1-5
1.4 Changes for Oracle Key Vault Client SDK Release 21.3	1-6
1.5 Changes for Oracle Key Vault Client SDK Release 21.2	1-6
1.5.1 New C and Java SDK APIs for Certificates, Certificate Requests, Private Keys, and Public Keys	1-6

2 Getting Started with the Oracle Key Vault Client SDK

2.1 About Getting Started with the Oracle Key Vault Client SDK	2-1
2.2 Who Should Use This Guide	2-2
2.3 Platforms Supported	2-2
2.4 Advantages of Using the Oracle Key Vault Client SDK	2-2

3 KMIP Features of the Oracle Key Vault Client SDK

3.1	KMIP Version	3-1
3.2	KMIP Profile Support	3-1
3.3	KMIP Managed Objects	3-1
3.4	KMIP Operations	3-2

4 Setting Up the Oracle Key Vault SDK

4.1	Enrolling an Endpoint	4-1
4.2	Downloading the C or Java SDK Software	4-1
4.3	Contents of the C SDK File	4-5
4.4	Contents of the Java SDK File	4-7

5 Oracle Key Vault Client SDK Program Structure

5.1	About the Oracle Key Vault Client SDK Program Structure	5-1
5.2	Oracle Key Vault Program Flow	5-1
5.2.1	Basic Program Flow	5-2
5.2.2	Advanced Program Flow	5-4
5.2.2.1	Oracle Key Vault Program with Batching	5-4
5.2.2.2	Detailed Oracle Key Vault Program	5-6
5.3	Oracle Key Vault Program Environment	5-8
5.4	Oracle Key Vault Program Connection	5-9
5.5	Oracle Key Vault Program Session	5-9

Part II Oracle Key Vault Client C SDK API Reference

6 Oracle Key Vault Datatypes and Structures

6.1	Oracle Key Vault Datatypes	6-1
6.2	Oracle Key Vault Structures and Enumerations	6-1
6.2.1	OKVAttr	6-2
6.2.2	OKVAttrNo	6-5
6.2.3	OKVCryptoContext	6-6
6.2.4	OKVDecryptResponse	6-7
6.2.5	OKVEncryptResponse	6-7
6.2.6	OKVEnv	6-8
6.2.7	OKVErr	6-9
6.2.8	OKVMemoryCtx	6-10
6.2.9	OKVObjNo	6-11

6.2.10	OKVOps	6-11
6.2.11	OKVopsNo	6-12
6.2.12	OKVServerInformation	6-13
6.2.13	OKVTTLV	6-13
6.2.14	OKVSignResponse	6-14
6.2.15	OKVSignVerifyResponse	6-14

7 Oracle Key Vault Client SDK Management APIs

7.1	okvEnvCreate	7-1
7.2	okvEnvFree	7-3
7.3	okvEnvFreeResultObj	7-4
7.4	okvEnvGetOpRequestObj	7-5
7.5	okvEnvSetConfig	7-7
7.6	okvEnvSetTrace	7-8

8 Oracle Key Vault Client SDK Connection Management APIs

8.1	okvConnect	8-1
8.2	okvConnSendRecvBytes	8-3
8.3	okvConnSet	8-4
8.4	okvConnUnSet	8-6
8.5	okvDisconnect	8-7

9 Oracle Key Vault Client SDK Memory Management APIs

9.1	okvFree	9-1
9.2	okvMalloc	9-2
9.3	okvRealloc	9-3

10 Oracle Key Vault Client SDK Error Handling APIs

10.1	okvErrGetDepth	10-1
10.2	okvErrGetDepthForBatch	10-3
10.3	okvErrGetNum	10-4
10.4	okvErrGetNumAtDepth	10-6
10.5	okvErrGetNumAtDepthForBatch	10-7
10.6	okvErrGetNumForBatch	10-9
10.7	okvErrReset	10-11
10.8	okvGetTextForErrNum	10-12

11 Oracle Key Vault Client SDK KMIP and Batch APIs

11.1	Oracle Key Vault Client SDK KMIP APIs	11-1
11.1.1	About the Oracle Key Vault Client SDK KMIP APIs	11-3
11.1.2	okvActivate	11-3
11.1.3	okvAddAttribute	11-5
11.1.4	okvCreateKey	11-8
11.1.5	okvDecrypt	11-10
11.1.6	okvDeleteAttribute	11-14
11.1.7	okvDestroy	11-16
11.1.8	okvEncrypt	11-18
11.1.9	okvGetAttributeList	11-21
11.1.10	okvGetAttributes	11-24
11.1.11	okvGetCertificate	11-26
11.1.12	okvGetCertificateRequest	11-29
11.1.13	okvGetKey	11-32
11.1.14	okvGetOpaqueData	11-34
11.1.15	okvGetPrivateKey	11-37
11.1.16	okvGetPublicKey	11-40
11.1.17	okvGetSecretData	11-43
11.1.18	okvGetTemplate	11-45
11.1.19	okvLocate	11-47
11.1.20	okvModifyAttribute	11-50
11.1.21	okvQueryCapability	11-52
11.1.22	okvRegCertificate	11-55
11.1.23	okvRegCertificateRequest	11-59
11.1.24	okvRegOpaqueData	11-63
11.1.25	okvRegKey	11-65
11.1.26	okvRegPrivateKey	11-69
11.1.27	okvRegPublicKey	11-72
11.1.28	okvRegSecretData	11-76
11.1.29	okvRegTemplate	11-79
11.1.30	okvRekey	11-81
11.1.31	okvRevoke	11-84
11.1.32	okvSign	11-86
11.1.33	okvSignVerify	11-89
11.1.34	okvCreateKeyPair	11-92
11.2	Oracle Key Vault Client SDK Batch APIs	11-95
11.2.1	okvBatchCreate	11-96
11.2.2	okvBatchExecute	11-97
11.2.3	okvBatchFree	11-98

11.2.4	okvGetBatchOperationCount	11-100
11.2.5	okvGetBatchOperationName	11-101

12 Oracle Key Vault Client SDK KMIP Attributes and Custom Attributes APIs

12.1	Oracle Key Vault Client SDK KMIP Attribute APIs	12-1
12.1.1	About the Oracle Key Vault KMIP Attribute APIs	12-6
12.1.2	Attribute Index and Element Index	12-7
12.1.3	okvAttrAddArchiveDate	12-8
12.1.4	okvAddAttributeObject	12-9
12.1.5	okvAttrAddActivationDate	12-10
12.1.6	okvAttrAddCertLen	12-11
12.1.7	okvAttrAddCertType	12-13
12.1.8	okvAttrAddCompromiseDate	12-14
12.1.9	okvAttrAddCompromiseOccurrenceDate	12-15
12.1.10	okvAttrAddContactInfo	12-16
12.1.11	okvAttrAddCryptoAlgo	12-17
12.1.12	okvAttrAddCryptoLen	12-18
12.1.13	okvAttrAddCryptoParams	12-19
12.1.14	okvAttrAddCryptoUsageMask	12-20
12.1.15	okvAttrAddDeactivationDate	12-21
12.1.16	okvAttrAddDestroyDate	12-22
12.1.17	okvAttrAddDigest	12-23
12.1.18	okvAttrAddDigitalSignAlgo	12-24
12.1.19	okvAttrAddExtractable	12-25
12.1.20	okvAttrAddFresh	12-26
12.1.21	okvAttrAddInitialDate	12-27
12.1.22	okvAttrAddLastChangeDate	12-28
12.1.23	okvAttrAddLeaseTime	12-29
12.1.24	okvAttrAddName	12-30
12.1.25	okvAttrAddNeverExtractable	12-32
12.1.26	okvAttrAddObjectGroup	12-33
12.1.27	okvAttrAddObjectType	12-34
12.1.28	okvAttrAddProcessStartDate	12-35
12.1.29	okvAttrAddProtectStopDate	12-36
12.1.30	okvAttrAddRevocationReason	12-37
12.1.31	okvAttrAddState	12-38
12.1.32	okvAttrAddUniqueID	12-39
12.1.33	okvAttrAddUsageLimits	12-40
12.1.34	okvAttrAddX509CertId	12-41

12.1.35	okvAttrAddX509CertIss	12-42
12.1.36	okvAttrAddX509CertIssAltName	12-44
12.1.37	okvAttrAddX509CertSubj	12-45
12.1.38	okvAttrAddX509CertSubjAltName	12-47
12.1.39	okvAttrGetActivationDate	12-48
12.1.40	okvAttrGetArchiveDate	12-49
12.1.41	okvAttrGetCertLen	12-50
12.1.42	okvAttrGetCertType	12-51
12.1.43	okvAttrGetCompromiseDate	12-52
12.1.44	okvAttrGetCompromiseOccurrenceDate	12-53
12.1.45	okvAttrGetContactInfo	12-54
12.1.46	okvAttrGetContactInfoLen	12-55
12.1.47	okvAttrGetCryptoAlgo	12-56
12.1.48	okvAttrGetCryptoLen	12-58
12.1.49	okvAttrGetCryptoParams	12-59
12.1.50	okvAttrGetCryptoUsageMask	12-60
12.1.51	okvAttrGetDeactivationDate	12-61
12.1.52	okvAttrGetDestroyDate	12-62
12.1.53	okvAttrGetDigest	12-63
12.1.54	okvAttrGetDigestLen	12-64
12.1.55	okvAttrGetDigitalSignAlgo	12-65
12.1.56	okvAttrGetExtractable	12-66
12.1.57	okvAttrGetFresh	12-67
12.1.58	okvAttrGetInitialDate	12-68
12.1.59	okvAttrGetLastChangeDate	12-69
12.1.60	okvAttrGetLeaseTime	12-70
12.1.61	okvAttrGetName	12-71
12.1.62	okvAttrGetNameValueLen	12-72
12.1.63	okvAttrGetNeverExtractable	12-73
12.1.64	okvAttrGetObjectGroup	12-74
12.1.65	okvAttrGetObjectGroupLen	12-76
12.1.66	okvAttrGetObjectType	12-77
12.1.67	okvAttrGetProcessStartDate	12-78
12.1.68	okvAttrGetProtectStopDate	12-79
12.1.69	okvAttrGetRevocationReason	12-80
12.1.70	okvAttrGetRevocationReasonMessageLen	12-81
12.1.71	okvAttrGetState	12-82
12.1.72	okvAttrGetUniqueID	12-83
12.1.73	okvAttrGetUniqueIDLen	12-84
12.1.74	okvAttrGetUsageLimits	12-85
12.1.75	okvAttrGetX509CertId	12-86

12.1.76	okvAttrGetX509CertIdIssuerLen	12-87
12.1.77	okvAttrGetX509CertIdSerialNoLen	12-88
12.1.78	okvAttrGetX509CertIss	12-90
12.1.79	okvAttrGetX509CertIssAltName	12-91
12.1.80	okvAttrGetX509CertIssAltNameLen	12-93
12.1.81	okvAttrGetX509CertIssDNLen	12-94
12.1.82	okvAttrGetX509CertSubj	12-95
12.1.83	okvAttrGetX509CertSubjAltName	12-97
12.1.84	okvAttrGetX509CertSubjAltNameLen	12-98
12.1.85	okvAttrGetX509CertSubjDNLen	12-100
12.1.86	okvGetAttributeObject	12-101
12.2	Oracle Key Vault Client SDK KMIP Custom Attribute APIs	12-102
12.2.1	About the KMIP Custom Attributes API	12-104
12.2.2	okvCustomAttrAddBigInteger	12-105
12.2.3	okvCustomAttrAddBoolean	12-107
12.2.4	okvCustomAttrAddByteString	12-108
12.2.5	okvCustomAttrAddDateTime	12-109
12.2.6	okvCustomAttrAddEnum	12-111
12.2.7	okvCustomAttrAddInteger	12-112
12.2.8	okvCustomAttrAddInterval	12-113
12.2.9	okvCustomAttrAddLongInteger	12-114
12.2.10	okvCustomAttrAddStructure	12-115
12.2.11	okvCustomAttrAddTextString	12-117
12.2.12	okvCustomAttrGet	12-118
12.2.13	okvCustomAttrGetBigInteger	12-119
12.2.14	okvCustomAttrGetBigIntegerLen	12-121
12.2.15	okvCustomAttrGetBoolean	12-122
12.2.16	okvCustomAttrGetByName	12-124
12.2.17	okvCustomAttrGetByteString	12-125
12.2.18	okvCustomAttrGetByteStringLen	12-127
12.2.19	okvCustomAttrGetByType	12-128
12.2.20	okvCustomAttrGetDateTime	12-129
12.2.21	okvCustomAttrGetEnum	12-130
12.2.22	okvCustomAttrGetInteger	12-132
12.2.23	okvCustomAttrGetInterval	12-133
12.2.24	okvCustomAttrGetLongInteger	12-135
12.2.25	okvCustomAttrGetStructure	12-136
12.2.26	okvCustomAttrGetTextString	12-138
12.2.27	okvCustomAttrGetTextStringLen	12-139

13 Oracle Key Vault Client SDK Extension Operation Management APIs

13.1	About the Oracle Key Vault Client SDK Extension Operation Management APIs	13-1
13.2	okvOpsCreate	13-1
13.3	okvOpsExecuteOp	13-2
13.4	okvOpsFree	13-4

14 Oracle Key Vault Client SDK TTLV Object APIs

14.1	About the Oracle Key Vault Client SDK TTLV Object APIs	14-2
14.2	okvTTLVAddToObject	14-2
14.3	okvTTLVAddToObjectByTag	14-3
14.4	okvTTLVGetChild	14-4
14.5	okvTTLVGetChildByTag	14-6
14.6	okvTTLVGetChildCount	14-7
14.7	okvTTLVGetChildCountByTag	14-8
14.8	okvTTLVGetFirstChildByTag	14-9
14.9	okvTTLVGetLen	14-10
14.10	okvTTLVGetRequest	14-12
14.11	okvTTLVGetResponse	14-13
14.12	okvTTLVGetTag	14-14
14.13	okvTTLVGetType	14-15
14.14	okvTTLVGetValue	14-16
14.15	okvTTLVGetValueCopy	14-17

15 Oracle Key Vault Client SDK Utility APIs

15.1	About the Oracle Key Vault Client SDK Utility APIs	15-4
15.2	okvAttrExtractTTLV	15-4
15.3	okvAttrMakeTTLV	15-5
15.4	okvCryptoContextCreate	15-6
15.5	okvCryptoContextFree	15-7
15.6	okvCryptoContextGetAuthEncryptionAdditionalData	15-8
15.7	okvCryptoContextGetAuthEncryptionTag	15-9
15.8	okvCryptoContextGetBlockCipherMode	15-11
15.9	okvCryptoContextGetIV	15-12
15.10	okvCryptoContextGetPadding	15-13
15.11	okvCryptoContextGetRandomIV	15-14
15.12	okvCryptoContextSetAuthEncryptionAdditionalData	15-15
15.13	okvCryptoContextSetAuthEncryptionTag	15-16
15.14	okvCryptoContextSetBlockCipherMode	15-17
15.15	okvCryptoContextSetIV	15-18

15.16	okvCryptoContextSetPadding	15-20
15.17	okvCryptoContextSetRandomIV	15-21
15.18	okvCryptoResponseGetAuthEncryptionTag	15-22
15.19	okvCryptoResponseGetDecryptedData	15-23
15.20	okvCryptoResponseGetEncryptedData	15-25
15.21	okvCryptoResponseGetIV	15-26
15.22	okvDecryptResponseCreate	15-27
15.23	okvDecryptResponseFree	15-28
15.24	okvEncryptResponseCreate	15-29
15.25	okvEncryptResponseFree	15-31
15.26	okvGetTextForAttributeNum	15-32
15.27	okvGetTextForTag	15-33
15.28	okvGetTextForTagEnum	15-34
15.29	okvGetTextForTagType	15-35
15.30	okvGetTextLenForAttributeNum	15-36
15.31	okvObjGetAttrNo	15-37
15.32	okvCryptoContextSetCryptoAlgo	15-38
15.33	okvCryptoContextSetHashingAlgo	15-39
15.34	okvCryptoContextSetDigitalSignAlgo	15-40
15.35	okvCryptoContextGetCryptoAlgo	15-41
15.36	okvCryptoContextGetHashingAlgo	15-42
15.37	okvCryptoContextGetDigitalSignAlgo	15-43
15.38	okvCryptoResponseGetSignatureData	15-45
15.39	okvCryptoResponseGetRecoveredData	15-46
15.40	okvCryptoResponseGetValidity	15-47
15.41	okvSignResponseCreate	15-48
15.42	okvSignResponseFree	15-49
15.43	okvSignVerifyResponseCreate	15-50
15.44	okvSignVerifyResponseFree	15-51

Part III Oracle Key Vault Client Java SDK API Reference

16 Oracle Key Vault Java SDK Packages

16.1	oracle.okv.exception Java Package	16-1
16.2	oracle.okv.kmip Java Package	16-2
16.3	oracle.okv.operation Java Package	16-3
16.4	oracle.okv.response Java Package	16-3
16.5	oracle.okv.service Java Package	16-4

17 Oracle Key Vault Java SDK APIs

17.1	Java SDK Management APIs	17-1
17.2	Java SDK Connection Management APIs	17-1
17.3	Java SDK KMIP APIs	17-2
17.4	Java SDK KMIP Batch APIs	17-3
17.5	Java SDK KMIP Attribute APIs	17-4
17.6	Java SDK KMIP Custom Attribute APIs	17-6
17.7	Java SDK Extension Operation Management APIs	17-7
17.8	Java SDK TTLV Object APIs	17-7
17.9	Java SDK Utility APIs	17-7

Part IV Oracle Key Vault Client SDK Troubleshooting

18 Troubleshooting

Index

Custom Legal Notice

Preface

Welcome to *Oracle Key Vault Developer's Guide*. This guide explains how to use the Oracle Key Vault client SDK to integrate Oracle and non-Oracle products directly with Oracle Key Vault.

This preface contains:

- [Audience](#)
- [Documentation Accessibility](#)
- [Diversity and Inclusion](#)
- [Related Documents](#)
- [Conventions](#)

Audience

This document is intended for application developers using the C and Java programming languages to manage Oracle and non-Oracle heterogenous solutions for use with Oracle Key Vault.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Documents

For more information, see these Oracle resources:

- *Oracle Key Vault Administrator's Guide*
- *Oracle Key Vault Developer's Guide*
- *Oracle Key Vault Licensing Information*
- *Oracle Key Vault Release Notes*
- *Oracle Key Vault RESTful Services Administrator's Guide*
- *Oracle Key Vault Root of Trust HSM Configuration Guide*

Additional information available:

- [Key Management Interoperability Protocol Specification Version 1.1](#)

To download the product data sheet, frequently asked questions, links to the latest product documentation, product download, and other collateral, visit Oracle Technical Resources (formerly Oracle Technology Network). You must register online before using Oracle Technical Services. Registration is free and can be done at

<https://www.oracle.com/technical-resources/>

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Part I

Introduction to the Oracle Key Vault Client SDK

Part I provides an overview and explains who should use this guide and the advantages of the Oracle Key Vault client SDK.

- [Changes in This Release](#)
This Oracle Key Vault release introduces new features that enhance the use of the Oracle Key Vault Client SDK.
- [Getting Started with the Oracle Key Vault Client SDK](#)
The Oracle Key Vault client SDK is designed for C and Java programmers who understand Oracle Key Vault.
- [KMIP Features of the Oracle Key Vault Client SDK](#)
The communication exchange between the Oracle Key Vault client SDK and the Oracle Key Vault server will make use of the KMIP protocol.
- [Setting Up the Oracle Key Vault SDK](#)
The client SDK is available in both C and Java.
- [Oracle Key Vault Client SDK Program Structure](#)
The Oracle Key Vault client SDK program structure covers areas such as the program flow, types, environment, connection, and session.

1

Changes in This Release

This Oracle Key Vault release introduces new features that enhance the use of the Oracle Key Vault Client SDK.

- [Changes for Oracle Key Vault Client SDK Release 21.6](#)
Oracle Key Vault Client SDK release 21.6 introduces several new features.
- [Changes for Oracle Key Vault Client SDK Release 21.5](#)
Oracle Key Vault Client SDK release 21.5 introduces no new features.
- [Changes for Oracle Key Vault Client SDK Release 21.4](#)
Oracle Key Vault Client SDK release 21.4 introduces several new features.
- [Changes for Oracle Key Vault Client SDK Release 21.3](#)
Oracle Key Vault Client SDK release 21.3 introduces no new features.
- [Changes for Oracle Key Vault Client SDK Release 21.2](#)
Oracle Key Vault Client SDK release 21.2 introduces several new features.

1.1 Changes for Oracle Key Vault Client SDK Release 21.6

Oracle Key Vault Client SDK release 21.6 introduces several new features.

- [Support for Sign and Signature Verify Operations](#)
Starting release 21.6, Oracle Key Vault C and Java SDKs now provide Sign and Verify capability.
- [Ability to Control the Extraction of Private Keys from Oracle Key Vault](#)
Starting in Oracle Key Vault release 21.6, to strengthen the protection of private keys, you can now restrict these keys from leaving Oracle Key Vault.

1.1.1 Support for Sign and Signature Verify Operations

Starting release 21.6, Oracle Key Vault C and Java SDKs now provide Sign and Verify capability.

You can use either RESTful services utility commands, `okvutil`, or C and Java SDK to perform sign and signature verify operations.

C SDK APIs

- KMIP cryptographic operations are as follows:
 - `okvSign`
 - `okvSignVerify`
- Cryptographic utility operations are as follows:
 - `okvCryptoContextGetCryptoAlgo`
 - `okvCryptoContextGetHashingAlgo`
 - `okvCryptoContextGetDigitalSignAlgo`

- okvCryptoContextSetHashingAlgo
- okvCryptoContextSetCryptoAlgo
- okvCryptoContextSetDigitalSignAlgo
- okvCryptoResponseGetSignatureData
- okvCryptoResponseGetRecoveredData
- okvCryptoResponseGetValidity
- okvSignResponseCreate
- okvSignVerifyResponseCreate
- okvSignResponseFree
- okvSignVerifyResponseFree

Java SDK APIs

- KMIP cryptographic operations are as follows:
 - okvSign
 - okvSignVerify
- Cryptographic utility operations are as follows:
 - getCryptoAlgo
 - getHashingAlgo
 - getDigitalSignAlgo
 - setCryptoAlgo
 - setHashingAlgo
 - setDigitalSignAlgo
 - getSignatureData
 - getRecoveredData
 - getValidity

Related Topics

- [Oracle Key Vault Client C SDK API Reference](#)
- [Oracle Key Vault Client Java SDK API Reference](#)

1.1.2 Ability to Control the Extraction of Private Keys from Oracle Key Vault

Starting in Oracle Key Vault release 21.6, to strengthen the protection of private keys, you can now restrict these keys from leaving Oracle Key Vault.

This restriction applies to the key material of the private keys, but not its metadata. If your site requires that private keys never leave Oracle Key Vault, then you can configure these keys to remain within Oracle Key Vault during operations. In this case, the Sign operation can be leveraged to use these keys without them ever leaving Oracle Key Vault itself.

You can use the Oracle Key Vault management console, RESTful services utility commands, the C SDK APIs, and Java SDK APIs to control the retrieval (extraction) of private keys from Oracle Key Vault, .

Related Topics

- [Oracle Key Vault Client C SDK API Reference](#)
- [Oracle Key Vault Client Java SDK API Reference](#)

1.2 Changes for Oracle Key Vault Client SDK Release 21.5

Oracle Key Vault Client SDK release 21.5 introduces no new features.

1.3 Changes for Oracle Key Vault Client SDK Release 21.4

Oracle Key Vault Client SDK release 21.4 introduces several new features.

- [C and Java SDK APIs for Cryptographic Operations](#)
Oracle Key Vault Client SDK release 21.4 adds the support for cryptographic operations.
- [Client Endpoint File Updated When A KMIP Server Operation Is Executed Using SDK](#)
The client endpoint file `okvclient.ora` is now updated when a KMIP server operation is executed using the SDK.
- [Ability to Control the Extraction of Symmetric Encryption Keys from Oracle Key Vault](#)
Starting in Oracle Key Vault release 21.4, to strengthen the protection of symmetric encryption keys, you now can restrict these keys from leaving Oracle Key Vault.

1.3.1 C and Java SDK APIs for Cryptographic Operations

Oracle Key Vault Client SDK release 21.4 adds the support for cryptographic operations.

Oracle Key Vault release 21.4 adds support for performing encryption and decryption cryptographic operations within Oracle Key Vault.

You can use either RESTful services utility commands or C and Java SDK to perform encryption and decryption operations.

C SDK APIs

- KMIP cryptographic operations are as follows:
 - `okvDecrypt`
 - `okvEncrypt`
- Attribute operations are as follows:
 - `okvAttrAddExtractable`
 - `okvAttrAddNeverExtractable`
 - `okvAttrGetExtractable`
 - `okvAttrGetNeverExtractable`
- Cryptographic utility operations are as follows:
 - `okvCryptoContextCreate`

- okvCryptoContextFree
- okvCryptoContextGetAuthEncryptionAdditionalData
- okvCryptoContextGetAuthEncryptionTag
- okvCryptoContextGetBlockCipherMode
- okvCryptoContextGetIV
- okvCryptoContextGetPadding
- okvCryptoContextGetRandomIV
- okvCryptoContextSetAuthEncryptionAdditionalData
- okvCryptoContextSetAuthEncryptionTag
- okvCryptoContextSetBlockCipherMode
- okvCryptoContextSetIV
- okvCryptoContextSetPadding
- okvCryptoContextSetRandomIV
- okvCryptoResponseGetAuthEncryptionTag
- okvCryptoResponseGetDecryptedData
- okvCryptoResponseGetEncryptedData
- okvCryptoResponseGetIV
- okvDecryptResponseCreate
- okvDecryptResponseFree
- okvEncryptResponseCreate
- okvEncryptResponseFree

Java SDK APIs

- KMIP cryptographic operations are as follows:
 - okvDecrypt
 - okvEncrypt
- Attribute operations are as follows:
 - okvAttrAddExtractable
 - okvAttrAddNeverExtractable
 - okvAttrGetExtractable
 - okvAttrGetNeverExtractable
- Cryptographic utility operations are as follows:
 - okvCryptoContextCreate

Related Topics

- [Oracle Key Vault Client C SDK API Reference](#)
- [Oracle Key Vault Client Java SDK API Reference](#)

1.3.2 Client Endpoint File Updated When A KMIP Server Operation Is Executed Using SDK

The client endpoint file `okvclient.ora` is now updated when a KMIP server operation is executed using the SDK.

Prior to Oracle Key Vault release 21.4, the client endpoint file `okvclient.ora` was not updated whenever a KMIP server operation was performed using the SDK. Now, the client endpoint file `okvclient.ora` will be updated if there are any new endpoint updates whenever a KMIP server operation is performed using the Oracle Key Vault client SDK.

1.3.3 Ability to Control the Extraction of Symmetric Encryption Keys from Oracle Key Vault

Starting in Oracle Key Vault release 21.4, to strengthen the protection of symmetric encryption keys, you now can restrict these keys from leaving Oracle Key Vault.

This restriction applies to the key material of the symmetric keys, but not its metadata. For example, Transparent Database Encryption (TDE) master encryption keys are stored in Oracle Key Vault. When an endpoint needs to decrypt the key, the PKCS#11 library fetches the TDE master encryption key from Oracle Key Vault to perform the decryption. If your site requires that symmetric keys never leave Oracle Key Vault, then you can configure these keys to remain within Oracle Key Vault during operations. In this case, the PKCS#11 library will send the encrypted data encryption key to Oracle Key Vault. Decryption is then performed within Oracle Key Vault and afterward, the plaintext data encryption key is returned to the PKCS#11 library. The Oracle Key Vault PKCS#11 library performs the encryption and decryption operation within Oracle Key Vault if the TDE master key is restricted to leave Oracle Key Vault, or if it cannot be extracted from Oracle Key Vault.

To control whether symmetric encryption keys can be retrieved (extracted) from Oracle Key Vault, you can use the Oracle Key Vault management console, RESTful services utility commands, the C SDK APIs, and Java SDK APIs.

New APIs for the C SDK to manage extractable attribute:

- `okvAttrAddExtractable`
- `okvAttrAddNeverExtractable`
- `okvAttrGetExtractable`
- `okvAttrGetNeverExtractable`

New APIs for the Java SDK to manage extractable attribute:

- `okvAttrAddExtractable`
- `okvAttrAddNeverExtractable`
- `okvAttrGetExtractable`
- `okvAttrGetNeverExtractable`

Related Topics

- [Managing the Extraction of Symmetric Keys from Oracle Key Vault](#)
- [Configuring the Global Default Extraction for New Symmetric Keys](#)

1.4 Changes for Oracle Key Vault Client SDK Release 21.3

Oracle Key Vault Client SDK release 21.3 introduces no new features.

1.5 Changes for Oracle Key Vault Client SDK Release 21.2

Oracle Key Vault Client SDK release 21.2 introduces several new features.

- [New C and Java SDK APIs for Certificates, Certificate Requests, Private Keys, and Public Keys](#)
In Oracle Key Vault release 21.2, new APIs enable you to perform operations such as registering and fetching objects, and adding attributes to those objects (for example, length, type, ID, subject, issuer, and algorithm).

1.5.1 New C and Java SDK APIs for Certificates, Certificate Requests, Private Keys, and Public Keys

In Oracle Key Vault release 21.2, new APIs enable you to perform operations such as registering and fetching objects, and adding attributes to those objects (for example, length, type, ID, subject, issuer, and algorithm).

C SDK APIs

Registration and fetch operations are as follows:

- `okvGetCertificate`
- `okvGetCertificateRequest`
- `okvGetPrivateKey`
- `okvGetPublicKey`
- `okvRegCertificate`
- `okvRegCertificateRequest`
- `okvRegPrivateKey`
- `okvRegPublicKey`

Attribute operations are as follows:

- `okvAttrAddCertLen`
- `okvAttrAddCertType`
- `okvAttrAddDigitalSignAlgo`
- `okvAttrAddX509CertId`
- `okvAttrAddX509CertIss`
- `okvAttrAddX509CertIssAltName`
- `okvAttrAddX509CertSubj`
- `okvAttrAddX509CertSubjAltName`
- `okvAttrGetCertLen`

- `okvAttrGetCertType`
- `okvAttrGetDigitalSignAlgo`
- `okvAttrGetX509CertId`
- `okvAttrGetX509CertIdIssuerLen`
- `okvAttrGetX509CertIdSerialNoLen`
- `okvAttrGetX509CertIss`
- `okvAttrGetX509CertIssAltName`
- `okvAttrGetX509CertIssAltNameLen`
- `okvAttrGetX509CertIssDNLen`
- `okvAttrGetX509CertSubj`
- `okvAttrGetX509CertSubjAltName`
- `okvAttrGetX509CertSubjAltNameLen`
- `okvAttrGetX509CertSubjDNLen`

Java SDK APIs

Registration and fetch operations are as follows:

- `okvGetCertificate`
- `okvGetCertificateRequest`
- `okvGetPrivateKey`
- `okvGetPublicKey`
- `okvRegCertificate`
- `okvRegCertificateRequest`
- `okvRegPrivateKey`
- `okvRegPublicKey`

Attribute operations are as follows:

- `okvAttrAddArchiveDate`
- `okvAttrAddCertLen`
- `okvAttrAddCertType`
- `okvAttrAddDigitalSignAlgo`
- `okvAttrAddInitialDate`
- `okvAttrAddLastChangeDate`
- `okvAttrAddState`
- `okvAttrAddX509CertId`
- `okvAttrAddX509CertIss`
- `okvAttrAddX509CertIssAltName`
- `okvAttrAddX509CertSubj`

- `okvAttrAddX509CertSubjAltName`
- `okvAttrGetCertLen`
- `okvAttrGetCertType`
- `okvAttrGetDigitalSignAlgo`
- `okvAttrGetX509CertId`
- `okvAttrGetX509CertIss`
- `okvAttrGetX509CertIssAltName`
- `okvAttrGetX509CertSubj`
- `okvAttrGetX509CertSubjAltName`

Related Topics

- [Getting Started with the Oracle Key Vault Client SDK](#)
The Oracle Key Vault client SDK is designed for C and Java programmers who understand Oracle Key Vault.

2

Getting Started with the Oracle Key Vault Client SDK

The Oracle Key Vault client SDK is designed for C and Java programmers who understand Oracle Key Vault.

- [About Getting Started with the Oracle Key Vault Client SDK](#)
The Oracle Key Vault Client SDK provides C and Java APIs to create custom applications that enable Oracle and non-Oracle products to integrate directly with Oracle Key Vault. However, it is not designed to manage endpoints or to function as an encryption library.
- [Who Should Use This Guide](#)
This guide is intended for proficient C and Java programmers who are adept Oracle Key Vault and Oracle Database administrative users.
- [Platforms Supported](#)
Oracle Key Vault Software Development Kit is supported on various platforms depending on the programming language.
- [Advantages of Using the Oracle Key Vault Client SDK](#)
Oracle Key Vault client SDK will allow an endpoint program to access the Oracle Key Vault server and be able to perform multiple KMIP operations on the objects stored in the Oracle Key Vault server.

2.1 About Getting Started with the Oracle Key Vault Client SDK

The Oracle Key Vault Client SDK provides C and Java APIs to create custom applications that enable Oracle and non-Oracle products to integrate directly with Oracle Key Vault. However, it is not designed to manage endpoints or to function as an encryption library.

The Oracle Key Vault Client SDK addresses product-specific key management issues.

The following are the features of the Oracle Key Vault Client SDK:

- Enables an endpoint program to access the Oracle Key Vault server and execute multiple KMIP operations on the Key Vault server objects.
- Available for C and Java platforms.
- Is designed to enable Oracle and non-Oracle products to manage keys, credentials, symmetric keys, and other secrets. Enables users to manage heterogeneous solutions. Users can create, register, retrieve, and delete objects, as well as add, delete, and modify attributes of objects.
- Supports authentication with the Oracle Key Vault server and also can use the Oracle Key Vault configuration files. Enables endpoints to use their own connection management. The client SDK can communicate with the Key Vault server by using a mutually authenticated secure connection (TLS).
- Enables endpoints to make use of their own memory management.

2.2 Who Should Use This Guide

This guide is intended for proficient C and Java programmers who are adept Oracle Key Vault and Oracle Database administrative users.

2.3 Platforms Supported

Oracle Key Vault Software Development Kit is supported on various platforms depending on the programming language.

C

- Linux
- Solaris SPARC64
- Solaris x64
- AIX
- HP-UX

Java

- Platform Neutral

2.4 Advantages of Using the Oracle Key Vault Client SDK

Oracle Key Vault client SDK will allow an endpoint program to access the Oracle Key Vault server and be able to perform multiple KMIP operations on the objects stored in the Oracle Key Vault server.

The key advantages of using the Oracle Key Vault Client SDK are:

- Externalize Key Management to Oracle Key Vault.
- Support KMIP operation and objects.
- Simplified connection setup.
- Tight integration with endpoint enrollment.
- Easy to embed the SDK in an existing C or Java program.
- Easy to update existing code that interfaces with another key management provider, providing the full power of KMIP key management.
- Simple and intuitive to use.
- Complies with various regulations and mandates that cover physical separation of encryption keys and encrypted data. Externalizing key management provides this separation, hence security of the overall environment is enhanced.

3

KMIP Features of the Oracle Key Vault Client SDK

The communication exchange between the Oracle Key Vault client SDK and the Oracle Key Vault server will make use of the KMIP protocol.

The Key Vault Client SDK simplifies the KMIP exposure to the endpoint and supports additional functionality that makes it easier for the endpoints to communicate with the Oracle Key Vault server.

- [KMIP Version](#)
The Oracle Key Vault client SDK supports Version 1.1 of the KMIP specification, limited to those objects and operations required by supported profiles.
- [KMIP Profile Support](#)
The Oracle Key Vault client SDK supports four KMIP profiles.
- [KMIP Managed Objects](#)
The Oracle Key Vault client SDK supports four KMIP managed objects.
- [KMIP Operations](#)
The Oracle Key Vault client SDK supports 19 KMIP operations.

3.1 KMIP Version

The Oracle Key Vault client SDK supports Version 1.1 of the KMIP specification, limited to those objects and operations required by supported profiles.

In addition, it also supports the encrypt, decrypt, sign, and signature verify operations and the `EXTRACTABLE` attribute as defined in later versions.

3.2 KMIP Profile Support

The Oracle Key Vault client SDK supports four KMIP profiles.

The supported profiles are as follows:

- Basic Asymmetric Key and Certificate Store
- Basic Symmetric Key Foundry and Server
- Basic Symmetric Key Store and Server
- Secret Data

3.3 KMIP Managed Objects

The Oracle Key Vault client SDK supports four KMIP managed objects.

These managed objects are as follows:

- Opaque object
- Secret data
- Symmetric key
- Template
- Certificate
- Public Key
- Private Key

3.4 KMIP Operations

The Oracle Key Vault client SDK supports 19 KMIP operations.

These KMIP operations are as follows:

- Create
- Register (of keys, certificates, secrets, opaque objects, and templates)
- Rekey
- Locate
- Get (of keys, certificates, secrets, opaque objects, and templates)
- Get Attribute
- Get Attribute List
- Add Attribute
- Modify Attribute
- Delete Attribute
- Activate
- Revoke
- Destroy
- Query
- Encrypt
- Decrypt
- Sign
- Signature Verify
- Create Key Pair

4

Setting Up the Oracle Key Vault SDK

The client SDK is available in both C and Java.

- [Enrolling an Endpoint](#)
An Endpoint must be registered and enrolled to the Oracle Key Vault server before downloading the SDK content to that endpoint.
- [Downloading the C or Java SDK Software](#)
You must download the appropriate Software Development Kit (SDK) software, either the C or Java version.
- [Contents of the C SDK File](#)
The contents of C SDK file include demo programs, the SDK library file, and other necessary files.
- [Contents of the Java SDK File](#)
The contents of Java SDK file include demo programs, the SDK library jar file, and other necessary files.

4.1 Enrolling an Endpoint

An Endpoint must be registered and enrolled to the Oracle Key Vault server before downloading the SDK content to that endpoint.

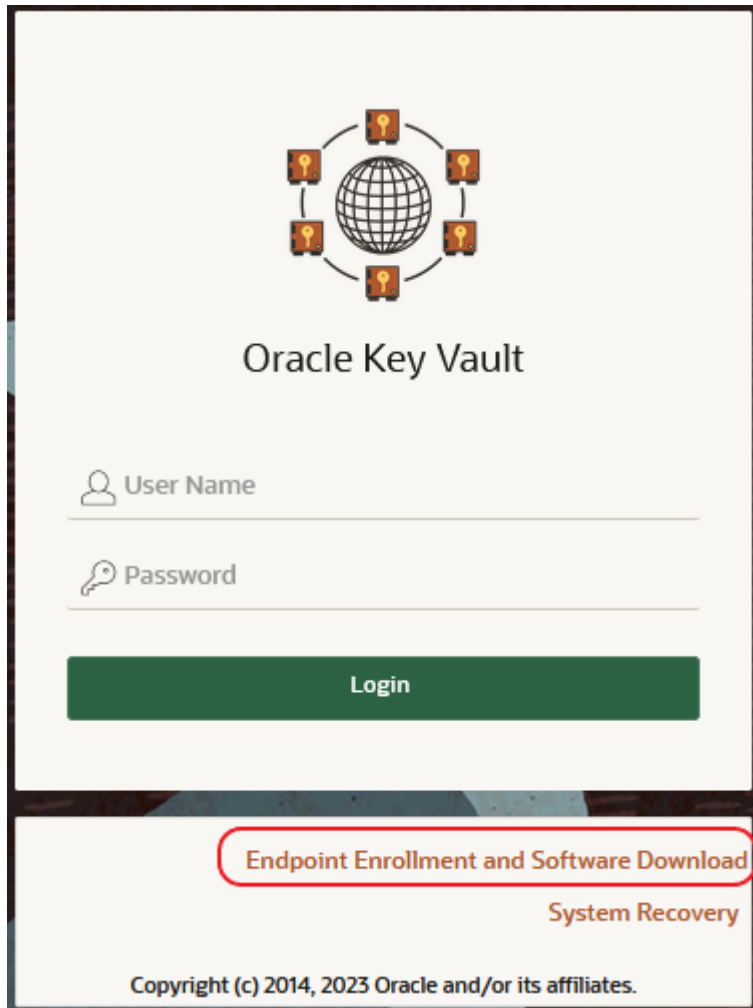
If the endpoint is not already registered and enrolled before downloading the SDK, please enroll the endpoint by following the instructions from [Enrolling Endpoints for Oracle Key Vault](#).

4.2 Downloading the C or Java SDK Software

You must download the appropriate Software Development Kit (SDK) software, either the C or Java version.

1. Access the Oracle Key Vault management console from the endpoint on which you wish to deploy the SDK.
2. The login page to the Oracle Key Vault management console appears.
Do not log in.
3. Click the **Endpoint Enrollment and Software Download** link below the **Login** button.

Figure 4-1 Endpoint Enrollment and Software Download



4. The **Enroll Endpoint & Download Software** screen appears.
There are four tabs along the top.
 - Enroll Endpoint & Download Software
 - Download Endpoint Software Only
 - Download RESTful Service Utility
 - Download Software Development Kit
5. Click the **Download Software Development Kit** tab.

Figure 4-2 Download Software Development Kit

Enroll Endpoint & Download Software | Download Endpoint Software Only | Download RESTful Service Utility | **Download Software Development Kit**

Enroll Endpoint & Download Software Cancel Clear Enroll

To enroll an endpoint, enter your endpoint Enrollment Token and click 'Submit Token'. Update the endpoint details if necessary and click 'Enroll' to complete the enrollment. Download the endpoint package when prompted.

Enrollment Token Submit Token

Endpoint Type

Endpoint Platform

Email

Description

6. The Download Software Development Kit screen appears with the option to select either the C or Java SDK.

Figure 4-3 Select C as the SDK Language

Enroll Endpoint & Download Software | Download Endpoint Software Only | Download RESTful Service Utility | **Download Software Development Kit**

Download Software Development Kit Cancel Download

To download the Software Development Kit, select the SDK language, choose the appropriate SDK platform (if applicable) and click 'Download'. You must have a previously provisioned endpoint to deploy and use the SDK.

SDK Language C Java

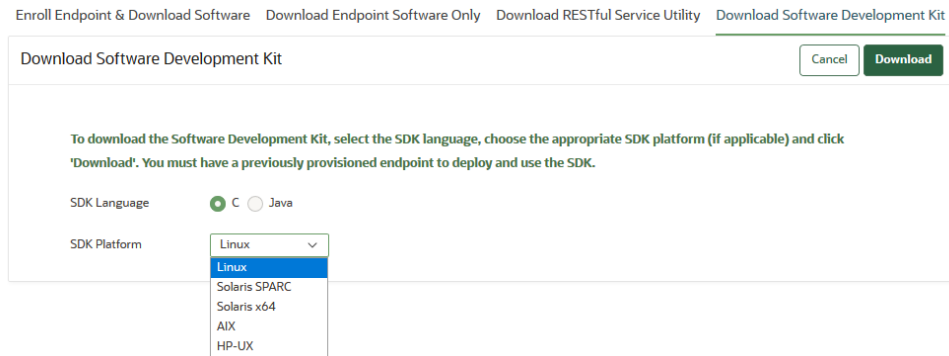
SDK Platform

7. If you select the C SDK, you must select the platform for deployment.

The platform options are:

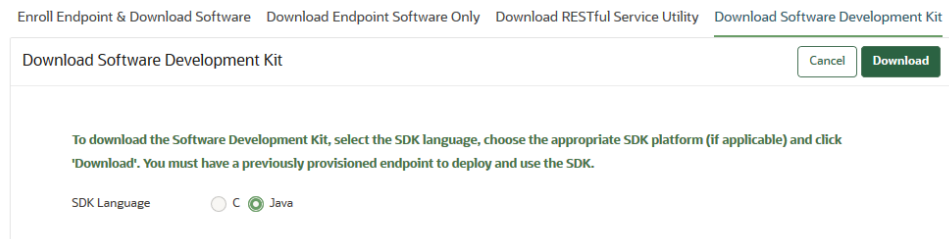
- Linux
- Solaris SPARC
- Solaris x64
- AIX
- HP-UX

Figure 4-4 Select SDK Platform



If you choose the Java SDK, it is platform independent and does not require you to choose a platform.

Figure 4-5 Select Java as the SDK Language



8. Click **Download**.
 Save the SDK zip file to the desired location.
9. Ensure that you have the necessary administrative privileges to install software on the endpoint.
10. Check that the `OKV_HOME` environment variable is correctly set.
 See the README file included in the zip file for more information.
11. Navigate to the directory in which you saved the zip file.
12. Unzip the SDK file.

For example, on Linux, to unzip the Java SDK file, use:

```
unzip -o okv_jsdk.zip -d $OKV_HOME
```

or for the C SDK file, use:

```
unzip -o okv_csdk.zip -d $OKV_HOME
```


 **Note:**

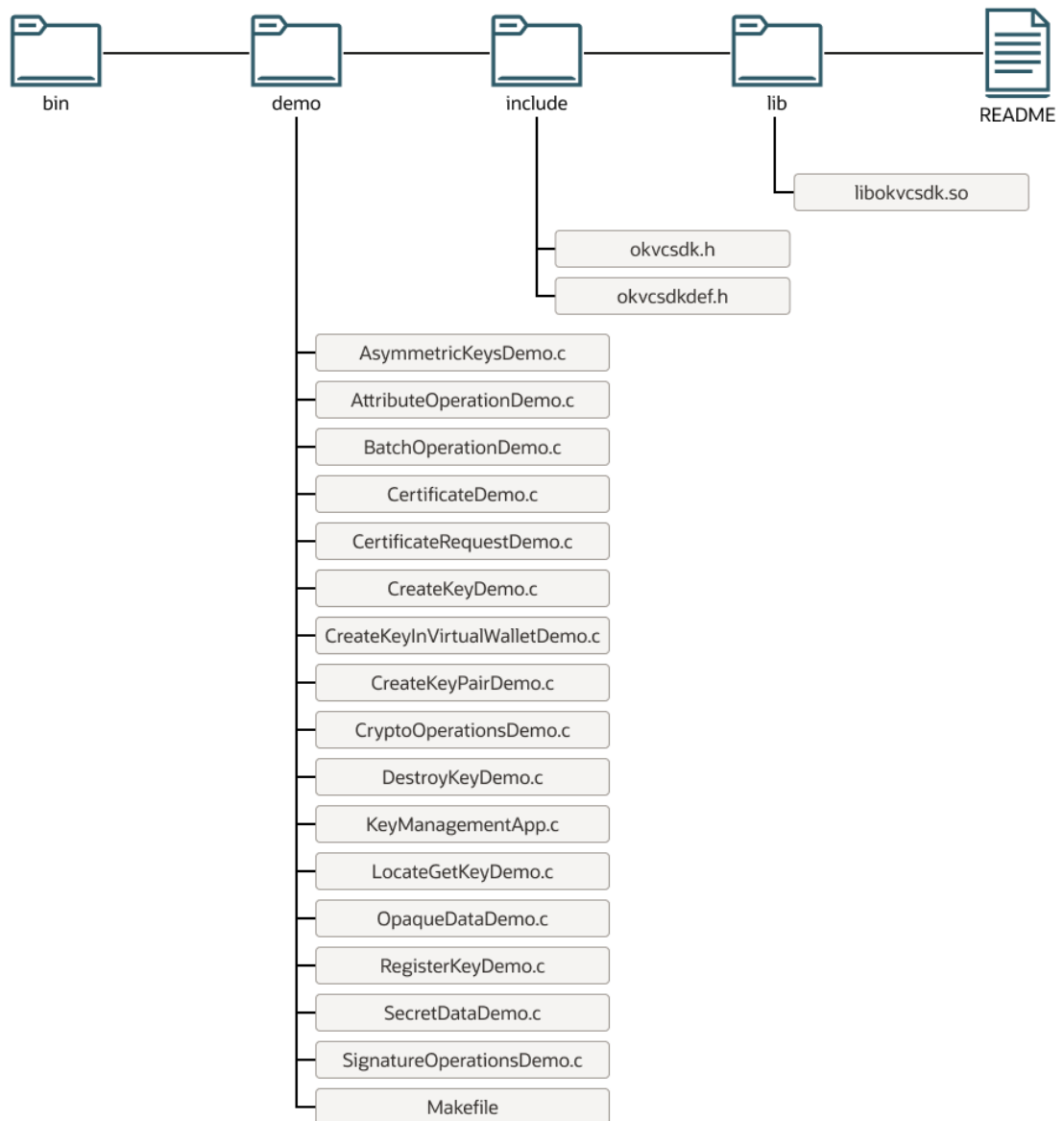
Oracle recommends you to deploy the SDK software contents under `OKV_HOME`. This applies even during redeployment or upgrade to new version of the SDK software.

Oracle recommends to redeploy the SDK software in the same location post upgrade to Oracle Key Vault 21.6 if already deployed in Oracle Key Vault 21.x.

4.3 Contents of the C SDK File

The contents of C SDK file include demo programs, the SDK library file, and other necessary files.

Figure 4-6 C SDK Directories and Files



The `include` directory contains header files for C SDK APIs. The `lib` directory contains the shared library object. `bin` is an empty directory to place the demo program object files and executables.

The `demo` directory contains sample programs which demonstrate the use of the C SDK APIs. The table below provides a brief description of each sample program.

Table 4-1 Sample Programs

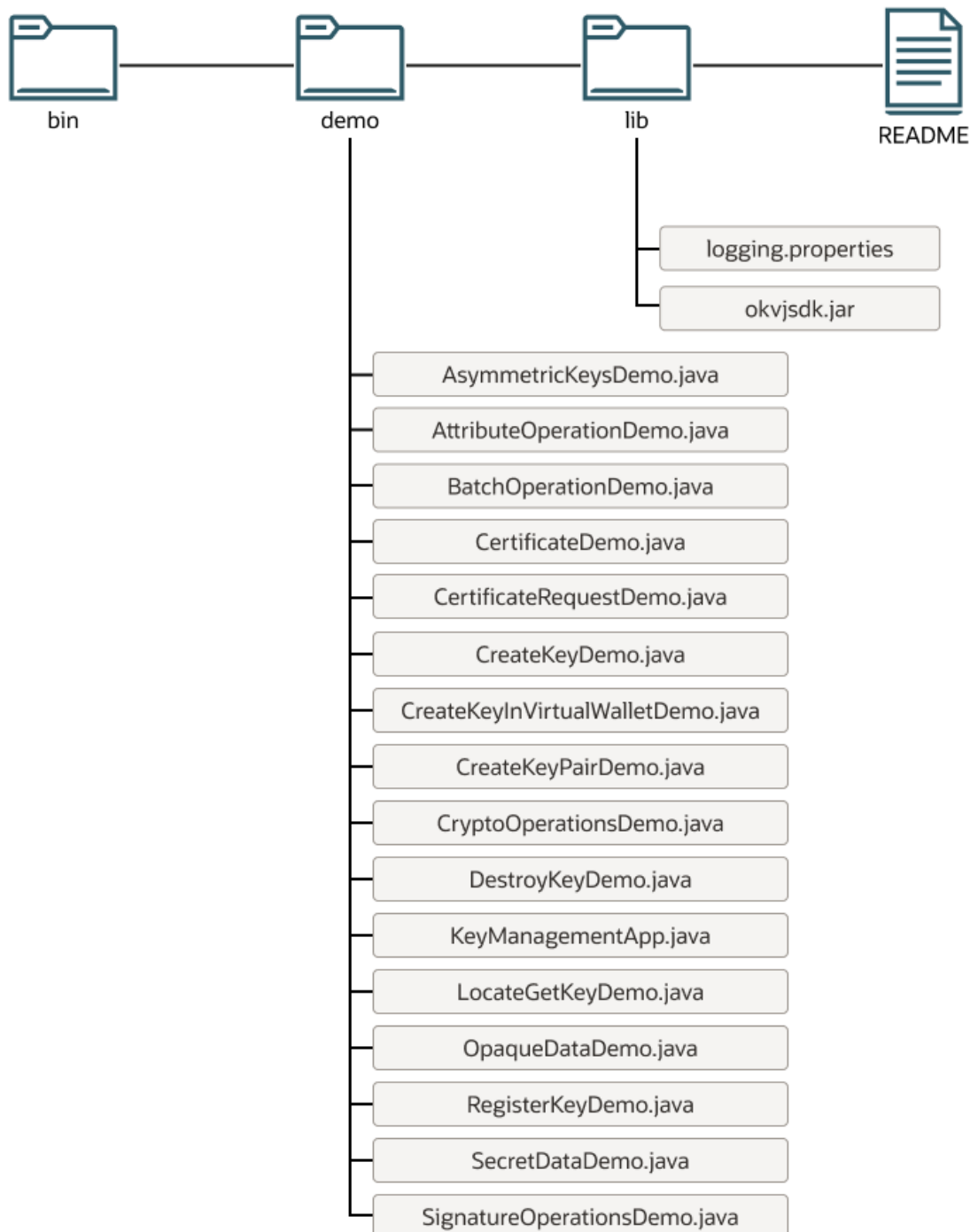
Sample Program	Description
<code>AsymmetricKeysDemo.c</code>	Application for Asymmetric Keys management operations such as register, activate, get, get all attributes of private and public keys.
<code>AttributeOperationDemo.c</code>	Application for KMIP attribute operations such as add, modify, get, and delete attributes.
<code>BatchOperationDemo.c</code>	Application to demonstrate batching such as batching of create, activate, add attribute, get key, and destroy operations.
<code>CertificateDemo.c</code>	Application for Certificate management operations such as register, activate, get certificate and get all attributes.
<code>CertificateRequestDemo.c</code>	Application for Certificate Request management operations such as register, get certificate request and get all attributes.
<code>CreateKeyDemo.c</code>	Application for KMIP create and activate key operations.
<code>CreateKeyInVirtualWalletDemo.c</code>	Application for KMIP create key operation in the given wallet and activate the key.
<code>CreateKeyPairDemo.c</code>	Application for KMIP create key pair and activate key operations.
<code>CryptoOperationsDemo.c</code>	Application to demonstrate encrypt and decrypt operations.
<code>DestroyKeyDemo.c</code>	Application for KMIP locate operation by given name and destroy the key.
<code>KeyManagementApp.c</code>	Application for Key management operations such as create, activate, get, deactivate, and destroy key.
<code>LocateGetKeyDemo.c</code>	Application for KMIP locate operation by given name and get the key details like key length, algorithm, and value.
<code>OpaqueDataDemo.c</code>	Application for Opaque Data management operations such as register, get, add attribute, and destroy opaque data.
<code>RegisterKeyDemo.c</code>	Application for KMIP register key operation.
<code>SecretDataDemo.c</code>	Application for Secret Data management operations such as register, activate, add attribute, deactivate, and destroy secret data.
<code>SignatureOperationsDemo.c</code>	Application to demonstrate sign and signature verify operations.

See the `README` file provided with the C SDK for complete instructions about environment configuration, compiling, and running the demo programs.

4.4 Contents of the Java SDK File

The contents of Java SDK file include demo programs, the SDK library jar file, and other necessary files.

Figure 4-7 Java SDK Directories and Files



The `lib` directory contains the Oracle Key Vault Client Java SDK jar file `okvjsdk.jar` and sample `java.util.logging` configuration file `logging.properties`. `bin` is an empty directory to place the Java demo program class files.

The `demo` directory contains sample programs which demonstrate the use of the Java SDK APIs. The table below provides a brief description of each sample program.

Table 4-2 Sample Programs

Sample Program	Description
<code>AsymmetricKeysDemo.java</code>	Application for Asymmetric Keys management operations such as register, activate, get, get all attributes of private and public keys.
<code>AttributeOperationDemo.java</code>	Application for KMIP attribute operations such as add, modify, get, and delete attributes.
<code>BatchOperationDemo.java</code>	Application to demonstrate batching such as batching of create, activate, add attribute, get key, and destroy operations.
<code>CertificateDemo.java</code>	Application for Certificate management operations such as register, activate, get certificate and get all attributes.
<code>CertificateRequestDemo.java</code>	Application for Certificate Request management operations such as register, get certificate request and get all attributes.
<code>CreateKeyDemo.java</code>	Application for KMIP create and activate key operations.
<code>CreateKeyInVirtualWalletDemo.java</code>	Application for KMIP create key operation in the given wallet and activate the key.
<code>CreateKeyPairDemo.java</code>	Application for KMIP create key pair and activate key operations.
<code>CryptoOperationsDemo.java</code>	Application to demonstrate encrypt and decrypt operations.
<code>DestroyKeyDemo.java</code>	Application for KMIP locate operation by given name and destroy the key.
<code>KeyManagementApp.java</code>	Application for Key management operations such as create, activate, get, deactivate, and destroy key.
<code>LocateGetKeyDemo.java</code>	Application for KMIP locate operation by given name and get the key details like key length, algorithm, and value.
<code>OpaqueDataDemo.java</code>	Application for Opaque Data management operations such as register, get, add attribute, and destroy opaque data.
<code>RegisterKeyDemo.java</code>	Application for KMIP register key operation.
<code>SecretDataDemo.java</code>	Application for Secret Data management operations such as register, activate, add attribute, deactivate, and destroy secret data.
<code>SignatureOperationsDemo.java</code>	Application to demonstrate sign and signature verify operations.

See the `README` file provided with the Java SDK for complete instructions about environment configuration, compiling, and running the demo programs.

5

Oracle Key Vault Client SDK Program Structure

The Oracle Key Vault client SDK program structure covers areas such as the program flow, types, environment, connection, and session.

- [About the Oracle Key Vault Client SDK Program Structure](#)
The program structure of an Oracle Key Vault SDK program describes the approach the Oracle Key Vault client will take to write an endpoint SDK program.
- [Oracle Key Vault Program Flow](#)
The Oracle Key Vault general program flow includes creating the environment handle, followed by the connection and session, then termination and release.
- [Oracle Key Vault Program Environment](#)
The Oracle Key Vault program environment is the region or block in the endpoint where the Oracle Key Vault functions are executed.
- [Oracle Key Vault Program Connection](#)
The Oracle Key Vault program connection has two types of connections: explicit and intrinsic.
- [Oracle Key Vault Program Session](#)
The Oracle Key Vault program session are of two types: Oracle Key Vault session and Oracle Key Vault call session.

5.1 About the Oracle Key Vault Client SDK Program Structure

The program structure of an Oracle Key Vault SDK program describes the approach the Oracle Key Vault client will take to write an endpoint SDK program.

The Oracle Key Vault SDK itself is written using certain assumptions and the Oracle Key Vault client must write the endpoint program code in a manner that is consistent with those assumptions.

The Oracle Key Vault client SDK is available for C and Java platforms. The Oracle Key Vault SDK follows the data types, calling conventions, syntax and semantics of the programming language.

The endpoint SDK program can be compiled and linked in the same manner as any other C or Java application. There is no need for any separate pre-processing or post compilations steps.

For an endpoint program to communicate with the Oracle Key Vault server, the endpoint SDK program must follow the program flow, link Oracle Key Vault client SDK library and account for the characteristics of the Oracle Key Vault program.

5.2 Oracle Key Vault Program Flow

The Oracle Key Vault general program flow includes creating the environment handle, followed by the connection and session, then termination and release.

Oracle Key Vault program flows are categorized by their structure and how much KMIP detail is involved to write them: basic and advanced.

- [Basic Program Flow](#)
A basic program works seamlessly with KMIP programs.
- [Advanced Program Flow](#)
The advanced program flow can be categorized as an Oracle Key Vault program with batching and detailed Oracle Key Vault program.

5.2.1 Basic Program Flow

A basic program works seamlessly with KMIP programs.

A basic Oracle Key Vault program has the following characteristics:

- It consists of Oracle Key Vault client SDK functions that perform broad KMIP operations such as creating, activating, retrieving, and registering keys or credentials with Oracle Key Vault server.
- The client need not be aware of the intricate KMIP details when using the functions.
- It contains functions to help the client focus on functionality such as creating and rotating a key, rather than handling details of the KMIP specification, setting up connections with Oracle Key Vault, and other operations.

Advantages of a basic program are as follows:

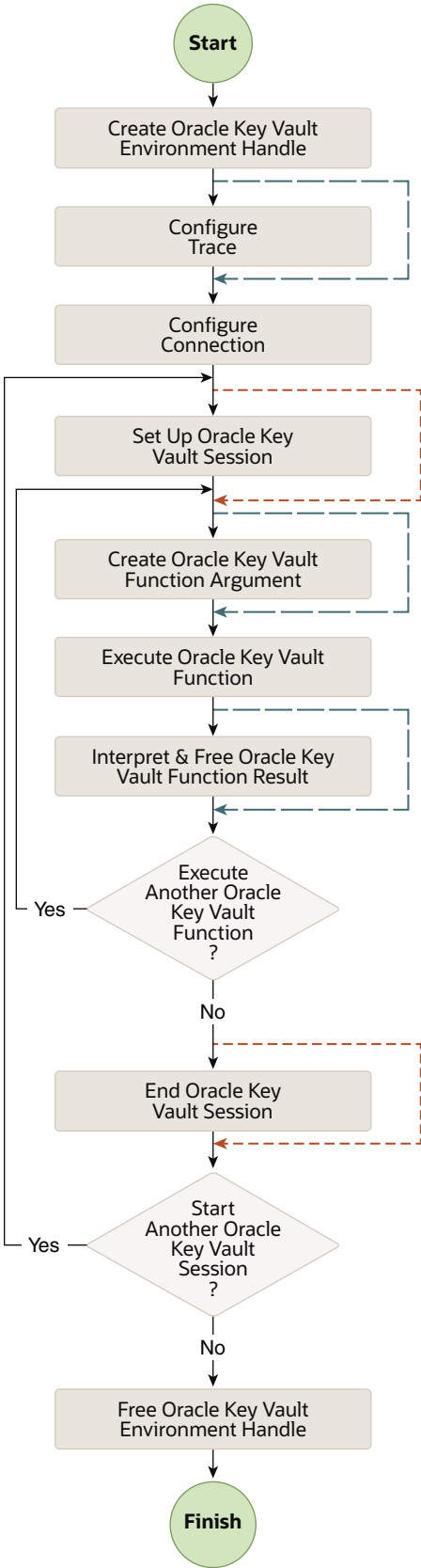
- It is use-case driven.
- It is KMIP agnostic. Very little KMIP knowledge is required to make use of these functions.
- It can be deployed quickly.
- It integrates easily.

The disadvantage of a basic program is that not every KMIP detail is supported.

The basic program flow has the following structure:

1. Create the Oracle Key Vault environment handle.
2. Optionally, configure the trace information.
3. Configure the connection information.
4. Optionally, set up the Oracle Key Vault program session.
 - Create Oracle Key Vault operations or function arguments, if required.
 - Execute the Oracle Key Vault operations or functions.
 - Interpret and free up the Oracle Key Vault operations or function results if necessary.
5. Terminate the Oracle Key Vault program session if it had been established earlier.
6. Release the Oracle Key Vault environment handle.

Figure 5-1 Basic Oracle Key Vault Program Flowchart



Example 5-1 Basic Oracle Key Vault Program

```
...
OKVEnv *env = okvEnvCreate(OKV_MEMORY_FUNCTIONS);
okvEnvSetConfig(env, (oratext *)config_file, (oratext *) connection_pwd);
okvEnvSetTrace(env, (oratext *)trace_dir, OKV_TRACE_DEBUG);
okvConnect(env);
okvCreateKey(env, ..., unique_id, &unique_id_len);
printf("unique identifier %s", unique_id);
okvActivate(env, unique_id);
okvDisconnect(env);
okvDestroy(env, unique_id);
okvEnvFree(&env);
...
```

5.2.2 Advanced Program Flow

The advanced program flow can be categorized as an Oracle Key Vault program with batching and detailed Oracle Key Vault program.

- [Oracle Key Vault Program with Batching](#)
Many KMIP operations such as locating and activating objects can be batched by using the `okvBatchCreate` API.
- [Detailed Oracle Key Vault Program](#)
The detailed Oracle Key Vault program can cover most of the use cases that are allowed by the KMIP protocol.

5.2.2.1 Oracle Key Vault Program with Batching

Many KMIP operations such as locating and activating objects can be batched by using the `okvBatchCreate` API.

Batching two or more KMIP operations means that the KMIP request packets for both the operations will be aggregated and sent to the Oracle Key Vault server together in one super or batched KMIP packet. This reduces round trips for the information exchanged between the client SDK and the Oracle Key Vault server.

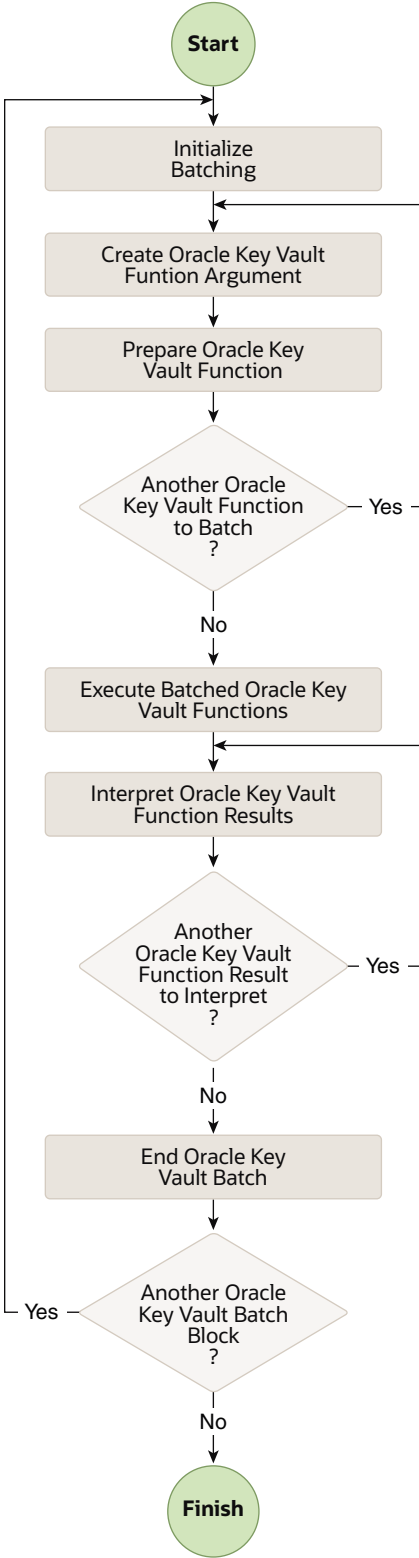
An Oracle Key Vault program with batching has the following structure:

1. Create the Oracle Key Vault environment handle.
2. Optionally, configure the trace information.
3. Configure the connection information.
 - Optionally, set up the Oracle Key Vault program session.
 - Start batching.
 - Create the Oracle Key Vault KMIP TTLV function arguments, if required.
 - Create the Oracle Key Vault functions.
 - Execute the batched operations. This will execute all the Oracle Key Vault functions and possibly process the data returned from the KMIP server.
 - Interpret any Oracle Key Vault function results, if required.
 - End batching.
 - Terminate the Oracle Key Vault program session if it was established earlier.

4. Release the Oracle Key Vault environment handle.

The Oracle Key Vault program flow with batching is same as basic program flow except for the Oracle Key Vault function execution part and is as shown in the figure below.

Figure 5-2 Advanced Oracle Key Vault Program with Batching Flowchart



Example 5-2 Advanced Oracle Key Vault Program With Batching

```
...
OKVEnv *env = okvEnvCreate(OKV_MEMORY_FUNCTIONS);
okvEnvSetConfig(env, (oratext *)config_file, (oratext *) connection_pwd);
okvEnvSetTrace(env, (oratext *)trace_dir, OKV_TRACE_DEBUG);
okvBatchCreate(env);
okvCreateKey(env, ..., unique_id, &unique_id_len);
okvActivate(env, (oratext *)NULL);
okvDestroy(env, (oratext *)NULL);
okvBatchExecute(env);
printf("unique identifier %s", unique_id);
okvBatchFree(env);
okvEnvFree(&env);
...
```

5.2.2.2 Detailed Oracle Key Vault Program

The detailed Oracle Key Vault program can cover most of the use cases that are allowed by the KMIP protocol.

A detailed Oracle Key Vault program consists of a set of Oracle Key Vault Client SDK functions that allow the client to write programs that are an actual representation of the KMIP packets being transported to the server. This requires the client to know KMIP protocol in some details.

The basic SDK program covers most of the common use cases. More complex operations or use cases can be done with a detailed Oracle Key Vault program.

The program structure is mostly the same as the basic Oracle Key Vault program structure. However, there is an additional operation handle that is used to define the KMIP operation.

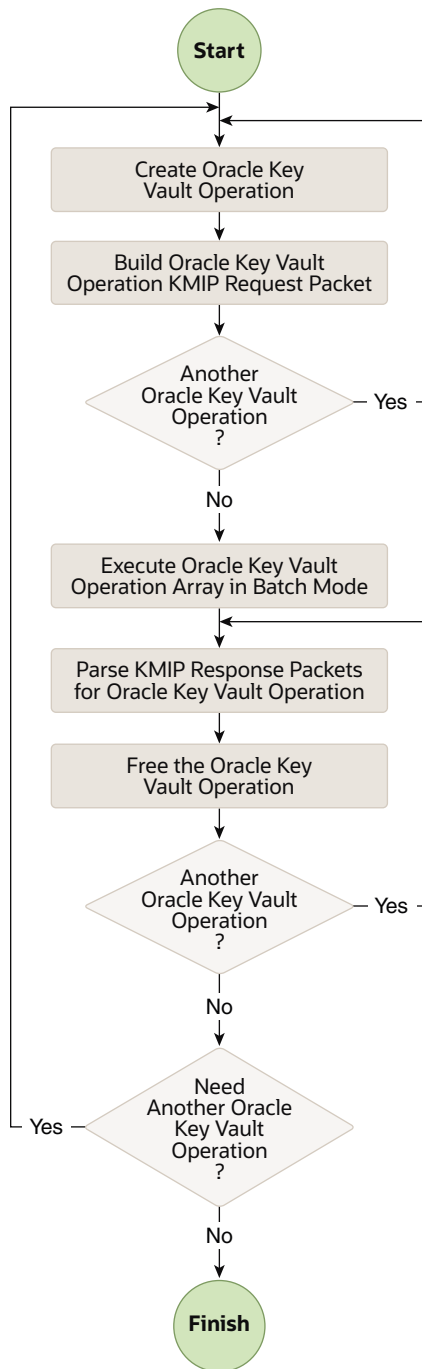
The Oracle Key Vault detailed program flow can also make use of batching the multiple KMIP operations.

A detailed Oracle Key Vault program has the following structure:

1. Create the Oracle Key Vault environment handle.
2. Optionally, configure the trace information.
3. Configure the connection information.
 - Optionally, configure the Oracle Key Vault program session.
 - Create an Oracle Key Vault operation array for multiple KMIP operations.
 - Build a KMIP request message for the Oracle Key Vault operations.
 - Execute the Oracle Key Vault operations, possibly in batch mode.
 - Unwrap the KMIP response message for the Oracle Key Vault operations.
 - Free up the Oracle Key Vault operation array.
 - Terminate the Oracle Key Vault program session if you had established it earlier.
4. Release the Oracle Key Vault environment handle.

The detailed Oracle Key Vault program flow is same as basic program flow except for the Oracle Key Vault function execution part and is as shown in the figure below.

Figure 5-3 Detailed Oracle Key Vault Program Flowchart



Example 5-3 Advanced Oracle Key Vault Detailed Program

```

...
OKVEnv *env = okvEnvCreate(OKV_MEMORY_FUNCTIONS);

/* Allocate Operation array for two KMIP operations */
OKVOps *ops[2];
ub4 alg = CRYPTO_ALG_AES;
okvEnvSetConfig(env, (oratext *)config_file, (oratext *) connection_pwd);

```

```

okvEnvSetTrace(env, (oratext *)trace_file, OKV_TRACE_DEBUG);

/* First OKV KMIP Operation */
ops[0] = okvOpsCreate(env, OKVOpCreate);
req = okvTTLVGetRequest(env, ops[0]);
okvTTLVAddToObject(env, req, OKVDEF_TAG_OBJ_TYPE, ...);
template = okvTTLVAddToObject(env, req, OKVDEF_TAG_TEMPLATE_ATTR_ST, ..);
attr = okvTTLVAddToObject(env, template, OKVDEF_TAG_ATTR_ST, ...);
okvTTLVAddToObject(env, attr, OKVDEF_TAG_ATTR_NAME, "Cryptographic
Algorithm" ...);
okvTTLVAddToObject(env, attr, OKVDEF_TAG_ATTR_INDEX, &ind, ..);
okvTTLVAddToObject(env, attr, OKVDEF_TAG_ATTR_VALUE, &alg, ..);

... so on for crypto algorithm len and crypto mask attributes ...

/* Second OKV KMIP Operation */
ops[1] = okvOpsCreate(env, OKVOpActivate);
req = okvTTLVGetRequest(env, ops[1]);

/* Note KMIP ID for activation is implicit since detailed operations are always
batched. */

/* Execute OKV KMIP Operations in Batch mode */
okvOpsExecuteOp(env, ops, 2);

/* Parse the result of the first OKV KMIP Operation */
resp = okvTTLVGetResponse(env, ops[0]);
tagid = okvTTLVGetChild(env, resp, 1, OKVDEF_TAG_ID, 0, &ctag_id_len);
ctag_id = okvTTLVGetValue(tagid);
ctag_id[ctag_id_len] = 0;
printf("\nCreated Key %s", ctag_id);

/* Parse the result of the second OKV KMIP Operation */
resp = okvTTLVGetResponse(env, ops[1]);
tagid = okvTTLVGetChild(env, resp, 0, OKVDEF_TAG_ID, 0, &atag_id_len);
atag_id = okvTTLVGetValue(tagid);
atag_id[atag_id_len] = 0;
printf("\nActivated Key %s", atag_id);

/* Free the two operations */
okvOpsFree(env, &ops[0]);
okvOpsFree(env, &ops[1]);
okvEnvFree(&env);
...

```

5.3 Oracle Key Vault Program Environment

The Oracle Key Vault program environment is the region or block in the endpoint where the Oracle Key Vault functions are executed.

The Oracle Key Vault program environment begins with the initialization of the Oracle Key Vault environment handle and ends with the freeing of this handle. The initialization and freeing of the Oracle Key Vault environment handle can be done in different endpoint program functions so the Oracle Key Vault environment exists across functions in the endpoint program.

The Oracle Key Vault program environment is limited to a process or thread only and, as such, the Oracle Key Vault environment will exist within a process or a thread only. The Oracle Key Vault environment handle must not be used in the threads or

processes forked after the Oracle Key Vault environment is initialized. The forked processes or threads can have their own Oracle Key Vault environments.

5.4 Oracle Key Vault Program Connection

The Oracle Key Vault program connection has two types of connections: explicit and intrinsic.

- **Explicit connections:** You must configure the connection that connects to the Oracle Key Vault server explicitly, perform a few Oracle Key Vault client SDK operations, and then disconnect from the Oracle Key Vault server.
- **Intrinsic connections:** You must configure the connection and then execute the Oracle Key Vault client SDK function. This function sets up the connections and then ends when the task is complete.

The difference between the two approaches is the number of times the connection between endpoint SDK Program and Oracle Key Vault server has to be setup. The connections are SSL connections and could prove to be costly for performance intensive applications.

There is a two-minute time-out on the Oracle Key Vault server connections if there is no activity on the connection. For explicit connections, the connection is reset automatically if it is disconnected.

5.5 Oracle Key Vault Program Session

The Oracle Key Vault program session are of two types: Oracle Key Vault session and Oracle Key Vault call session.

An Oracle Key Vault program session exists from the time the endpoint program explicitly connects to the Oracle Key Vault server, to the time it explicitly disconnects from the Oracle Key Vault server. This is described as the first case in the previous section (explicit connections). There can be multiple Oracle Key Vault function calls during an Oracle Key Vault session, that is, between the time the connection is setup and is disconnected.

The second case described in the previous section (intrinsic connections) sets up the connection only for the duration of one Oracle Key Vault client SDK function. This temporary internal session is called Oracle Key Vault program call session or Oracle Key Vault call session.

In general, if there are a number of KMIP operations to be executed together in time and program space, then it is better to set up the Oracle Key Vault session. If there are just one or two operations to be executed, and if they are batched, then there is no need to set up the Oracle Key Vault session explicitly.

Oracle Key Vault program sessions exist within an Oracle Key Vault program environment. More than one Oracle Key Vault session can exist within an Oracle Key Vault program environment in a serial fashion. One Oracle Key Vault session cannot be embedded in another Oracle Key Vault session. Since the scope of an Oracle Key Vault environment is a single process or a thread, the Oracle Key Vault session is also limited to a process or thread.

An Oracle Key Vault session by definition encompasses both batched and non-batched Oracle Key Vault functions. While batching saves the round trips to the Oracle Key Vault server, an Oracle Key Vault session reduces the need to repeatedly set up a connection with the Oracle Key Vault server.

Part II

Oracle Key Vault Client C SDK API Reference

Part II provides information about the Oracle Key Vault C SDK APIs.

- [Oracle Key Vault Datatypes and Structures](#)
This section describes the Oracle Key Vault datatypes and structures.
- [Oracle Key Vault Client SDK Management APIs](#)
The Oracle Key Vault client SDK management APIs control the Oracle Key Vault Interface program environment.
- [Oracle Key Vault Client SDK Connection Management APIs](#)
This section describes the interfaces for Oracle Key Vault connection management.
- [Oracle Key Vault Client SDK Memory Management APIs](#)
This section describes the Oracle Key Vault interfaces required to handle endpoint specified memory management.
- [Oracle Key Vault Client SDK Error Handling APIs](#)
This section describes the interfaces for Oracle Key Vault error management.
- [Oracle Key Vault Client SDK KMIP and Batch APIs](#)
The SDK KMIP APIs provide functions for creating keys, activating keys, adding attributes to keys, destroying keys, and other operations. The batch APIs enable you to perform these activities in a batch operation.
- [Oracle Key Vault Client SDK KMIP Attributes and Custom Attributes APIs](#)
This section describes the interfaces that help create and interpret both KMIP attributes and KMIP custom attributes.
- [Oracle Key Vault Client SDK Extension Operation Management APIs](#)
Oracle Key Vault client SDK provides operations used to execute custom KMIP requests.
- [Oracle Key Vault Client SDK TTLV Object APIs](#)
The SDK `TTLV` object APIs enable you to perform activities such as getting the child of an `OKVTTLV` object.
- [Oracle Key Vault Client SDK Utility APIs](#)
You can use the Oracle Key Vault client SDK utility APIs with other Oracle Key Vault functions to simplify common operations.

6

Oracle Key Vault Datatypes and Structures

This section describes the Oracle Key Vault datatypes and structures.

- [Oracle Key Vault Datatypes](#)
This section describes the datatypes provided with the Oracle Key Vault SDK.
- [Oracle Key Vault Structures and Enumerations](#)
This section describes the structures and enumerations provided with the Oracle Key Vault SDK.

6.1 Oracle Key Vault Datatypes

This section describes the datatypes provided with the Oracle Key Vault SDK.

Oracle Key Vault client SDK defines a set of C datatypes that are used throughout the Oracle Key Vault client SDK. These definitions are available to the endpoint program upon inclusion of `okvcsdk.h`. The following table lists the datatypes and their description.

Table 6-1 Oracle Key Vault Datatypes

Datatype	Description
<code>ub1</code>	Unsigned byte of at least 1 byte.
<code>sb1</code>	Signed byte of at least 1 byte.
<code>ub2</code>	Unsigned byte of at least 2 bytes.
<code>sb2</code>	Signed byte of at least 2 bytes.
<code>ub4</code>	Unsigned byte of at least 4 bytes.
<code>sb4</code>	Signed byte of at least 4 bytes.
<code>ub8</code>	Unsigned byte of at least 8 bytes.
<code>sb8</code>	Signed byte of at least 8 bytes.
<code>OKVErrNo</code>	Same as <code>ub4</code> .
<code>OKVTag</code>	Same as <code>ub4</code> .
<code>OKVType</code>	Same as <code>ub1</code> .
<code>oratext</code>	Character byte of size 1 byte.

6.2 Oracle Key Vault Structures and Enumerations

This section describes the structures and enumerations provided with the Oracle Key Vault SDK.

- [OKVAttr](#)
`OKVAttr` has a collection of all the KMIP attributes, single or multi-instance attributes, supported by the KMIP specification.

- **OKVAttrNo**
OKVAttrNo defines the KMIP attributes with OKVATTRMAX as the count of the KMIP attributes.
- **OKVCryptoContext**
OKVCryptoContext holds the required parameters for cryptographic operations.
- **OKVDecryptResponse**
OKVDecryptResponse contains the decrypt operation response details.
- **OKVEncryptResponse**
OKVEncryptResponse contains the encrypt operation response details.
- **OKVEnv**
OKVEnv is the Oracle Key Vault environment handle that controls the endpoint SDK program behavior.
- **OKVErr**
OKVErr is the Oracle Key Vault error management handle that captures errors in an Oracle Key Vault operation.
- **OKVMemoryCtx**
OKVMemoryCtx is the Oracle Key Vault memory management context that holds the memory context and pointers to endpoint defined memory functions.
- **OKVObjNo**
OKVObjNo defines the KMIP managed object types with OKVOBJMAX as the maximum possible count of the KMIP managed object types.
- **OKVOps**
OKVOps is the Oracle Key Vault operation handle.
- **OKVOpsNo**
OKVOpsNo defines the KMIP Operations with OKVOPSMAX as the count of the maximum possible KMIP operations.
- **OKVServerInformation**
OKVServerInformation is the Oracle Key Vault specific information that is returned by the Oracle Key Vault server for the Oracle Key Vault query operation.
- **OKVTTLV**
OKVTTLV defines the Oracle Key Vault structure for a TTLV object.
- **OKVSignResponse**
OKVSignResponse contains the sign operation response details.
- **OKVSignVerifyResponse**
OKVSignVerifyResponse contains the signature verify operation response details.

6.2.1 OKVAttr

OKVAttr has a collection of all the KMIP attributes, single or multi-instance attributes, supported by the KMIP specification.

Multi-instance attributes also have a field for the count of the multi-instance attribute. Attributes that have text string and byte string have a length associated with the value pointers.

Definition

```

/* Client SDK collection of attribtues */
struct OKVAttr
{
    struct
    {
        oratext *id;
        ub4      idl;
    } unique_identifier;
    ub4      name_count;
    struct
    {
        oratext *name;
        ub4      name1;
        ub4      type;
    } name[OKV_MAX_ATTR_INSTANCES];
    OKVObjNo object_type;
    ub4 crypto_algorithm;
    ub4 crypto_length;
    ub4 crypto_parameters_count;
    struct
    {
        ub4 block_cipher_mode;
        ub4 padding_method;
        ub4 hashing_algorithm;
        ub4 key_role_type;
    } crypto_parameters[OKV_MAX_ATTR_INSTANCES];
    ub4 cert_type;
    ub4 cert_length;
    struct
    {
        ub1 *issuer;
        ub4 issuerl;
        ub1 *serial_number;
        ub4 serial_numberl;
    } X509_cert_identifier;
    struct
    {
        ub1 *distinguished_name;
        ub4 distinguished_name1;
        ub4 alternative_name_count;
        struct
        {
            ub1 *name;
            ub4 name1;
        } alternative_name[OKV_MAX_ALTERNATE_NAMES];
    } X509_cert_subject;
    struct
    {
        ub1 *distinguished_name;
        ub4 distinguished_name1;
        ub4 alternative_name_count;
        struct
        {
            ub1 *name;
            ub4 name1;
        } alternative_name[OKV_MAX_ALTERNATE_NAMES];
    } X509_cert_issuer;
    ub4 digital_signature_algorithm_count;

```

```

ub4 digital_signature_algorithm[OKV_MAX_ATTR_INSTANCES];
ub4 digest_count;
struct
{
    ub4 hashing_algorithm;
    ub4 key_format_type;
    ub1 *digest_value;
    ub4 digest_value1;
} digest[OKV_MAX_ATTR_INSTANCES];
ub4 crypto_usage_mask;
ub4 lease_time;
struct
{
    ub8 total;
    ub8 count;
    ub4 unit;
} usage_limits;
ub4 state;
ub8 initial_date;
ub8 activation_date;
ub8 process_start_date;
ub8 protect_stop_date;
ub8 deactivation_date;
ub8 destroy_date;
ub8 compromise_occurrence_date;
ub8 compromise_date;
struct
{
    ub4 reason_code;
    oratext *message;
    ub4 message1;
} revocation_reason;
ub8 archive_date;
ub8 fresh;
ub4 link_count;
struct
{
    ub4 type;
    oratext *linked_object_identifier;
    ub4 linked_object_identifier1;
} link[OKV_MAX_ATTR_INSTANCES];
ub8 last_change_date;
ub8 extractable;
ub8 never_extractable;

/* Un-Supported Attributes * /

    Crypto Domain Parameters
    Cert_Identifier
    Cert_Subject
    Cert_Issuer
    Object_Group[]
    Contact_Information
    Application_Specific_Information[]
    Operation_Policy_Name
*/
};
typedef struct OKVAttr OKVAttr;

```

6.2.2 OKVAttrNo

OKVAttrNo defines the KMIP attributes with OKVATTRMAX as the count of the KMIP attributes.

Definition

```
/* KMIP Attributes */
typedef enum
{
    OKVAttrNone = 0,
    OKVAttrUniqueId,
    OKVAttrName,
    OKVAttrObjType,
    OKVAttrCryptoAlg,
    OKVAttrCryptoLen,
    OKVAttrCryptoParams,
    OKVAttrCryptoDomainParams,
    OKVAttrCertType,
    OKVAttrCertLength,
    OKVAttrX509CertId,
    OKVAttrX509CertSubject,
    OKVAttrX509CertIssuer,
    OKVAttrCertId,
    OKVAttrCertSubject,
    OKVAttrCertIssuer,
    OKVAttrDigitalSignAlgo,
    OKVAttrDigest,
    OKVAttrOpsPolicyName,
    OKVAttrCryptoUsageMask,
    OKVAttrLeaseTime,
    OKVAttrUsageLimits,
    OKVAttrState,
    OKVAttrInitialDate,
    OKVAttrActivationDate,
    OKVAttrProcessStartDate,
    OKVAttrProtectStopDate,
    OKVAttrDeactivationDate,
    OKVAttrDestroyDate,
    OKVAttrCompromiseOccurrenceDate,
    OKVAttrCompromiseDate,
    OKVAttrRevocationReason,
    OKVAttrArchiveDate,
    OKVAttrObjectGroup,
    OKVAttrFresh,
    OKVAttrLink,
    OKVAttrAppSpecificInfo,
    OKVAttrContactInfo,
    OKVAttrLastChangeDate,
    OKVAttrExtractable,
    OKVAttrNeverExtractable,
    OKVAttrInvalid = 255
} OKVAttrNo;
#define OKVATTRMAX 42
```

6.2.3 OKVCryptoContext

OKVCryptoContext holds the required parameters for cryptographic operations.

Definition

```
/* Crypto Context */
struct OKVCryptoContext
{
    OKVOpsNo crypto_operation;
    ub4 block_cipher_mode;
    ub4 padding;
    ub8 random_iv;
    ub1 *iv;
    ub4 ivl;
    ub1 *auth_encryption_additional_data;
    ub4 auth_encryption_additional_data1;
    ub1 *auth_encryption_tag;
    ub4 auth_encryption_tag1;
    ub4 crypto_algo;
    ub4 hashing_algo;
    ub4 digital_sign_algo;
};
typedef struct OKVCryptoContext OKVCryptoContext;
```

Parameters

Parameter	Description
crypto_operation	Type of cryptographic operation.
block_cipher_mode	Block Cipher Mode value.
padding	Padding value.
random_iv	Random IV value.
iv	IV value.
ivl	IV value length.
auth_encryption_additional_data	Authenticated encryption additional data value.
auth_encryption_additional_data1	Authenticated encryption additional data value length.
auth_encryption_tag	Authenticated encryption tag value.
auth_encryption_tag1	Authenticated encryption tag value length.
crypto_algo	Cryptographic algorithm.
hashing_algo	Hashing algorithm.
digital_sign_algo	Digital signature algorithm.

6.2.4 OKVDecryptResponse

OKVDecryptResponse contains the decrypt operation response details.

Definition

```
struct OKVDecryptResponse {
    ub1 *decrypted_data;
    ub4 decrypted_data1;
};
typedef struct OKVDecryptResponse OKVDecryptResponse;
```

Parameters

Parameter	Description
decrypted_data	Decrypted data value.
decrypted_data1	Decrypted data value length.

6.2.5 OKVEncryptResponse

OKVEncryptResponse contains the encrypt operation response details.

Definition

```
struct OKVEncryptResponse {
    ub1 *encrypted_data;
    ub4 encrypted_data1;
    ub1 *iv;
    ub4 iv1;
    ub1 *auth_encryption_tag;
    ub4 auth_encryption_tag1;
};
typedef struct OKVEncryptResponse OKVEncryptResponse;
```

Parameters

Parameter	Description
encrypted_data	Encrypted data value.
encrypted_data1	Encrypted data value length.
iv	IV value.
iv1	IV value length.
auth_encryption_tag	Authenticated encryption tag value.
auth_encryption_tag1	Authenticated encryption tag value length.

6.2.6 OKVEnv

OKVEnv is the Oracle Key Vault environment handle that controls the endpoint SDK program behavior.

OKVEnv also holds Service Provider Interfaces (SPI) handles used in the endpoint SDK program, the request and result OKVTTLV objects for Oracle Key Vault functions.

Definition

```

/* Oracle Key Vault Environment */
struct OKVEnv
{
    OKVConnCtx      *conn_spi;
    OKVMemoryCtx   *mem_spi;
    OKVParseCtx    *parse_spi;
    ub4             flag;
    #define OKVENV_CONN_SETUP    0x00000001
    #define OKVENV_BATCH_MODE    0x00000002
    #define OKVENV_CONN_SPI      0x00000004
    #define OKVENV_NATCONN_SPI   0x00000008
    #define OKVENV_MEM_SPI       0x00000010
    #define OKVENV_NATMEM_SPI    0x00000020
    #define OKVENV_PACK_XML     0x00000040
    OKVTTLV         *request_obj;
    OKVTTLV         *result_obj;
    OKVErr          *err;
    OKVTrcCtx       *trc_ctx;
    ub4             batch_cnt;
    OKVBatchCtx     **batch;
    ub4             batch_err_ctx_cnt;
    OKVBatchErrCtx **batch_err_ctx;
};
typedef struct OKVEnv OKVEnv;

```

Parameters

Parameter	Description
conn_spi	Stores the handle for the connection management SPI. If the endpoint program does not specify one then it stores the handle for the native connection management.
mem_spi	Stores the handle for the memory management SPI. If the endpoint program does not specify one then it stores the handle for the native memory management.
parse_spi	Stores the context for parse management. Since the serialization of OKVTTLV objects is internal to Oracle Key Vault Client SDK, parse_spi is set and unset internally only. KMIP v1.1 can have a regular TTLV packing or XML style packing. In the first version of Oracle Key Vault Client SDK, TTLV packing is supported.
flag	Controls the operational behavior of the Oracle Key Vault client SDK program. Most of the flags are self explanatory.
request_obj	For Oracle Key Vault API functions having OKVTTLV objects as arguments, the object is created beforehand. The allocated memory for this object is pointed to by request_obj.

Parameter	Description
result_obj	For Oracle Key Vault API functions that return OKVTTLV objects, the object has to be interpreted by the EndPoint program after the call is done i.e. the memory for the Oracle Key Vault API functions is cleaned up. The memory for the OKVTTLV object is not cleaned at the Oracle Key Vault function call and is pointed to by result_obj.
err	This is the error handle that captures the errors in Oracle Key Vault operation. Multiple errors can be reported for a given operation. These errors will be captured in the error stack.
trc_ctx	Stores the handle for trace management.
batch_cnt	This is the count of batch operations.
batch	This is the array of batch operations along with the place holders for results.
batch_err_ctx_cnt	This is the count of batch error context.
batch_err_ctx	Batch error context will hold the information such as Oracle Key Vault operation name and errors related to that operation if any.

6.2.7 OKVErr

OKVErr is the Oracle Key Vault error management handle that captures errors in an Oracle Key Vault operation.

Multiple errors can be reported for a given operation. These errors will be captured in the error stack.

Definition

```
/* Oracle Key Vault Error Management */
struct OKVErr
{
    #define OKVERR_CNT 100
    ub1 err_cnt;
    ub4 err_stack[OKVERR_CNT];
};
typedef struct OKVErr OKVErr;
```

Parameters

Parameter	Description
err_cnt	Count of errors in the error stack, which indicates the depth of the error stack.
err_stack	Stack of error numbers captured.

6.2.8 OKVMemoryCtx

OKVMemoryCtx is the Oracle Key Vault memory management context that holds the memory context and pointers to endpoint defined memory functions.

It also holds pointers to the `malloc`, `realloc`, and `free` functions supplied by the endpoint program.

Definition

```
/* Memory Function Context */
struct OKVMemoryCtx
{
    void      *ctx;                /* Context */
    void *    (*okvMalloc)(void *ctx, size_t size); /* Malloc */
    void *    (*okvRealloc)(void *ctx, void **ptr, size_t size); /* Realloc */
    void      (*okvFree)(void *ctx, void **ptr);    /* Free */
};
typedef struct OKVMemoryCtx OKVMemoryCtx;
```

Parameters

Parameter	Description
<code>ctx</code>	The endpoint program defined memory context.
<code>okvMalloc</code>	Pointer to the endpoint program defined function to allocate memory. This function should clear the memory allocated, that is, set all allocated bytes to zero.
<code>okvRealloc</code>	Pointer to the endpoint program defined function to re-allocate the size of the previously allocated and possibly populated memory.
<code>okvFree</code>	Pointer to the endpoint program defined function to free the memory allocated using <code>okvMalloc</code> or <code>okvRealloc</code> . The pointer should be set to <code>NULL</code> after freeing it.

Related Topics

- [okvFree](#)
`okvFree` is a pointer to the endpoint program defined function to free the memory allocated using `okvMalloc` or `okvRealloc`.
- [okvMalloc](#)
`okvMalloc` is a pointer to the endpoint program defined function that should allocate memory.
- [okvRealloc](#)
`okvRealloc` is a pointer to the endpoint program defined function that should reallocate memory.

6.2.9 OKVObjNo

OKVObjNo defines the KMIP managed object types with OKVOBJMAX as the maximum possible count of the KMIP managed object types.

Definition

```
/* OKV KMIP Managed Objects */
typedef enum
{
    OKVObjNone = 0,          /* No Object Type */
    OKVObjCert = 1,         /* Certificate */
    OKVObjSymmetric,        /* Symmetric Key */
    OKVObjPublic,           /* Public Key */
    OKVObjPrivate,          /* Private Key */
    OKVObjTemplate = 6,     /* Template */
    OKVObjSecret,           /* Secret Data */
    OKVObjOpaque            /* Opaque Object */
} OKVObjNo;
#define OKVOBJMAX          8
```

6.2.10 OKVOps

OKVOps is the Oracle Key Vault operation handle.

Definition

```
/* Oracle Key Vault KMIP Operation */
struct OKVOps
{
    OKVOpsNo    ops;
    OKVErr      err;
    OKVTTLV     *item;
    OKVTTLV     *req;
    ub4         res;
    OKVTTLV     *resp;
    OKVErr      *errb;
};
typedef struct OKVOps OKVOps;
```

OKVOps captures the request and response OKVTTLV structures for a given Oracle Key Vault KMIP operation along with the result (pass or fail) of the operation.

Parameters

Parameter	Description
ops	KMIP operation associated with this Oracle Key Vault operation handle.
err	Error handle for batch operations.
item	Batch item of this KMIP operation.
req	KMIP Request OKVTTLV object.
res	Result of the KMIP operation.
resp	KMIP Response OKVTTLV object.

Parameter	Description
errb	Error handle pointer for batch operations.

6.2.11 OKVOpsNo

OKVOpsNo defines the KMIP Operations with OKVOPSMAX as the count of the maximum possible KMIP operations.

Definition

```

/* KMIP Operations */
typedef enum
{
    OKVOpNone = 0, /* Wrong Operation */
    OKVOpCreate = 1, /* Create */
    OKVOpCreateKeyPair,
    OKVOpRegister, /* Register */
    OKVOpRekey, /* Rekey */
    OKVOpDeriveKey,
    OKVOpCertify,
    OKVOpRecertify,
    OKVOpLocate, /* Locate */
    OKVOpCheck, /* Check */
    OKVOpGet, /* Get */
    OKVOpGetAttributes, /* Get Attributes */
    OKVOpGetAttributeList, /* Get Attribute List */
    OKVOpAddAttribute, /* Add Attribute */
    OKVOpModifyAttribute, /* Modify Attribute */
    OKVOpDeleteAttribute, /* Delete Attribute */
    OKVOpObtainLease,
    OKVOpGetUsageAllocation,
    OKVOpActivate, /* Activate */
    OKVOpRevoke, /* Revoke */
    OKVOpDestroy, /* Destroy */
    OKVOpArchive,
    OKVOpRecover,
    OKVOpValidate,
    OKVOpQuery, /* Query */
    OKVOpCancel,
    OKVOpPoll,
    OKVOpNotify,
    OKVOpPut,
    OKVOpRekeyKeyPair,
    OKVOpDiscoverVersions, /* Discover Versions */
    OKVOpEncrypt, /* Encrypt */
    OKVOpDecrypt, /* Decrypt */
    OKVOpSign, /* Sign */
    OKVOpSignVerify, /* Verify */
} OKVOpsNo;
#define OKVOPSMAX 35

```

6.2.12 OKVServerInformation

OKVServerInformation is the Oracle Key Vault specific information that is returned by the Oracle Key Vault server for the Oracle Key Vault query operation.

Definition

```
struct OKVServerInformation
{
    oratext server_name[30];
    oratext server_version[30];
};
typedef struct OKVServerInformation OKVServerInformation;
```

Parameters

Parameter	Description
server_name	Should be ORACLE KEYVAULT SERVER if the endpoint program is communicating with the Oracle Key Vault server.
server_version	The version of the Oracle Key Vault server the endpoint program is communicating with.

6.2.13 OKVTTLV

OKVTTLV defines the Oracle Key Vault structure for a TTLV object.

Definition

```
/* Oracle Key Vault KMIP TTLV Structure */
struct OKVTTLV
{
    OKVTag    tag;
    OKVType   typ;
    ub4       len;
    ub1       *val;
    ub4       ttlv_array_cnt;
    OKVTTLV **ttl_array;
};
typedef struct OKVTTLV OKVTTLV;
```

Parameters

Parameter	Description
tag	The tag value of the TTLV object.
typ	The type value of the TTLV object.
len	The length of the value of the TTLV object.
val	The value of the TTLV object.
ttl_array_cnt	The count of the child TTLV objects for this TTLV object.
ttl_array	An array of the child TTLV objects for this TTLV object.

6.2.14 OKVSignResponse

OKVSignResponse contains the sign operation response details.

Syntax

```
struct OKVSignResponse {
    ub1 *signature_data;
    ub4 signature_data1;
};
```

Parameters

Table 6-2 Parameters

Parameter	Description
signature_data	Signature data value.
signature_data1	Signature data value length.

6.2.15 OKVSignVerifyResponse

OKVSignVerifyResponse contains the signature verify operation response details.

Syntax

```
struct OKVSignVerifyResponse {
    ub1 *recovered_data;
    ub4 recovered_data1;
    ub4 validity;
};
```

Parameters

Table 6-3 Parameters

Parameter	Description
recovered_data	Recovered data value.
recovered_data1	Recovered data value length.
validity	Validity indicator, which may take the value of OKVDEF_VALIDITY_VALID, OKVDEF_VALIDITY_INVALID, or OKVDEF_VALIDITY_UNKNOWN.

7

Oracle Key Vault Client SDK Management APIs

The Oracle Key Vault client SDK management APIs control the Oracle Key Vault Interface program environment.

- [okvEnvCreate](#)
`okvEnvCreate` creates the Oracle Key Vault environment handle and the Oracle Key Vault SDK program begins with a successful call to this function.
- [okvEnvFree](#)
`okvEnvFree` frees the Oracle Key Vault environment handle, which marks the end of the Oracle Key Vault environment.
- [okvEnvFreeResultObj](#)
`okvEnvFreeResultObj` frees the OKVTTLV result descriptor that was returned by the Oracle Key Vault functions.
- [okvEnvGetOpRequestObj](#)
`okvEnvGetOpRequestObj` gets the root (top-level parent) of the OKVTTLV descriptor for Oracle Key Vault KMIP functions.
- [okvEnvSetConfig](#)
`okvEnvSetConfig` sets up the Oracle Key Vault connection configuration context.
- [okvEnvSetTrace](#)
`okvEnvSetTrace` sets up the Oracle Key Vault trace configuration context.

7.1 okvEnvCreate

`okvEnvCreate` creates the Oracle Key Vault environment handle and the Oracle Key Vault SDK program begins with a successful call to this function.

Category

Management API

Purpose

`okvEnvCreate` is used to create the Oracle Key Vault environment handle which in turn holds error handle, tracing context and the various Service Provider Interface handles required by the Endpoint program. All of the Oracle Key Vault functions are done within the purview of this handle. The Oracle Key Vault environment begins with a successful call to this function.

Syntax

```
OKVEnv *okvEnvCreate(OKVMemoryCtx *memctx);
```

Parameters

Parameter	IN/OUT	Description
memctx	IN	Oracle Key Vault memory management context.

Return Values

Return Value	Description
OKVEnv*	Oracle Key Vault environment handle. Success: A valid pointer to the Oracle Key Vault environment handle is returned. Failure: A NULL pointer is returned.

Comments

Endpoints using the Oracle Key Vault memory management should pass in `OKV_MEMORY_FUNCTIONS` to `okvEnvCreate`.

The Oracle Key Vault client SDK provides the client with an option to define their own memory management context and memory management functions.

Suppose the client has defined `clientMalloc()`, `clientRealloc()`, `clientFree()`, and `clientCtxP` for memory management. The client can make use of these functions by initializing the Oracle Key Vault environment handle with the Oracle Key Vault memory context structure.

```
...
OKVMemoryCtx clientMemory;
clientMemory.ctx = clientCtxP;
clientMemory.okvMalloc = &clientMalloc;
clientMemory.okvRealloc = &clientRealloc;
clientMemory.okvFree = &clientFree;
okvEnvCreate(&clientMemory);
...
```

Example

```
OKVEnv *env = (OKVEnv *) NULL;

/* Setup the Oracle Key Vault Environment handle */
printf("\nSetting up Oracle Key Vault Environment handle\n");
env = okvEnvCreate(OKV_MEMORY_FUNCTIONS);
if (!env)
{
    printf("\tCould not setup the Oracle Key Vault Environment handle\n");
    return 1;
}
else
{
    printf("\tSuccessfully setup Oracle Key Vault Environment handle\n\n");
}
```

Related Topics

- [okvEnvFree](#)
okvEnvFree frees the Oracle Key Vault environment handle, which marks the end of the Oracle Key Vault environment.
- [okvEnvFreeResultObj](#)
okvEnvFreeResultObj frees the OKVTTLV result descriptor that was returned by the Oracle Key Vault functions.
- [okvEnvGetOpRequestObj](#)
okvEnvGetOpRequestObj gets the root (top-level parent) of the OKVTTLV descriptor for Oracle Key Vault KMIP functions.
- [okvEnvSetConfig](#)
okvEnvSetConfig sets up the Oracle Key Vault connection configuration context.
- [okvEnvSetTrace](#)
okvEnvSetTrace sets up the Oracle Key Vault trace configuration context.

7.2 okvEnvFree

okvEnvFree frees the Oracle Key Vault environment handle, which marks the end of the Oracle Key Vault environment.

Category

Management API

Purpose

okvEnvFree is used to free the Oracle Key Vault environment handle. It marks the end of Oracle Key Vault environment.

Syntax

```
void okvEnvFree(OKVEnv **env);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault Interface environment handle.

Return Values

No values returned.

Comments

None.

Example

```
OKVEnv *env = (OKVEnv *) NULL;

/* Setup the Oracle Key Vault Environment handle */
printf("\nSetting up Oracle Key Vault Environment handle\n");
```

```
env = okvEnvCreate(OKV_MEMORY_FUNCTIONS);

if (!env)
{
    printf("\tCould not setup the Oracle Key Vault Environment handle\n");
    return 1;
}
else
{
    printf("\tSuccessfully setup Oracle Key Vault Environment handle\n\n");
}
...
/* Do some KMIP operations */
...
/* Free the env handle */
printf("Releasing the Environment handle\n");
okvEnvFree(&env);
return 0;
```

Related Topics

- [okvEnvCreate](#)
okvEnvCreate creates the Oracle Key Vault environment handle and the Oracle Key Vault SDK program begins with a successful call to this function.
- [okvEnvFreeResultObj](#)
okvEnvFreeResultObj frees the OKVTTLV result descriptor that was returned by the Oracle Key Vault functions.
- [okvEnvGetOpRequestObj](#)
okvEnvGetOpRequestObj gets the root (top-level parent) of the OKVTTLV descriptor for Oracle Key Vault KMIP functions.
- [okvEnvSetConfig](#)
okvEnvSetConfig sets up the Oracle Key Vault connection configuration context.
- [okvEnvSetTrace](#)
okvEnvSetTrace sets up the Oracle Key Vault trace configuration context.

7.3 okvEnvFreeResultObj

okvEnvFreeResultObj frees the OKVTTLV result descriptor that was returned by the Oracle Key Vault functions.

Category

Management API

Purpose

okvEnvFreeResultObj will free the OKVTTLV result descriptor that was returned by the Oracle Key Vault functions.

Oracle Key Vault KMIP functions at times return OKVTTLV descriptors that have to be explored further either using Oracle Key Vault helper or Oracle Key Vault KMIP Extension functions. The OKVTTLV parent for the result descriptor is stored in Oracle Key Vault environment handle and is not freed upon completion of the Oracle Key Vault function.

After the Oracle Key Vault function result descriptor has been interpreted, it can be freed using `okvEnvFreeResultObj`.

Syntax

```
void okvEnvFreeResultObj(OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault Interface environment handle.

Return Values

No values returned.

Comments

The subsequent Oracle Key Vault functions calls will free the result descriptor of the previous Oracle Key Vault function.

Example

```
/* Setup the Oracle Key Vault Environment handle 'env' */  
...  
/* Do some KMIP operations */  
...  
okvEnvFreeResultObj(env);
```

Related Topics

- [okvEnvCreate](#)
`okvEnvCreate` creates the Oracle Key Vault environment handle and the Oracle Key Vault SDK program begins with a successful call to this function.
- [okvEnvFree](#)
`okvEnvFree` frees the Oracle Key Vault environment handle, which marks the end of the Oracle Key Vault environment.
- [okvEnvGetOpRequestObj](#)
`okvEnvGetOpRequestObj` gets the root (top-level parent) of the OKVTTLV descriptor for Oracle Key Vault KMIP functions.
- [okvEnvSetConfig](#)
`okvEnvSetConfig` sets up the Oracle Key Vault connection configuration context.
- [okvEnvSetTrace](#)
`okvEnvSetTrace` sets up the Oracle Key Vault trace configuration context.

7.4 okvEnvGetOpRequestObj

`okvEnvGetOpRequestObj` gets the root (top-level parent) of the OKVTTLV descriptor for Oracle Key Vault KMIP functions.

Category

Management API

Purpose

Some KMIP functions will use an OKVTTLV descriptor argument to build the TTLV Request. `okvEnvGetOpRequestObj` is used to get the root (top-level parent) of the OKVTTLV descriptor for Oracle Key Vault KMIP functions.

Oracle Key Vault functions like `okvAttrAddUniqueID` will create an OKVTTLV attribute descriptor but these functions need a parent OKVTTLV descriptor.

`okvEnvGetOpRequestObj()` returns the parent OKVTTLV descriptor for such Oracle Key Vault functions.

Syntax

```
OKVTTLV *okvEnvGetOpRequestObj (OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
OKVTTLV *	OKVTTLV object. Success: A valid pointer to the OKVTTLV descriptor is returned. Failure: A NULL pointer is returned.

Comments

None.

Example

```
OKVTTLV *request = (OKVTTLV *)NULL;
...
/* Setup the Oracle Key Vault Environment handle 'env' */
...
request = okvEnvGetOpRequestObj(env);
```

Related Topics

- [okvEnvCreate](#)
`okvEnvCreate` creates the Oracle Key Vault environment handle and the Oracle Key Vault SDK program begins with a successful call to this function.
- [okvEnvFree](#)
`okvEnvFree` frees the Oracle Key Vault environment handle, which marks the end of the Oracle Key Vault environment.
- [okvEnvFreeResultObj](#)
`okvEnvFreeResultObj` frees the OKVTTLV result descriptor that was returned by the Oracle Key Vault functions.

- [okvEnvSetConfig](#)
okvEnvSetConfig sets up the Oracle Key Vault connection configuration context.
- [okvEnvSetTrace](#)
okvEnvSetTrace sets up the Oracle Key Vault trace configuration context.

7.5 okvEnvSetConfig

okvEnvSetConfig sets up the Oracle Key Vault connection configuration context.

Category

Management API

Purpose

okvEnvSetConfig is used to specify the password for the SSL connection wallet. The SSL connection wallet will be created at the time of enrollment. The password specified at the time of endpoint enrollment is the one used with this function. If no password was specified at the time of enrollment, NULL should be used as the password.

okvEnvSetConfig will also specify the configuration file that will be used to set up the connection configuration for holding details like the server IP address, server port number, and other information which will be needed during establishing connection with the Oracle Key Vault server.

Syntax

```
OKVErrNo okvEnvSetConfig(OKVEnv *env, oratext *conn_config_file,
                        oratext *conn_pwd);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
conn_config_file	IN	Oracle Key Vault connection configuration file.
conn_pwd	IN	Password of the SSL connection wallet.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The connection configuration file is the okvclient.ora file, which is created at the time of Oracle Key Vault endpoint enrollment.

If you do not specify the full path to the connection configuration file, then the API tries to look for configuration file under `$OKV_HOME/conf`. Make sure to set up the `$OKV_HOME` to the directory where the endpoint software was installed.

Example

```
oratext *pwd = (oratext *)NULL;
...
/* Setup the Oracle Key Vault Environment handle 'env' */
...
printf("Setting up Oracle Key Vault connection configuration\n");
okvEnvSetConfig(env, (oratext *)NULL, (oratext *)pwd);
```

Related Topics

- [okvEnvCreate](#)
`okvEnvCreate` creates the Oracle Key Vault environment handle and the Oracle Key Vault SDK program begins with a successful call to this function.
- [okvEnvFree](#)
`okvEnvFree` frees the Oracle Key Vault environment handle, which marks the end of the Oracle Key Vault environment.
- [okvEnvFreeResultObj](#)
`okvEnvFreeResultObj` frees the OKVTTLV result descriptor that was returned by the Oracle Key Vault functions.
- [okvEnvGetOpRequestObj](#)
`okvEnvGetOpRequestObj` gets the root (top-level parent) of the OKVTTLV descriptor for Oracle Key Vault KMIP functions.
- [okvEnvSetTrace](#)
`okvEnvSetTrace` sets up the Oracle Key Vault trace configuration context.

7.6 okvEnvSetTrace

`okvEnvSetTrace` sets up the Oracle Key Vault trace configuration context.

Category

Management API

Purpose

`okvEnvSetTrace` is used to specify the location of the trace file and also the trace level. The trace file will record the internal traces generated by the endpoint SDK program and can be useful for diagnostics and debugging. The level of tracing determines how fine-grained or coarse-grained the tracing should be. In ascending order, debug levels take the following values:

- `OKV_TRACE_OFF` - No tracing
- `OKV_TRACE_FATAL` - Fatal level only tracing
- `OKV_TRACE_ERROR` - Error tracing
- `OKV_TRACE_WARN` - Warning tracing
- `OKV_TRACE_INFO` - Informational tracing
- `OKV_TRACE_DEBUG` - Debug tracing

- `OKV_TRACE_ALL` - All tracing

Syntax

```
OKVErrNo okvEnvSetTrace(OKVEnv *env, oratext *trace_file, ub1 debug_level);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>trace_file</code>	IN	Location of client SDK trace file.
<code>debug_level</code>	IN	Level of tracing.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
oratext *trace_dir = (oratext *)NULL;
...
/* Setup the Oracle Key Vault Environment handle 'env' */
...
trace_dir = (oratext *)"/tmp";
printf("Setting up Tracing\n");
okvEnvSetTrace(env, (oratext *)trace_dir, OKV_TRACE_INFO);
```

Related Topics

- [okvEnvCreate](#)
`okvEnvCreate` creates the Oracle Key Vault environment handle and the Oracle Key Vault SDK program begins with a successful call to this function.
- [okvEnvFree](#)
`okvEnvFree` frees the Oracle Key Vault environment handle, which marks the end of the Oracle Key Vault environment.
- [okvEnvFreeResultObj](#)
`okvEnvFreeResultObj` frees the OKVTTLV result descriptor that was returned by the Oracle Key Vault functions.
- [okvEnvGetOpRequestObj](#)
`okvEnvGetOpRequestObj` gets the root (top-level parent) of the OKVTTLV descriptor for Oracle Key Vault KMIP functions.
- [okvEnvSetConfig](#)
`okvEnvSetConfig` sets up the Oracle Key Vault connection configuration context.

8

Oracle Key Vault Client SDK Connection Management APIs

This section describes the interfaces for Oracle Key Vault connection management.

- [okvConnect](#)
`okvConnect` begins the Oracle Key Vault interface session and creates a connection to the Oracle Key Vault server.
- [okvConnSendRecvBytes](#)
`okvConnSendRecvBytes` sends a KMIP request message to the Oracle Key Vault server and retrieves the KMIP response message sent back from the Oracle Key Vault server.
- [okvConnSet](#)
`okvConnSet` can be used to set up the user client connection provider which can be used to establish connection to the Oracle Key Vault server.
- [okvConnUnSet](#)
`okvConnUnSet` is used to free the client connection provider.
- [okvDisconnect](#)
`okvDisconnect` ends the Oracle Key Vault interface session and disconnects the Secure Sockets Layer (SSL) connection between the endpoint and the Oracle Key Vault server.

8.1 okvConnect

`okvConnect` begins the Oracle Key Vault interface session and creates a connection to the Oracle Key Vault server.

Category

Connection management API

Purpose

`okvConnect` is used to begin the Oracle Key Vault session and create a connection to the Oracle Key Vault Server. Subsequent Oracle Key Vault functions will use this connection for communicating with the Oracle Key Vault Server.

Syntax

```
OKVErrNo okvConnect (OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
OKVErrNo err_no;
...
/* Setup the Oracle Key Vault Environment handle 'env' */
...
printf("Setting up Oracle Key Vault session\n");
err_no = okvConnect(env);

if (err_no)
{
    printf("Could not setup the Oracle Key Vault session\n");
    return 1;
}
else
{
    printf("Successfully setup Oracle Key Vault Session\n");
}
```

Related Topics

- [okvConnSendRecvBytes](#)
`okvConnSendRecvBytes` sends a KMIP request message to the Oracle Key Vault server and retrieves the KMIP response message sent back from the Oracle Key Vault server.
- [okvConnSet](#)
`okvConnSet` can be used to set up the user client connection provider which can be used to establish connection to the Oracle Key Vault server.
- [okvConnUnSet](#)
`okvConnUnSet` is used to free the client connection provider.
- [okvDisconnect](#)
`okvDisconnect` ends the Oracle Key Vault interface session and disconnects the Secure Sockets Layer (SSL) connection between the endpoint and the Oracle Key Vault server.

8.2 okvConnSendRecvBytes

`okvConnSendRecvBytes` sends a KMIP request message to the Oracle Key Vault server and retrieves the KMIP response message sent back from the Oracle Key Vault server.

Category

Connection management API

Purpose

`okvConnSendRecvBytes` is used to send a KMIP request message to the Oracle Key Vault server and retrieve the KMIP response message sent back from the Oracle Key Vault server. The response returned by the Oracle Key Vault server cannot exceed the maximum payload supported between the Oracle Key Vault client and server.

Syntax

```
OKVErrNo okvConnSendRecvBytes (OKVEnv *env,
                                ub1 *reqmsg, ub4 reqmsgl,
                                ub1 **respmsg, ub4 *respmsgl);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>reqmsg</code>	IN	KMIP TTLV request message.
<code>reqmsgl</code>	IN	KMIP TTLV request message length.
<code>respmsg</code>	IN/OUT	KMIP TTLV response message.
<code>respmsgl</code>	IN/OUT	KMIP TTLV response message length.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The endpoint program needs to allocate space for the response message. If the response message cannot fit in the allocated space the function will return an error.

Example

```
OKVErrNo err_no;
...
/* Setup the Oracle Key Vault Environment handle 'env' */
```



```
...
err_no = okvConnSendRecvBytes(env, (ub1 *)NULL, (ub4)0, (ub1 **)NULL, (ub4 *)0);

if (err_no)
{
    printf("Error while executing okvConnSendRecvBytes\n");
    return 1;
}
else
{
    printf("Successfully executed okvConnSendRecvBytes\n");
}
```

Related Topics

- [okvConnect](#)
okvConnect begins the Oracle Key Vault interface session and creates a connection to the Oracle Key Vault server.
- [okvConnSet](#)
okvConnSet can be used to set up the user client connection provider which can be used to establish connection to the Oracle Key Vault server.
- [okvConnUnSet](#)
okvConnUnSet is used to free the client connection provider.
- [okvDisconnect](#)
okvDisconnect ends the Oracle Key Vault interface session and disconnects the Secure Sockets Layer (SSL) connection between the endpoint and the Oracle Key Vault server.

8.3 okvConnSet

okvConnSet can be used to set up the user client connection provider which can be used to establish connection to the Oracle Key Vault server.

Category

Connection management API

Purpose

okvConnSet can be used to set up the user client connection provider which can be used to establish connection to the Oracle Key Vault server. Subsequent Oracle Key Vault functions will use this connection for communicating with the Oracle Key Vault server.

Syntax

```
OKVErrNo okvConnSet(OKVEnv *env,
                    void *connCtx,
                    OKVErrNo (*connectFn)(void *ctx),
                    void (*disconnectFn)(void *ctx),
                    OKVErrNo (*sendRecvFn)(void *ctx,
                                             ub1 *send_bytes,
                                             ub4 send_bytes_len,
                                             ub1 **recv_bytes,
                                             ub4 *recv_bytes_len));
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
connCtx	IN	Client defined connection context.
connectFn	IN	Client defined connect function.
disconnectFn	IN	Client defined disconnect function.
sendRecvFn	IN	Client defined send response to Oracle Key Vault server and receive response from Oracle Key Vault server function.
ctx	IN	Client defined connection context.
send_bytes	IN	KMIP TTLV request message.
send_bytes_len	IN	KMIP TTLV request message length.
recv_bytes	IN/OUT	KMIP TTLV response message.
recv_bytes_len	IN/OUT	KMIP TTLV response message length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The Oracle Key Vault Client SDK also provides native connection management support. The endpoint program does not have to do anything special if it wants the Oracle Key Vault client SDK to take care of connection management.

Example

```

/* Suppose the client has defined clientConnect(), clientDisconnect(),
   clientSendRecv() and clientNatCtxP for connection management. The
   client can make use of these functions by initializing the Oracle Key
   Vault environment handle with the Oracle Key Vault connection context
   structure */
...
OKVErrNo err_no;
err_no = okvConnSet(env, clientNatCtxP, clientConnect(...), clientDisconnect(...),
clientSendRecv(...));

if (err_no)
{

```

```

    printf("Error while setting the client defined connection functions to
environment handle\n");
}
else
{
    printf("Successfully set the environment handle with client defined
connection functions");
}

```

Related Topics

- [okvConnect](#)
okvConnect begins the Oracle Key Vault interface session and creates a connection to the Oracle Key Vault server.
- [okvConnSendRecvBytes](#)
okvConnSendRecvBytes sends a KMIP request message to the Oracle Key Vault server and retrieves the KMIP response message sent back from the Oracle Key Vault server.
- [okvConnUnSet](#)
okvConnUnSet is used to free the client connection provider.
- [okvDisconnect](#)
okvDisconnect ends the Oracle Key Vault interface session and disconnects the Secure Sockets Layer (SSL) connection between the endpoint and the Oracle Key Vault server.

8.4 okvConnUnSet

okvConnUnSet is used to free the client connection provider.

Category

Connection management API

Purpose

okvConnUnSet is used to free the client connection provider.

Syntax

```
void okvConnUnSet (OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Return Values

No values returned.

Comments

The Oracle Key Vault client SDK also provides native connection management support. The endpoint program does not have to do anything special if it wants the Oracle Key Vault client SDK to take care of connection management.

Example

```
okvConnUnSet (env) ;
```

Related Topics

- [okvConnect](#)
`okvConnect` begins the Oracle Key Vault interface session and creates a connection to the Oracle Key Vault server.
- [okvConnSendRecvBytes](#)
`okvConnSendRecvBytes` sends a KMIP request message to the Oracle Key Vault server and retrieves the KMIP response message sent back from the Oracle Key Vault server.
- [okvConnSet](#)
`okvConnSet` can be used to set up the user client connection provider which can be used to establish connection to the Oracle Key Vault server.
- [okvDisconnect](#)
`okvDisconnect` ends the Oracle Key Vault interface session and disconnects the Secure Sockets Layer (SSL) connection between the endpoint and the Oracle Key Vault server.

8.5 okvDisconnect

`okvDisconnect` ends the Oracle Key Vault interface session and disconnects the Secure Sockets Layer (SSL) connection between the endpoint and the Oracle Key Vault server.

Category

Connection management API

Purpose

`okvDisconnect` ends the Oracle Key Vault session and will disconnect SSL connection between the endpoint program and the Oracle Key Vault server.

Syntax

```
OKVErrNo okvDisconnect (OKVEnv *env) ;
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
OKVErrNo err_no;
printf("Disconnecting Oracle Key Vault Session\n");
err_no = okvDisconnect(env);

if (err_no)
{
    printf("Could not disconnect from Oracle Key Vault session\n");
    return 1;
}
else
{
    printf("Successfully disconnected from Oracle Key Vault Session\n");
}
```

Related Topics

- [okvConnect](#)
`okvConnect` begins the Oracle Key Vault interface session and creates a connection to the Oracle Key Vault server.
- [okvConnSendRecvBytes](#)
`okvConnSendRecvBytes` sends a KMIP request message to the Oracle Key Vault server and retrieves the KMIP response message sent back from the Oracle Key Vault server.
- [okvConnSet](#)
`okvConnSet` can be used to set up the user client connection provider which can be used to establish connection to the Oracle Key Vault server.
- [okvConnUnSet](#)
`okvConnUnSet` is used to free the client connection provider.

9

Oracle Key Vault Client SDK Memory Management APIs

This section describes the Oracle Key Vault interfaces required to handle endpoint specified memory management.

- **okvFree**
okvFree is a pointer to the endpoint program defined function to free the memory allocated using okvMalloc or okvRealloc.
- **okvMalloc**
okvMalloc is a pointer to the endpoint program defined function that should allocate memory.
- **okvRealloc**
okvRealloc is a pointer to the endpoint program defined function that should reallocate memory.

9.1 okvFree

okvFree is a pointer to the endpoint program defined function to free the memory allocated using okvMalloc or okvRealloc.

Category

Memory management API

Purpose

okvFree is a pointer to the endpoint program defined function to free the memory allocated using okvMalloc or okvRealloc. The pointer should be set to NULL after freeing it.

Syntax

```
void (*okvFree)(void *ctx, void **ptr);
```

Parameters

Parameter	IN/OUT	Description
ctx	IN	Memory context (context of OKVMemoryCtx)
ptr	IN	Previously allocated memory

Return Values

No values returned.

Comments

None.

Related Topics

- [okvMalloc](#)
okvMalloc is a pointer to the endpoint program defined function that should allocate memory.
- [okvRealloc](#)
okvRealloc is a pointer to the endpoint program defined function that should reallocate memory.

9.2 okvMalloc

okvMalloc is a pointer to the endpoint program defined function that should allocate memory.

Category

Memory management API

Purpose

okvMalloc is a pointer to the endpoint program defined function that should allocate memory.

Syntax

```
void * (*okvMalloc)(void *ctx, size_t size);
```

Parameters

Parameter	IN/OUT	Description
ctx	IN	Memory context of OKVMemoryCtx.
size	IN	Size of memory to be allocated.

Return Values

Return Value	Description
void*	Memory pointer to allocated memory. Success: A valid pointer to the allocated memory is returned. Failure: A NULL pointer is returned if the function cannot allocate memory of requested size.

Comments

None.

Related Topics

- [okvFree](#)
okvFree is a pointer to the endpoint program defined function to free the memory allocated using okvMalloc or okvRealloc.

- [okvRealloc](#)
okvRealloc is a pointer to the endpoint program defined function that should reallocate memory.

9.3 okvRealloc

okvRealloc is a pointer to the endpoint program defined function that should reallocate memory.

Category

Memory management API

Purpose

okvRealloc is a pointer to the endpoint program defined function that should reallocate memory. The data in the previously allocated memory should be copied to the newly allocated memory.

Syntax

```
void * (*okvRealloc)(void *ctx, void **ptr, size_t size);
```

Parameters

Parameter	IN/OUT	Description
ctx	IN	Memory context (context of OKVMemoryCtx).
ptr	IN	Previously allocated memory.
size	IN	Size of the memory to be allocated.

Return Values

Return Value	Description
void*	Memory pointer to reallocated memory. Success: A valid pointer to the re-allocated memory is returned. Failure: A NULL pointer is returned if the function cannot allocate memory of requested size.

Comments

None.

Related Topics

- [okvFree](#)
okvFree is a pointer to the endpoint program defined function to free the memory allocated using okvMalloc or okvRealloc.
- [okvMalloc](#)
okvMalloc is a pointer to the endpoint program defined function that should allocate memory.

10

Oracle Key Vault Client SDK Error Handling APIs

This section describes the interfaces for Oracle Key Vault error management.

- [okvErrGetDepth](#)
`okvErrGetDepth` is used to return the depth of the error stack otherwise 0 is returned.
- [okvErrGetDepthForBatch](#)
`okvErrGetDepthForBatch` is used to return the depth of the error stack for the provided batch job number otherwise 0 is returned.
- [okvErrGetNum](#)
`okvErrGetNum` returns the error number on top of the error stack.
- [okvErrGetNumAtDepth](#)
`okvErrGetNumAtDepth` returns the error number at the specified depth of the error stack.
- [okvErrGetNumAtDepthForBatch](#)
`okvErrGetNumAtDepthForBatch` returns the error number at the specified depth of the error stack for the provided batch job number.
- [okvErrGetNumForBatch](#)
`okvErrGetNumForBatch` returns the error number on top of the error stack for the provided batch job number.
- [okvErrReset](#)
`okvErrReset` resets the error stack in the environment handle.
- [okvGetTextForErrNum](#)
`okvGetTextForErrNum` returns the text of the error number.

10.1 okvErrGetDepth

`okvErrGetDepth` is used to return the depth of the error stack otherwise 0 is returned.

Category

Error handling API

Purpose

`okvErrGetDepth` is used to return the depth of the error stack otherwise 0 is returned if no error was recorded in the error stack.

Syntax

```
ub1 okvErrGetDepth(OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
ub1	Oracle Key Vault error stack depth. Success: A non-zero positive number, which is the depth of the error stack, is returned. Failure: Zero is returned, since depth is zero if no error is recorded.

Comments

None.

Example

```
ub4 err_depth = okvErrGetDepth(env);

if (err_depth == 0)
{
    printf("No Error \n");
}
else
{
    printf("Error\n");
}
```

Related Topics

- [okvErrGetDepthForBatch](#)
`okvErrGetDepthForBatch` is used to return the depth of the error stack for the provided batch job number otherwise 0 is returned.
- [okvErrGetNum](#)
`okvErrGetNum` returns the error number on top of the error stack.
- [okvErrGetNumAtDepth](#)
`okvErrGetNumAtDepth` returns the error number at the specified depth of the error stack.
- [okvErrGetNumForBatch](#)
`okvErrGetNumForBatch` returns the error number on top of the error stack for the provided batch job number.
- [okvErrGetNumAtDepthForBatch](#)
`okvErrGetNumAtDepthForBatch` returns the error number at the specified depth of the error stack for the provided batch job number.
- [okvErrReset](#)
`okvErrReset` resets the error stack in the environment handle.

- `okvGetTextForErrNum`
`okvGetTextForErrNum` returns the text of the error number.

10.2 okvErrGetDepthForBatch

`okvErrGetDepthForBatch` is used to return the depth of the error stack for the provided batch job number otherwise 0 is returned.

Category

Error handling API

Purpose

`okvErrGetDepthForBatch` is used to return the depth of the error stack for the provided batch job number, otherwise 0 is returned.

Syntax

```
ub1 okvErrGetDepthForBatch(OKVEnv *env, ub4 batch_job_no);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>batch_job_no</code>	IN	Batch job number.

Return Values

Return Value	Description
<code>ub1</code>	Oracle Key Vault error stack depth. Success: A non-zero positive number which is the depth of the error stack for the respective batch job is returned. Failure: Zero is returned, since depth is zero if no error is recorded for the respective batch job.

Comments

Here `batch_job_no` is the number in which the operations are batched. For example, if the user wants to create a key, activate a key, revoke it, and then destroy it, all of these operations are batched in the same order. That is, `batch_job_no` for create a key is 1, `batch_job_no` for activate a key is 2, `batch_job_no` for revoke is 3 and `batch_job_no` for destroy is 4. Once the batch job execution finishes, the user can pass in the batch job number for `okvErrGetDepthForBatch` to get the depth of the errors from the respective batch job error stack.

If batch job number provided is invalid, then zero (0) is returned by this API.

Example

```
ub4 err_depth = 0;
okvBatchCreate(env);
```

```
okvCreateKey(...); /* 1st Batch Job */
okvActivate(...); /* 2nd Batch Job */
okvRevoke(...); /* 3rd Batch Job */
okvDestroy(...); /* 4th Batch Job */
okvBatchExecute(env);

/* Check error on top of the error stack for 1st batch job */
if (okvErrGetNumForBatch(env, 1))
{
    printf("Found error for 1st batch job");
    err_depth = okvErrGetDepthForBatch(env, 1);
    printf("Depth of the error stack is %d", err_depth);
}
```

Related Topics

- [okvErrGetDepth](#)
`okvErrGetDepth` is used to return the depth of the error stack otherwise 0 is returned.
- [okvErrGetNum](#)
`okvErrGetNum` returns the error number on top of the error stack.
- [okvErrGetNumAtDepth](#)
`okvErrGetNumAtDepth` returns the error number at the specified depth of the error stack.
- [okvErrGetNumForBatch](#)
`okvErrGetNumForBatch` returns the error number on top of the error stack for the provided batch job number.
- [okvErrGetNumAtDepthForBatch](#)
`okvErrGetNumAtDepthForBatch` returns the error number at the specified depth of the error stack for the provided batch job number.
- [okvErrReset](#)
`okvErrReset` resets the error stack in the environment handle.
- [okvGetTextForErrNum](#)
`okvGetTextForErrNum` returns the text of the error number.

10.3 okvErrGetNum

`okvErrGetNum` returns the error number on top of the error stack.

Category

Error handling API

Purpose

`okvErrGetNum` returns the error number on top of the error stack. `OKV_SUCCESS` is returned if no error recorded.

Syntax

```
OKVErrNo okvErrGetNum(OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: The error number on top of the error stack is returned. Failure: OKV_SUCCESS (0) is returned if there is no error.

Comments

None.

Example

```
printf("Setting up Oracle Key Vault session\n");
okvConnect(env);

if (okvErrGetNum(env))
{
    printf("Could not setup the Oracle Key Vault session\n");
    return 1;
}
else
{
    printf("Successfully setup Oracle Key Vault session\n\n");
}
```

Related Topics

- [okvErrGetDepth](#)
okvErrGetDepth is used to return the depth of the error stack otherwise 0 is returned.
- [okvErrGetDepthForBatch](#)
okvErrGetDepthForBatch is used to return the depth of the error stack for the provided batch job number otherwise 0 is returned.
- [okvErrGetNumAtDepth](#)
okvErrGetNumAtDepth returns the error number at the specified depth of the error stack.
- [okvErrGetNumForBatch](#)
okvErrGetNumForBatch returns the error number on top of the error stack for the provided batch job number.
- [okvErrGetNumAtDepthForBatch](#)
okvErrGetNumAtDepthForBatch returns the error number at the specified depth of the error stack for the provided batch job number.
- [okvErrReset](#)
okvErrReset resets the error stack in the environment handle.

- [okvGetTextForErrNum](#)
okvGetTextForErrNum returns the text of the error number.

10.4 okvErrGetNumAtDepth

okvErrGetNumAtDepth returns the error number at the specified depth of the error stack.

Category

Error handling API

Purpose

okvErrGetNumAtDepth returns the error number at the specified depth of the error stack otherwise OKV_SUCCESS is returned.

Syntax

```
OKVErrNo okvErrGetNumAtDepth(OKVEnv *env, ub1 depth);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
depth	IN	Depth at which the error number is needed.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: The error number at the specified depth in the error stack is returned. Otherwise: OKV_SUCCESS (0) is returned if there is no error.

Comments

okvErrGetNumAtDepth returns OKV_SUCCESS if the depth specified is more than that returned by okvErrGetDepth.

Example

```
ub4 err_depth = okvErrGetDepth(env);

while (err_depth > 0)
{
    ub4 error = 0;

    /* Get error number to get error text */
    error = okvErrGetNumAtDepth(env, err_depth--);
    printf("Error %d: %s \n", error, okvGetTextForErrNum(error));
}
```

Related Topics

- [okvErrGetDepth](#)
`okvErrGetDepth` is used to return the depth of the error stack otherwise 0 is returned.
- [okvErrGetDepthForBatch](#)
`okvErrGetDepthForBatch` is used to return the depth of the error stack for the provided batch job number otherwise 0 is returned.
- [okvErrGetNum](#)
`okvErrGetNum` returns the error number on top of the error stack.
- [okvErrGetNumForBatch](#)
`okvErrGetNumForBatch` returns the error number on top of the error stack for the provided batch job number.
- [okvErrGetNumAtDepthForBatch](#)
`okvErrGetNumAtDepthForBatch` returns the error number at the specified depth of the error stack for the provided batch job number.
- [okvErrReset](#)
`okvErrReset` resets the error stack in the environment handle.
- [okvGetTextForErrNum](#)
`okvGetTextForErrNum` returns the text of the error number.

10.5 okvErrGetNumAtDepthForBatch

`okvErrGetNumAtDepthForBatch` returns the error number at the specified depth of the error stack for the provided batch job number.

Category

Error handling API

Purpose

`okvErrGetNumAtDepthForBatch` returns the error number at the specified depth of the error stack for the provided batch job number, otherwise `OKV_SUCCESS` is returned.

Syntax

```
OKVErrNo okvErrGetNumAtDepthForBatch(OKVEnv *env, ub4 batch_job_no,
                                     ub1 depth);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>batch_job_no</code>	IN	Batch job number.
<code>depth</code>	IN	Depth at which the error number is needed.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: The error number at the specified depth in the error stack is returned for the respective batch job number. Otherwise: OKV_SUCCESS (0) is returned if there is no error.

Comments

`batch_job_no` is the number in which the operations are batched. For example, if the user wants to create a key, activate a key, revoke it, and then destroy it, all of these operations are batched in the same order; that is, `batch_job_no` for create a key is 1, `batch_job_no` for activate a key is 2, `batch_job_no` for revoke is 3, and `batch_job_no` for destroy is 4. Once the batch execution finishes, the user can pass in the batch job number and the depth at which the error is needed for `okvErrGetNumAtDepthForBatch` to get the error details.

If the batch job number provided is invalid, then OKV_SUCCESS (0) is returned by this API. `okvErrGetNumAtDepthForBatch` returns OKV_SUCCESS if the depth specified is more than that returned by `okvErrGetDepthForBatch`.

Example

```
ub4 err_depth = 0;
okvBatchCreate(env);
okvCreateKey(...); /* 1st Batch Job */
okvActivate(...); /* 2nd Batch Job */
okvRevoke(...);   /* 3rd Batch Job */
okvDestroy(...);  /* 4th Batch Job */
okvBatchExecute(env);

/* Check error on top of the error stack for 1st batch job */
if (okvErrGetNumForBatch(env, 1))
{
    printf("Found error for 1st Batch Job");
    err_depth = okvErrGetDepthForBatch(env, 1);
    printf("Depth of the error stack is %d", err_depth);

    while (err_depth > 0)
    {
        ub4 error = 0;
        /* Get error number to get error text */
        error = okvErrGetNumAtDepthForBatch(env, 1, err_depth--);
        printf("Error %d: %s \n", error, okvGetTextForErrNum(error));
    }
}
```

Related Topics

- [okvErrGetDepth](#)
`okvErrGetDepth` is used to return the depth of the error stack otherwise 0 is returned.

- [okvErrGetDepthForBatch](#)
`okvErrGetDepthForBatch` is used to return the depth of the error stack for the provided batch job number otherwise 0 is returned.
- [okvErrGetNum](#)
`okvErrGetNum` returns the error number on top of the error stack.
- [okvErrGetNumAtDepth](#)
`okvErrGetNumAtDepth` returns the error number at the specified depth of the error stack.
- [okvErrGetNumForBatch](#)
`okvErrGetNumForBatch` returns the error number on top of the error stack for the provided batch job number.
- [okvErrReset](#)
`okvErrReset` resets the error stack in the environment handle.
- [okvGetTextForErrNum](#)
`okvGetTextForErrNum` returns the text of the error number.

10.6 okvErrGetNumForBatch

`okvErrGetNumForBatch` returns the error number on top of the error stack for the provided batch job number.

Category

Error handling API

Purpose

`okvErrGetNumForBatch` returns the error number on top of the error stack for the provided batch job number. `OKV_SUCCESS` is returned if no error recorded.

Syntax

```
OKVErrNo okvErrGetNumForBatch(OKVEnv *env, ub4 batch_job_no);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>batch_job_no</code>	IN	Batch job number.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: The error number on top of the error stack for the respective batch job is returned. Failure: <code>OKV_SUCCESS</code> (0) is returned if there is no error.

Comments

`batch_job_no` is the number in which the operations are batched. For example, if the user wants to create a key, activate a key, revoke it and then destroy it, all of these operations are batched in the same order. That is, `batch_job_no` for create a key is 1, `batch_job_no` for activate a key is 2, `batch_job_no` for revoke is 3, and `batch_job_no` for destroy is 4. Once the batch execution finishes, the user can pass in the batch job number for `okvErrGetNumForBatch` to get the error from the top of the respective batch job error stack.

If batch job number provided is invalid, then `OKV_SUCCESS (0)` is returned by this API.

Example

```
okvBatchCreate(env);
okvCreateKey(...); /* 1st Batch Job */
okvActivate(...); /* 2nd Batch Job */
okvRevoke(...); /* 3rd Batch Job */
okvDestroy(...); /* 4th Batch Job */
okvBatchExecute(env);

/* Check error on top of the error stack for 1st Batch Job */
if (okvErrGetNumForBatch(env, 1))
{
    printf("Found error for 1st Batch Job");
}
```

Related Topics

- [okvErrGetDepth](#)
`okvErrGetDepth` is used to return the depth of the error stack otherwise 0 is returned.
- [okvErrGetDepthForBatch](#)
`okvErrGetDepthForBatch` is used to return the depth of the error stack for the provided batch job number otherwise 0 is returned.
- [okvErrGetNum](#)
`okvErrGetNum` returns the error number on top of the error stack.
- [okvErrGetNumAtDepth](#)
`okvErrGetNumAtDepth` returns the error number at the specified depth of the error stack.
- [okvErrGetNumAtDepthForBatch](#)
`okvErrGetNumAtDepthForBatch` returns the error number at the specified depth of the error stack for the provided batch job number.
- [okvErrReset](#)
`okvErrReset` resets the error stack in the environment handle.
- [okvGetTextForErrNum](#)
`okvGetTextForErrNum` returns the text of the error number.

10.7 okvErrReset

okvErrReset resets the error stack in the environment handle.

Category

Error handling API

Purpose

okvErrReset resets the error stack in the environment handle.

Syntax

```
void okvErrReset(OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Return Values

No values returned.

Comments

None.

Example

```
/* Do some KMIP operations like adding attribute to an object and get the same
   attributes, below is an illustration of using 'okvErrReset' when getting
   the individual attributes
*/

ub4 umask = 0;
ub4 state = 0;
printf("Trying to get Crypto Usage Mask value from State Attribute\n");
okvAttrGetCryptoUsageMask(env, ttlv, &umask);

if (okvErrGetNum(env))
/* Check for errors */
okvErrReset(env); /* this will come in handy when we don't want to keep
                  getting the same errors for the next set of API
                  calls where we try to get the individual Attribute
                  values */

printf("Trying to get State value from State Attribute\n");
okvAttrGetState(env, ttlv, &state);

if (okvErrGetNum(env))
/* Check for errors */
okvErrReset(env);
```

Related Topics

- [okvErrGetDepth](#)
`okvErrGetDepth` is used to return the depth of the error stack otherwise 0 is returned.
- [okvErrGetDepthForBatch](#)
`okvErrGetDepthForBatch` is used to return the depth of the error stack for the provided batch job number otherwise 0 is returned.
- [okvErrGetNum](#)
`okvErrGetNum` returns the error number on top of the error stack.
- [okvErrGetNumAtDepth](#)
`okvErrGetNumAtDepth` returns the error number at the specified depth of the error stack.
- [okvErrGetNumForBatch](#)
`okvErrGetNumForBatch` returns the error number on top of the error stack for the provided batch job number.
- [okvErrGetNumAtDepthForBatch](#)
`okvErrGetNumAtDepthForBatch` returns the error number at the specified depth of the error stack for the provided batch job number.
- [okvGetTextForErrNum](#)
`okvGetTextForErrNum` returns the text of the error number.

10.8 okvGetTextForErrNum

`okvGetTextForErrNum` returns the text of the error number.

Category

Error handling API

Purpose

`okvGetTextForErrNum` returns the text of the the error number. If the error number is not valid, a pointer to `NULL` is returned.

Syntax

```
oratext *okvGetTextForErrNum(OKVErrNo err_no);
```

Parameters

Parameter	IN/OUT	Description
<code>errno</code>	IN	Oracle Key Vault error number

Return Values

Return Value	Description
orertext *	Oracle Key Vault error text. Success: Pointer to text of the error is returned. Failure: NULL pointer is returned if the error number is not valid.

Comments

None.

Example

```
ub4 error = 0;
printf("Error %d: %s \n", error, okvGetTextForErrNum(error));
```

Related Topics

- [okvErrGetDepth](#)
`okvErrGetDepth` is used to return the depth of the error stack otherwise 0 is returned.
- [okvErrGetDepthForBatch](#)
`okvErrGetDepthForBatch` is used to return the depth of the error stack for the provided batch job number otherwise 0 is returned.
- [okvErrGetNum](#)
`okvErrGetNum` returns the error number on top of the error stack.
- [okvErrGetNumAtDepth](#)
`okvErrGetNumAtDepth` returns the error number at the specified depth of the error stack.
- [okvErrGetNumForBatch](#)
`okvErrGetNumForBatch` returns the error number on top of the error stack for the provided batch job number.
- [okvErrGetNumAtDepthForBatch](#)
`okvErrGetNumAtDepthForBatch` returns the error number at the specified depth of the error stack for the provided batch job number.
- [okvErrReset](#)
`okvErrReset` resets the error stack in the environment handle.

11

Oracle Key Vault Client SDK KMIP and Batch APIs

The SDK KMIP APIs provide functions for creating keys, activating keys, adding attributes to keys, destroying keys, and other operations. The batch APIs enable you to perform these activities in a batch operation.

- [Oracle Key Vault Client SDK KMIP APIs](#)
This section describes the interfaces for the Oracle Key Vault functions for KMIP operations.
- [Oracle Key Vault Client SDK Batch APIs](#)
This section describes the interfaces for the Oracle Key Vault KMIP batch functions.

11.1 Oracle Key Vault Client SDK KMIP APIs

This section describes the interfaces for the Oracle Key Vault functions for KMIP operations.

- [About the Oracle Key Vault Client SDK KMIP APIs](#)
The Oracle Key Vault KMIP APIs enable you to perform actions such as managing keys and secret data.
- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDecrypt](#)
`okvDecrypt` performs the decryption operation on the provided data using KMIP object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvEncrypt](#)
`okvEncrypt` performs the encryption operation on the provided data using KMIP object.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetCertificate](#)
`okvGetCertificate` implements the KMIP Get operation for the Certificate object.

- [okvGetCertificateRequest](#)
`okvGetCertificateRequest` implements the KMIP Get operation for the Certificate request object.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetPrivateKey](#)
`okvGetPrivateKey` implements the KMIP Get operation for the KMIP private key object.
- [okvGetPublicKey](#)
`okvGetPublicKey` implements the KMIP Get operation for the KMIP public key object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegCertificate](#)
`okvRegCertificate` implements the KMIP Register operation for the KMIP certificate object.
- [okvRegCertificateRequest](#)
`okvRegCertificateRequest` implements the KMIP Register operation for the certificate request object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegPrivateKey](#)
`okvRegPrivateKey` implements the KMIP Register operation for the KMIP private key object.
- [okvRegPublicKey](#)
`okvRegPublicKey` implements the KMIP Register operation for the KMIP public key object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.

- [okvRegTemplate](#)
okvRegTemplate implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
okvRekey implements the KMIP Rekey operation.
- [okvRevoke](#)
okvRevoke implements the KMIP Revoke operation.
- [okvSign](#)
okvSign implements the KMIP Sign operation.
- [okvSignVerify](#)
okvSignVerify implements the KMIP Signature Verify operation.
- [okvCreateKeyPair](#)
okvCreateKeyPair implements the KMIP Create Key Pair operation.

11.1.1 About the Oracle Key Vault Client SDK KMIP APIs

The Oracle Key Vault KMIP APIs enable you to perform actions such as managing keys and secret data.

Many of these functions take unique identifier as an input argument. As per KMIP v1.1, the unique identifier can be optional when the commands are batched given that the KMIP server can determine a single unique identifier from the previous commands. So if the previous command like locate returns only one unique identifier for possible use-cases, and the following commands operate on this unique identifier, the unique identifier can be omitted from the following commands.

The unique identifiers, along with their lengths, will be returned from the KMIP API functions. The unique identifiers needs to be NULL terminated by the endpoint program.

The endpoint program can pass in a larger buffer and the length will be used to determine the actual unique identifier bits in the larger buffer.

11.1.2 okvActivate

okvActivate implements the KMIP Activate operation.

Category

KMIP API

Purpose

okvActivate implements the KMIP Activate operation. It will activate the KMIP object identified by its unique identifier.

Syntax

```
OKVErrNo okvActivate(OKVEnv *env, oratext *uid);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Parameter	IN/OUT	Description
uid	IN	Unique identifier (can be NULL for batching).

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```

/* Create the KMIP object, say Key for example and get its unique
   identifier as part of its creation in 'uid' and then activate
   it as below
*/

okvActivate(env, &uid[0]);

if (okvErrGetNum(env))
{
    printf("Error while activating the object\n");
}

```

Related Topics

- [okvAddAttribute](#)
okvAddAttribute implements the KMIP Add attribute operation.
- [okvCreateKey](#)
okvCreateKey implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
okvDeleteAttribute implements the KMIP Delete attribute operation.
- [okvDestroy](#)
okvDestroy implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
okvGetAttributeList implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
okvGetAttributes implements KMIP Get attribute operation.
- [okvGetKey](#)
okvGetKey implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
okvGetOpaqueData implements the KMIP Get operation for the KMIP opaque data object.

- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.3 okvAddAttribute

`okvAddAttribute` implements the KMIP Add attribute operation.

Category

KMIP API

Purpose

`okvAddAttribute` implements the KMIP Add attribute operation. It adds an attribute to the KMIP object specified by the unique identifier.

Syntax

```
OKVErrNo okvAddAttribute(OKVEnv *env, oratext *uid,
                        OKVTTLV **attr);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier (can be NULL for batching).

Parameter	IN/OUT	Description
attr	IN	Attribute to be added to the KMIP object.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The API has the below exceptions when used with Oracle Key Vault server:

- If a single instance attribute is added to an object using this API and the object already has an instance of the attribute, then the attribute won't get overwritten, but a general failure error will be thrown. Please use the `okvModifyAttribute` API to modify attribute values.
- If a protect stop date later than the deactivation date is passed in request TTLV, the server will not give an error and the protect stop date will be added to registered KMIP object.
- If a process start date is added using this API, the server will give permission denied error. As a workaround the attribute can be added during registration using APIs `okvRegKey`, `okvRegSecretData`, `okvRegOpaqueData`, and `okvRegTemplate`.

Example

```

/* Create the KMIP object, say Key for example and get its unique
   identifier as part of its creation in 'uid', we can add an attribute
   to it as shown below */

OKVTTLV *attr_in = (OKVTTLV *)NULL;
OKVTTLV *req = (OKVTTLV *)NULL;
oratext *name_value = (oratext *)"attribute_name";
ub4 name_valuel = strlen("attribute_name");
req = okvEnvGetOpRequestObj(env);
attr_in = okvAddAttributeObject(env, req, OKVAttrName, (ub4) 0);

okvAttrAddName(env, attr_in, name_value, name_valuel, 1);
okvAddAttribute(env, &uid[0], &attr_in);

if (okvErrGetNum(env))
{
    printf("Error while adding Name attribute to the object\n");
}

```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.

- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.4 okvCreateKey

`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.

Category

KMIP API

Purpose

`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object. The unique identifier of the symmetric key object generated by the Oracle Key Vault server is returned as `oid`. The maximum length of the unique ID for Oracle Key Vault SDK is defined by `OKV_UNIQUE_ID_MAXLEN`.

Syntax

```
OKVErrNo okvCreateKey(OKVEnv *env,
                      OKVType alg, ub4 len, ub4 mask,
                      OKVTTLV *template_names_attrs,
                      oratext *wallet_name, ub4 wallet_name1,
                      oratext *oid, ub4 *oid1);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>alg</code>	IN	Symmetric key algorithm.
<code>len</code>	IN	Key length of the symmetric key.
<code>mask</code>	IN	Cryptographic usage mask of the symmetric key.
<code>template_names_attrs</code>	IN	Template names or attributes that will form the template-attribute.
<code>wallet_name</code>	IN	Wallet name value.
<code>wallet_name1</code>	IN	Length of the wallet name value.
<code>oid</code>	OUT	Unique identifier of the generated key.
<code>oid1</code>	OUT	Unique identifier length of the generated key.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

It is recommended to add a KMIP Name attribute to symmetric key object to help identify it in future.

The caller has to allocate the memory for the unique identifier returned by this function. The length of allocated memory is passed in via the length of the unique identifier argument `uidl`. Sufficient memory to store the returned unique identifier should be allocated.

A symmetric key of the specified length for the specified algorithm and for a specific use (cryptographic usage mask) is generated in wallet `wallet_name` if specified else it is generated in the default wallet if present with the endpoint.

If `mask` is set to zero 0, then a default value of symmetric key's cryptographic usage mask (encrypt|decrypt|wrap_key|unwrap_key) is assigned during its creation.

Example

```
/* Parameters to create symmetric key */
OKVType algo = CRYPTO_ALG_AES;

/* Key length 128, because AES keys are 128, 192 or 256 bits in length*/
ub4 key_len = 128;
ub4 usage_mask = CRYPTO_MASK_ENCRYPT | CRYPTO_MASK_DECRYPT;
oratext uid[OKV_UNIQUE_ID_MAXLEN + 1];
ub4 uidl = sizeof(uid);
OKVTTLV *template = (OKVTTLV *)NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;

/* Set up the environment handle 'env' and also the memory and connection
management as shown in previous sections */
memset(uid, 0, uidl);
template = okvEnvGetOpRequestObj(env);

/* Add name attribute object to template attribute */
attr_in = okvAddAttributeObject(env, template, OKVAttrName, (ub4) 0);
okvAttrAddName(env, attr_in, (oratext *)"My New Key", strlen("My New Key"), 1);
printf("\tCreating a Symmetric key\n");

okvCreateKey(env, algo, key_len, usage_mask, template,
             (oratext *)NULL, (ub4)0, &uid[0], uidl);

if (okvErrGetNum(env))
{
    printf("Error while creating the key\n");
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.

- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.5 okvDecrypt

`okvDecrypt` performs the decryption operation on the provided data using KMIP object.

Category

KMIP API

Purpose

okvDecrypt performs the decryption operation on the provided data using KMIP object.

Syntax

```
OKVErrNo okvDecrypt(OKVEnv *env, oratext *uid, ub1 *data, ub4 datal,
                   OKVCryptoContext *crypto_context,
                   OKVDecryptResponse *decrypt_response);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
uid	IN	Unique identifier (can be NULL for batching).
data	IN	Data to be decrypted.
datal	IN	Length of the data to be decrypted.
crypto_context	IN	Cryptographic context contains required parameters for decryption like cryptographic parameters and IV.
decrypt_response	OUT	Contains the decrypt operation response details.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

crypto_context can be created and freed using okvCryptoContextCreate and okvCryptoContextFree helper APIs. It contains the required parameters for decryption and the user will need to set it explicitly by making use of helper APIs like okvCryptoContextSetBlockCipherMode, okvCryptoContextSetPadding, okvCryptoContextSetRandomIV, okvCryptoContextSetIV, okvCryptoContextSetAuthEncryptionAdditionalData, and okvCryptoContextSetAuthEncryptionTag. The user can also get the respective parameter values that were set in crypto_context using helper APIs okvCryptoContextGetBlockCipherMode, okvCryptoContextGetPadding, okvCryptoContextGetRandomIV, okvCryptoContextGetIV, okvCryptoContextGetAuthEncryptionAdditionalData, and okvCryptoContextGetAuthEncryptionTag.

`decrypt_response` will need to explicitly be allocated using helper API `okvDecryptResponseCreate` before passing it as an OUT parameter to `okvDecrypt` API. Once the decrypt operation is completed, we can get the decrypted data details from `decrypt_response` using helper API `okvCryptoResponseGetDecryptedData`. `decrypt_response` needs to be freed using `okvDecryptResponseFree` helper API.

Example

/* Create a Symmetric Key for example and get its unique identifier as part of its creation in `uid`, we can use the 'uid' for decrypting the encrypted data as shown below */

```
OKVCryptoContext *crypto_context = (OKVCryptoContext *)NULL;
OKVEncryptResponse *encrypt_response = (OKVEncryptResponse *)NULL;
OKVDecryptResponse *decrypt_response = (OKVDecryptResponse *)NULL;
ub1 data[] = "OKV crypto operations demo.";
ub4 datal = strlen((const char *) data);
ub1 iv[] = "5432109876543210";
ub4 ivl = strlen((const char *) iv);
ub1 encrypted_data[100];
ub4 encrypted_datal = sizeof(encrypted_data);
ub1 decrypted_data[100];
ub4 decrypted_datal = sizeof(decrypted_data);

/* Encrypt */
crypto_context = okvCryptoContextCreate(env, OKVOpEncrypt);
okvCryptoContextSetBlockCipherMode(env, crypto_context, BLK_CIPHER_CBC);
okvCryptoContextSetPadding(env, crypto_context, PADDING_PKCS5);
okvCryptoContextSetIV(env, crypto_context, iv, ivl);

encrypt_response = okvEncryptResponseCreate(env);

okvEncrypt(env, uid, data, datal, crypto_context, encrypt_response);
if (okvErrGetNum(env))
{
    printf("Error while performing the encryption operation.\n");
}

memset(encrypted_data, 0, encrypted_datal);
okvCryptoResponseGetEncryptedData(env, encrypt_response, encrypted_data,
&encrypted_datal);
printf("Successfully encrypted the data\n");
printf("\tEncrypted Data Length: %d\n", encrypted_datal);
printf("\tEncrypted Data: %s\n", encrypted_data);

okvCryptoContextFree(env, &crypto_context);
okvEncryptResponseFree(env, &encrypt_response);

/*Decrypt */
crypto_context = okvCryptoContextCreate(env, OKVOpEncrypt);
okvCryptoContextSetBlockCipherMode(env, crypto_context, BLK_CIPHER_CBC);
okvCryptoContextSetPadding(env, crypto_context, PADDING_PKCS5);
okvCryptoContextSetIV(env, crypto_context, iv, ivl);

decrypt_response = okvDecryptResponseCreate(env);
okvDecrypt(env, uid, encrypted_data, encrypted_datal, crypto_context,
decrypt_response);
if (okvErrGetNum(env))
{
```

```
    printf("Error while performing the decryption operation.\n");
}

memset(decrypted_data, 0, decrypted_data1);
okvCryptoResponseGetDecryptedData(env, decrypt_response, decrypted_data,
&decrypted_data1);
printf("Successfully decrypted the data\n");
printf("\tDecrypted Data Length: %d\n", decrypted_data1);
printf("\tDecrypted Data: %s\n", decrypted_data);

okvCryptoContextFree(env, &crypto_context);
okvDecryptResponseFree(env, &decrypt_response);
```

Related Topics

- [okvCryptoContextCreate](#)
`okvCryptoContextCreate` creates the cryptographic context required for cryptographic operations.
- [okvCryptoContextFree](#)
`okvCryptoContextFree` frees the memory allocated to cryptographic context structure.
- [okvCryptoContextGetAuthEncryptionAdditionalData](#)
`okvCryptoContextGetAuthEncryptionAdditionalData` gets the authenticated encryption additional data parameter value from cryptographic context structure.
- [okvCryptoContextGetAuthEncryptionTag](#)
`okvCryptoContextGetAuthEncryptionTag` gets the authenticated encryption tag parameter value from cryptographic context structure.
- [okvCryptoContextGetBlockCipherMode](#)
`okvCryptoContextGetBlockCipherMode` gets the block cipher mode parameter value from cryptographic context structure.
- [okvCryptoContextGetIV](#)
`okvCryptoContextGetIV` gets the IV parameter value from cryptographic context structure.
- [okvCryptoContextGetPadding](#)
`okvCryptoContextGetPadding` gets the padding parameter value from cryptographic context structure.
- [okvCryptoContextGetRandomIV](#)
`okvCryptoContextGetRandomIV` gets the random IV parameter value from cryptographic context structure.
- [okvCryptoContextSetAuthEncryptionAdditionalData](#)
`okvCryptoContextSetAuthEncryptionAdditionalData` sets the authenticated encryption additional data parameter value in the cryptographic context structure.
- [okvCryptoContextSetAuthEncryptionTag](#)
`okvCryptoContextSetAuthEncryptionTag` sets the authenticated encryption tag parameter value in the cryptographic context structure.
- [okvCryptoContextSetBlockCipherMode](#)
`okvCryptoContextSetBlockCipherMode` sets the block cipher mode parameter value in the cryptographic context structure.
- [okvCryptoContextSetIV](#)
`okvCryptoContextSetIV` sets the IV parameter value in the cryptographic context structure.

- [okvCryptoContextSetPadding](#)
`okvCryptoContextSetPadding` sets the padding parameter value in the cryptographic context structure.
- [okvCryptoContextSetRandomIV](#)
`okvCryptoContextSetRandomIV` sets the random IV parameter value in the cryptographic context structure.
- [okvCryptoResponseGetDecryptedData](#)
`okvCryptoResponseGetDecryptedData` gets the decrypted data value from decrypt response structure.
- [okvDecryptResponseCreate](#)
`okvDecryptResponseCreate` creates the decrypt response structure to hold the decrypt operation response details.
- [okvDecryptResponseFree](#)
`okvDecryptResponseFree` frees the memory allocated to decrypt response structure.
- [okvEncrypt](#)
`okvEncrypt` performs the encryption operation on the provided data using KMIP object.

11.1.6 okvDeleteAttribute

`okvDeleteAttribute` implements the KMIP Delete attribute operation.

Category

KMIP API

Purpose

`okvDeleteAttribute` implements the KMIP Delete attribute operation. It deletes an attribute specified by an attribute name and attribute index of the KMIP object specified by the unique identifier.

Syntax

```
OKVErrNo okvDeleteAttribute(OKVEnv *env, oratext *uid,
                             oratext *attr_name,
                             ub4 attr_index,
                             OKVTTLV **attr);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier (can be NULL for batching).
<code>attr_name</code>	IN	Name of attribute to be deleted.
<code>attr_index</code>	IN	Index of the attribute to be deleted.
<code>attr</code>	OUT	Attribute to be deleted from the KMIP object.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
/* Create the KMIP object, say Key for example and get its unique identifier
   as part of its creation in 'uid'. Add contact information attribute and
   to delete it, it can done as shown below */

OKVTTLV *attr_del = (OKVTTLV *) NULL;
oratext *attr_name = okvGetTextForAttributeNum(OKVAttrContactInfo);

/* Passing Contact Info attribute to be deleted at attribute index 0 */
okvDeleteAttribute(env, &uid[0], attr_name, (ub4)0, &attr_del);

if (okvErrGetNum(env))
{
    printf("Error while deleting the contact info attribute of the object\n");
}
```

Related Topics

- [okvActivate](#)
okvActivate implements the KMIP Activate operation.
- [okvAddAttribute](#)
okvAddAttribute implements the KMIP Add attribute operation.
- [okvCreateKey](#)
okvCreateKey implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDestroy](#)
okvDestroy implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
okvGetAttributeList implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
okvGetAttributes implements KMIP Get attribute operation.
- [okvGetKey](#)
okvGetKey implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
okvGetOpaqueData implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
okvGetSecretData implements the KMIP Get operation for the KMIP secret data object.

- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.7 okvDestroy

`okvDestroy` implements the KMIP Destroy operation.

Category

KMIP API

Purpose

`okvDestroy` implements the KMIP Destroy operation. It will destroy the KMIP object specified by unique identifier.

Syntax

```
OKVErrNo okvDestroy(OKVEnv *env, oratext *uid);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier (can be NULL for batching).

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
/* Create the KMIP object, say Key for example and get its unique
   identifier as part of its creation in 'uid', activate it,
   revoke it and then you can destroy it as below */

okvDestroy(env, &uid[0]);

if (okvErrGetNum(env))
{
    printf("Error while destroying the object\n");
}
```

Related Topics

- [okvActivate](#)
okvActivate implements the KMIP Activate operation.
- [okvAddAttribute](#)
okvAddAttribute implements the KMIP Add attribute operation.
- [okvCreateKey](#)
okvCreateKey implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
okvDeleteAttribute implements the KMIP Delete attribute operation.
- [okvGetAttributeList](#)
okvGetAttributeList implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
okvGetAttributes implements KMIP Get attribute operation.
- [okvGetKey](#)
okvGetKey implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
okvGetOpaqueData implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
okvGetSecretData implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
okvGetTemplate implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
okvLocate implements the KMIP Locate operation.

- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.8 okvEncrypt

`okvEncrypt` performs the encryption operation on the provided data using KMIP object.

Category

KMIP API

Purpose

`okvEncrypt` performs the encryption operation on the provided data using KMIP object.

Syntax

```
OKVErrNo okvEncrypt(OKVEnv *env, oratext *uid, ub1 *data, ub4 datal,
                   OKVCryptoContext *crypto_context,
                   OKVEncryptResponse *encrypt_response);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier (can be NULL for batching).
<code>data</code>	IN	Data to be encrypted.
<code>datal</code>	IN	Length of the data to be encrypted.

Parameter	IN/OUT	Description
crypto_context	IN	Cryptographic context contains required parameters for encryption like cryptographic parameters and IV.
encrypt_response	OUT	Contains the encrypt operation response details.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

`crypto_context` can be created and freed using `okvCryptoContextCreate` and `okvCryptoContextFree` helper APIs. It contains the required parameters for encryption and the user will need to set it explicitly by making use of helper APIs like `okvCryptoContextSetBlockCipherMode`, `okvCryptoContextSetPadding`, `okvCryptoContextSetRandomIV`, `okvCryptoContextSetIV`, `okvCryptoContextSetAuthEncryptionAdditionalData`, and `okvCryptoContextSetAuthEncryptionTag`. The user can also get the respective parameter values that was set in `crypto_context` using helper APIs `okvCryptoContextGetBlockCipherMode`, `okvCryptoContextGetPadding`, `okvCryptoContextGetRandomIV`, `okvCryptoContextGetIV`, `okvCryptoContextGetAuthEncryptionAdditionalData`, and `okvCryptoContextGetAuthEncryptionTag`.

`encrypt_response` will need to explicitly be allocated using helper API `okvEncryptResponseCreate` before passing it as an OUT parameter to `okvEncrypt` API. Once the encrypt operation is completed, we can get the encrypted data details from `encrypt_response` using helper APIs `okvCryptoResponseGetEncryptedData`, `okvCryptoResponseGetIV`, and `okvCryptoResponseGetAuthEncryptionTag`. `encrypt_response` needs to be freed using `okvEncryptResponseFree` helper API.

Example

```
/* Create a Symmetric Key for example and get its unique identifier as part of its
creation in 'uid', we can use the 'uid' for encryption as shown below */
```

```
OKVCryptoContext *crypto_context = (OKVCryptoContext *)NULL;
OKVEncryptResponse *encrypt_response = (OKVEncryptResponse *)NULL;
ub1 data[] = "OKV crypto operations demo.";
ub4 datal = strlen((const char *) data);
ub1 iv[] = "5432109876543210";
ub4 ivl = strlen((const char *) iv);
ub1 encrypted_data[100];
```



```
ub4 encrypted_data1 = sizeof(encrypted_data);

/* Encrypt */
crypto_context = okvCryptoContextCreate(env, OKVOpEncrypt);
okvCryptoContextSetBlockCipherMode(env, crypto_context, BLK_CIPHER_CBC);
okvCryptoContextSetPadding(env, crypto_context, PADDING_PKCS5);
okvCryptoContextSetIV(env, crypto_context, iv, iv1);

encrypt_response = okvEncryptResponseCreate(env);

okvEncrypt(env, uid, data, data1, crypto_context, encrypt_response);
if (okvErrGetNum(env))
{
    printf("Error while performing the encryption operation.\n");
}

memset(encrypted_data, 0, encrypted_data1);
okvCryptoResponseGetEncryptedData(env, encrypt_response, encrypted_data,
&encrypted_data1);
printf("Successfully encrypted the data\n");
printf("\tEncrypted Data Length: %d\n", encrypted_data1);
printf("\tEncrypted Data: %s\n", encrypted_data);

okvCryptoContextFree(env, &crypto_context);
okvEncryptResponseFree(env, &encrypt_response);
```

Related Topics

- [okvCryptoContextCreate](#)
`okvCryptoContextCreate` creates the cryptographic context required for cryptographic operations.
- [okvCryptoContextFree](#)
`okvCryptoContextFree` frees the memory allocated to cryptographic context structure.
- [okvCryptoContextGetAuthEncryptionAdditionalData](#)
`okvCryptoContextGetAuthEncryptionAdditionalData` gets the authenticated encryption additional data parameter value from cryptographic context structure.
- [okvCryptoContextGetAuthEncryptionTag](#)
`okvCryptoContextGetAuthEncryptionTag` gets the authenticated encryption tag parameter value from cryptographic context structure.
- [okvCryptoContextGetBlockCipherMode](#)
`okvCryptoContextGetBlockCipherMode` gets the block cipher mode parameter value from cryptographic context structure.
- [okvCryptoContextGetIV](#)
`okvCryptoContextGetIV` gets the IV parameter value from cryptographic context structure.
- [okvCryptoContextGetPadding](#)
`okvCryptoContextGetPadding` gets the padding parameter value from cryptographic context structure.
- [okvCryptoContextGetRandomIV](#)
`okvCryptoContextGetRandomIV` gets the random IV parameter value from cryptographic context structure.

- [okvCryptoContextSetAuthEncryptionAdditionalData](#)
`okvCryptoContextSetAuthEncryptionAdditionalData` sets the authenticated encryption additional data parameter value in the cryptographic context structure.
- [okvCryptoContextSetAuthEncryptionTag](#)
`okvCryptoContextSetAuthEncryptionTag` sets the authenticated encryption tag parameter value in the cryptographic context structure.
- [okvCryptoContextSetBlockCipherMode](#)
`okvCryptoContextSetBlockCipherMode` sets the block cipher mode parameter value in the cryptographic context structure.
- [okvCryptoContextSetIV](#)
`okvCryptoContextSetIV` sets the IV parameter value in the cryptographic context structure.
- [okvCryptoContextSetPadding](#)
`okvCryptoContextSetPadding` sets the padding parameter value in the cryptographic context structure.
- [okvCryptoContextSetRandomIV](#)
`okvCryptoContextSetRandomIV` sets the random IV parameter value in the cryptographic context structure.
- [okvCryptoResponseGetAuthEncryptionTag](#)
`okvCryptoResponseGetAuthEncryptionTag` gets the authenticated encryption tag value from encrypt response structure.
- [okvCryptoResponseGetEncryptedData](#)
`okvCryptoResponseGetEncryptedData` gets the encrypted data value from encrypt response structure.
- [okvCryptoResponseGetIV](#)
`okvCryptoResponseGetIV` gets the IV value from encrypt response structure used by server for encryption, if the random IV was set and IV was not provided in the request.
- [okvDecrypt](#)
`okvDecrypt` performs the decryption operation on the provided data using KMIP object.
- [okvEncryptResponseCreate](#)
`okvEncryptResponseCreate` creates the encrypt response structure to hold the encrypt operation response details.
- [okvEncryptResponseFree](#)
`okvEncryptResponseFree` frees the memory allocated to encrypt response structure.

11.1.9 okvGetAttributeList

`okvGetAttributeList` implements KMIP Get attribute list operation.

Category

KMIP API

Purpose

`okvGetAttributeList` implements KMIP Get attribute list operation. It retrieves the names of the regular and custom attributes of a KMIP object specified by the unique identifier.

`attr_names_count` specifies how many `attr_names` can be accommodated in `attr_names` and `okvGetAttributeList()` will only copy that many attribute names. If there are more attributes then `attr_names_count` will be modified to store the actual number of attributes in the returned request.

Syntax

```
OKVErrNo okvGetAttributeList(OKVEnv *env, oratext *uid,
                             ub4 *attr_names_count, oratext **attr_names);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault Interface environment handle.
<code>uid</code>	IN	Unique identifier (can be <code>NULL</code> for batching).
<code>attr_names_count</code>	IN/OUT	Count of the attributes.
<code>attr_names</code>	OUT	Names of the attributes.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The list retrieved is unordered.

Example

```
/* Create the KMIP object, say Key for example and get its unique identifier
   as part of its creation in 'uid'. Add attributes like say name, contact info
   and then names of these attributes can be retrieved as below */
...
ub4 attr_list_count = 0;
oratext **attr_names = (oratext **)NULL;

printf("\tGetting the count of attributes associated with the key\n");
okvGetAttributeList(env, uid, &attr_list_count, (oratext **)NULL);

if (okvErrGetNum(env))
{
    printf("Error while getting the attribute list count\n");
}

printf("\tGetting the attribute names associated with the key\n");
attr_names = (oratext **)calloc(attr_list_count, sizeof(oratext *));

for (i = 0; i < attr_list_count; i++)
{
    /* Allocate memory to hold attribute names */
    attr_names[i] = (oratext *)calloc(OKV_NAME_MAXLEN,
    sizeof(oratext));
```

```
}  
  
okvGetAttributeList(env, uid, &attr_list_count, (oratext **)attr_names);  
  
if (okvErrGetNum(env))  
{  
    printf("Error while getting the attribute list names\n");  
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.

- [okvRekey](#)
okvRekey implements the KMIP Rekey operation.
- [okvRevoke](#)
okvRevoke implements the KMIP Revoke operation.

11.1.10 okvGetAttributes

okvGetAttributes implements KMIP Get attribute operation.

Category

KMIP API

Purpose

okvGetAttributes implements KMIP Get attribute operation. It retrieves the specified list of regular and custom attributes for a given KMIP object specified by the unique identifier.

Syntax

```
OKVErrNo okvGetAttributes(OKVEnv *env, oratext *uid,
                          ub4 attr_names_count,
                          oratext **attr_names,
                          OKVTTLV **attrs);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
uid	IN	Unique identifier (can be NULL for batching).
attr_names_count	IN	Count of the attributes to be retrieved.
attr_names	IN	Names of the attributes to be retrieved.
attrs	OUT	Attributes retrieved.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The list retrieved is unordered.

Example

```
/* Create the KMIP object, say Key for example and get its unique
   identifier as part of its creation in 'uid'. Add contact information
```

```
Name, Cryptographic Alogirthm, Cryptographic Length attributes to the
created key and then all of these attributes can be retrieved as below */
...
OKVTTLV *attrs = (OKVTTLV *) NULL;
oratext *attr_name_list[3];

attr_name_list[0] = okvGetTextForAttributeNum(OKVAttrName);
attr_name_list[1] = okvGetTextForAttributeNum(OKVAttrCryptoAlg);
attr_name_list[2] = okvGetTextForAttributeNum(OKVAttrCryptoLen);

okvGetAttributes(env, uid, 3, (oratext **) attr_name_list, &attrs);

if (okvErrGetNum(env))
{
    printf("Error while getting the attributes of the object\n");
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.

- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.11 okvGetCertificate

`okvGetCertificate` implements the KMIP Get operation for the Certificate object.

Category

KMIP API

Purpose

`okvGetCertificate` implements the KMIP Get operation for the Certificate object.

For the specified unique identifier of the certificate, the certificate type, certificate length, the actual certificate bytes in the endpoint program supplied buffer and the actual length of the certificate bytes are returned.

If the length of the certificate buffer supplied is smaller than the length of the actual certificate retrieved from the Oracle Key Vault Server, then `certificateLen` is populated with the actual `certificate` length but `certificate` is set to NULL.

Syntax

```
OKVErrNo okvGetCertificate(OKVEnv *env, oratext *uid,
                           ub4 *certificate_type,
                           ub1 *certificate, ub4 *certificateLen);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier of the certificate (can be NULL for batching).
<code>certificate_type</code>	OUT	Type of certificate.
<code>certificate</code>	OUT	Certificate.
<code>certificateLen</code>	OUT	Length of the certificate.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
/* Create a Certificate for example and get its unique
   identifier as part of its creation in 'uid' */
...
ub1 *cert;
ub4 cert1 = 128001;
ub4 cert_type = 0;
cert = (ub1 *)malloc(cert1 * sizeof(ub1));

printf("\tGetting the certificate\n");

okvGetCertificate(env, uid, &cert_type, cert, &cert1);

if (okvErrGetNum(env))
{
    printf("Error while getting the certificate\n");
}

/* Free 'cert' */
```

Related Topics

- [okvActivate](#)
okvActivate implements the KMIP Activate operation.
- [okvAddAttribute](#)
okvAddAttribute implements the KMIP Add attribute operation.
- [okvCreateKey](#)
okvCreateKey implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
okvDeleteAttribute implements the KMIP Delete attribute operation.
- [okvDestroy](#)
okvDestroy implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
okvGetAttributeList implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
okvGetAttributes implements KMIP Get attribute operation.

- [okvGetCertificateRequest](#)
`okvGetCertificateRequest` implements the KMIP Get operation for the Certificate request object.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetPrivateKey](#)
`okvGetPrivateKey` implements the KMIP Get operation for the KMIP private key object.
- [okvGetPublicKey](#)
`okvGetPublicKey` implements the KMIP Get operation for the KMIP public key object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegCertificate](#)
`okvRegCertificate` implements the KMIP Register operation for the KMIP certificate object.
- [okvRegCertificateRequest](#)
`okvRegCertificateRequest` implements the KMIP Register operation for the certificate request object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegPrivateKey](#)
`okvRegPrivateKey` implements the KMIP Register operation for the KMIP private key object.
- [okvRegPublicKey](#)
`okvRegPublicKey` implements the KMIP Register operation for the KMIP public key object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.

- [okvRegTemplate](#)
okvRegTemplate implements the KMIP Register operation for the KMIP template object.
- [okvRegKey](#)
okvRegKey implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRevoke](#)
okvRevoke implements the KMIP Revoke operation.

11.1.12 okvGetCertificateRequest

okvGetCertificateRequest implements the KMIP Get operation for the Certificate request object.

Category

KMIP API

Purpose

okvGetCertificateRequest implements the KMIP Get operation for the Certificate request object.

For the specified unique identifier of the certificate request, the certificate request type, certificate request length, the actual certificate request bytes in the endpoint program supplied buffer and the actual length of the certificate request bytes are returned.

If the length of the certificate request buffer supplied is smaller than the length of the actual certificate request retrieved from the Oracle Key Vault Server, then the certificate_requestl is populated with the actual certificate request length but certificate_request is set to NULL.

Syntax

```
OKVErrNo okvGetCertificateRequest(OKVEnv *env, oratext *uid,
                                  ub4 *certificate_request_type,
                                  ub1 *certificate_request,
                                  ub4 *certificate_requestl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
uid	IN	Unique identifier of the certificate request (can be NULL for batching).
certificate_request_type	OUT	Type of certificate request.
certificate_request	OUT	Certificate request.
certificate_requestl	OUT	Length of the certificate request.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
/* Create a Certificate Request for example and get its unique
   identifier as part of its creation in 'uid' */
...
ub1 *cert_req;
ub4 cert_req1 = 128001;
ub4 cert_req_type = 0;

cert_req = (ub1 *)malloc(cert_req1 * sizeof(ub1));
printf("\tGetting the certificate request\n");

okvGetCertificateRequest(env, uid, &cert_req_type, cert_req,
                        &cert_req1);

if (okvErrGetNum(env))
{
    printf("Error while getting the certificate request\n");
}

/* Free 'cert_req' */
```

Related Topics

- [okvActivate](#)
okvActivate implements the KMIP Activate operation.
- [okvAddAttribute](#)
okvAddAttribute implements the KMIP Add attribute operation.
- [okvCreateKey](#)
okvCreateKey implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
okvDeleteAttribute implements the KMIP Delete attribute operation.
- [okvDestroy](#)
okvDestroy implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
okvGetAttributeList implements KMIP Get attribute list operation.

- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetCertificate](#)
`okvGetCertificate` implements the KMIP Get operation for the Certificate object.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetPrivateKey](#)
`okvGetPrivateKey` implements the KMIP Get operation for the KMIP private key object.
- [okvGetPublicKey](#)
`okvGetPublicKey` implements the KMIP Get operation for the KMIP public key object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegCertificate](#)
`okvRegCertificate` implements the KMIP Register operation for the KMIP certificate object.
- [okvRegCertificateRequest](#)
`okvRegCertificateRequest` implements the KMIP Register operation for the certificate request object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegPrivateKey](#)
`okvRegPrivateKey` implements the KMIP Register operation for the KMIP private key object.
- [okvRegPublicKey](#)
`okvRegPublicKey` implements the KMIP Register operation for the KMIP public key object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.

- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.13 okvGetKey

`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.

Category

KMIP API

Purpose

`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.

For the specified unique identifier of the symmetric key, the key length, key algorithm, the actual key bytes in the endpoint program supplied buffer and the actual length of the key bytes are returned.

If the length of the key buffer supplied is smaller than the length of the actual key retrieved from the Oracle Key Vault Server, then the `keyl` is populated with the actual key length but `key` is set to `NULL`.

Syntax

```
OKVErrNo okvGetKey(OKVEnv *env, oratext *uid,  
                  ub4 *key_alg, ub4 *key_len,  
                  ub1 *key, ub4 *keyl);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier of the key (can be <code>NULL</code> for batching).
<code>key_alg</code>	OUT	Symmetric key algorithm.
<code>key_len</code>	OUT	Key length of the symmetric key provided at the time of creation.
<code>key</code>	OUT	Symmetric key.
<code>keyl</code>	OUT	Length of the symmetric key.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
/* Create a Symmetric Key for example and get its unique
   identifier as part of its creation in 'uid' */
...
ub1 *key;
ub4 keyl = 128001;
ub4 key_algo = 0;
ub4 key_len = 0;
key = (ub1 *)malloc(keyl * sizeof(ub1));
printf("\tGetting the key\n");
okvGetKey(env, uid, &key_algo, &key_len, key, &keyl);
key[keyl] = 0;

if (okvErrGetNum(env))
{
    printf("Error while getting the key\n");
}

/* Free 'key' */
```

Related Topics

- [okvActivate](#)
okvActivate implements the KMIP Activate operation.
- [okvAddAttribute](#)
okvAddAttribute implements the KMIP Add attribute operation.
- [okvCreateKey](#)
okvCreateKey implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
okvDeleteAttribute implements the KMIP Delete attribute operation.
- [okvDestroy](#)
okvDestroy implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
okvGetAttributeList implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
okvGetAttributes implements KMIP Get attribute operation.
- [okvGetOpaqueData](#)
okvGetOpaqueData implements the KMIP Get operation for the KMIP opaque data object.

- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.14 okvGetOpaqueData

`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.

Category

KMIP API

Purpose

`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.

For the specified unique identifier of the opaque data, the opaque data type, the opaque data length and the opaque data bytes in the endpoint program supplied buffer is returned.

If the length of the opaque data buffer supplied is smaller than the length of the actual opaque data retrieved from the Oracle Key Vault server, then `opaque_data1` is populated with the actual opaque data length but `opaque_data` is set to `NULL`.

Syntax

```
OKVErrNo okvGetOpaqueData(OKVEnv *env, oratext *uid,
                          ub4 *opaque_data_type,
                          ub1 *opaque_data, ub4 *opaque_data1);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
uid	IN	Unique identifier of the opaque object (can be NULL for batching).
opaque_data_type	OUT	Type of opaque object.
opaque_data	OUT	Opaque object.
opaque_data1	OUT	Length of opaque object.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
/* Create an opaque data for example and get its unique
   identifier as part of its creation in 'uid' */
...
ub1    *opaque_data;
ub4    opaque_data_len = 128001;
ub4    opaque_data_type = 0;
opaque_data = (ub1 *)malloc(opaque_data_len*sizeof(ub1));

okvGetOpaqueData(env, &uid[0], &opaque_data_type, &opaque_data[0], &opaque_data_len);

if (okvErrGetNum(env))
{
    printf("Error while getting the opaque data\n");
}

/* Free "opaque_data" */
```

Related Topics

- [okvActivate](#)
okvActivate implements the KMIP Activate operation.

- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.15 okvGetPrivateKey

`okvGetPrivateKey` implements the KMIP Get operation for the KMIP private key object.

Category

KMIP API

Purpose

`okvGetPrivateKey` implements the KMIP Get operation for the KMIP private key object.

For the specified unique identifier of the private key, the private key length, private key algorithm, the actual private key bytes in the endpoint program supplied buffer and the actual length of the private key bytes are returned.

If the length of the private key buffer supplied is smaller than the length of the actual private key retrieved from the Oracle Key Vault server, then `private_key1` is populated with the actual private key length but `private_key` is set to NULL.

Syntax

```
OKVErrNo okvGetPrivateKey(OKVEnv *env, oratext *uid,
                          ub4 *private_key_alg, ub4 *private_key_len,
                          ub1 *private_key, ub4 *private_key1);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier of the private key (can be NULL for batching).
<code>private_key_alg</code>	OUT	Private key algorithm.
<code>private_key_len</code>	OUT	Key length of the private key provided at the time of creation.
<code>private_key</code>	OUT	Private key.
<code>private_key1</code>	OUT	Length of the private key.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS</code> (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
/* Create a Private Key for example and get its unique
   identifier as part of its creation in 'uid' */
...
ub1 *private_key;
ub4 private_keyl = 128001;
ub4 private_key_algo = 0;
ub4 private_key_len = 0;
private_key = (ub1 *)malloc(private_keyl * sizeof(ub1));

printf("\tGetting the private key\n");

okvGetPrivateKey(env, uid, &private_key_algo, &private_key_len,
                private_key, &private_keyl);

private_key[private_keyl] = 0;

if (okvErrGetNum(env))
{
    printf("Error while getting the private key\n");
}

/* Free 'private_key' */
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetCertificate](#)
`okvGetCertificate` implements the KMIP Get operation for the Certificate object.
- [okvGetCertificateRequest](#)
`okvGetCertificateRequest` implements the KMIP Get operation for the Certificate request object.

- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetPublicKey](#)
`okvGetPublicKey` implements the KMIP Get operation for the KMIP public key object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegCertificate](#)
`okvRegCertificate` implements the KMIP Register operation for the KMIP certificate object.
- [okvRegCertificateRequest](#)
`okvRegCertificateRequest` implements the KMIP Register operation for the certificate request object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegPrivateKey](#)
`okvRegPrivateKey` implements the KMIP Register operation for the KMIP private key object.
- [okvRegPublicKey](#)
`okvRegPublicKey` implements the KMIP Register operation for the KMIP public key object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.16 okvGetPublicKey

`okvGetPublicKey` implements the KMIP Get operation for the KMIP public key object.

Category

KMIP API

Purpose

`okvGetPublicKey` implements the KMIP Get operation for the KMIP public key object.

For the specified unique identifier of the public key, the public key length, public key algorithm, the actual public key bytes in the endpoint program supplied buffer and the actual length of the public key bytes are returned.

If the length of the public key buffer supplied is smaller than the length of the actual public key retrieved from the Oracle Key Vault Server, then the `public_keyl` is populated with the actual public key length but `public_key` is set to NULL.

Syntax

```
OKVErrNo okvGetPublicKey(OKVEnv *env, oratext *uid,
                        ub4 *public_key_alg, ub4 *public_key_len,
                        ub1 *public_key, ub4 *public_keyl);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier of the public key (can be NULL for batching).
<code>public_key_alg</code>	OUT	Public key algorithm.
<code>public_key_len</code>	OUT	Key length of the public key provided at the time of creation.
<code>public_key</code>	OUT	Public key.
<code>public_keyl</code>	OUT	Length of the public key.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
/* Create a Public Key for example and get its unique
   identifier as part of its creation in 'uid' */
...
ub1 *public_key;
ub4 public_keyl = 128001;
ub4 public_key_algo = 0;
ub4 public_key_len = 0;
public_key = (ub1 *)malloc(public_keyl * sizeof(ub1));

printf("\tGetting the public key\n");

okvGetPublicKey(env, uid, &public_key_algo, &public_key_len,
               public_key, &public_keyl);

public_key[public_keyl] = 0;

if (okvErrGetNum(env))
{
    printf("Error while getting the public key\n");
}

/* Free 'public_key' */
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetCertificate](#)
`okvGetCertificate` implements the KMIP Get operation for the Certificate object.
- [okvGetCertificateRequest](#)
`okvGetCertificateRequest` implements the KMIP Get operation for the Certificate request object.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.

- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetPrivateKey](#)
`okvGetPrivateKey` implements the KMIP Get operation for the KMIP private key object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegCertificate](#)
`okvRegCertificate` implements the KMIP Register operation for the KMIP certificate object.
- [okvRegCertificateRequest](#)
`okvRegCertificateRequest` implements the KMIP Register operation for the certificate request object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegPrivateKey](#)
`okvRegPrivateKey` implements the KMIP Register operation for the KMIP private key object.
- [okvRegPublicKey](#)
`okvRegPublicKey` implements the KMIP Register operation for the KMIP public key object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.17 okvGetSecretData

`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.

Category

KMIP API

Purpose

`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.

For the specified unique identifier of the secret data, the secret data type, the secret data length and the secret data bytes in the endpoint program supplied buffer is returned.

If the length of the secret data buffer supplied is smaller than the length of the actual secret data retrieved from the Oracle Key Vault server, then the `secret_data1` is populated with the actual secret data length but `secret_data` is set to NULL.

Syntax

```
OKVErrNo okvGetSecretData(OKVEnv *env, oratext *uid,
                          ub4 *secret_data_type,
                          ub1 *secret_data, ub4 *secret_data1);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier of the secret data (can be NULL for batching).
<code>secret_data_type</code>	OUT	Type of secret data.
<code>secret_data</code>	OUT	Secret data.
<code>secret_data1</code>	OUT	Length of secret data.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
/* Create a secret data for example and get its unique
   identifier as part of its creation in 'uid' */
```



```
...
ub1 *secret_data;
ub4 secret_data_len = 128001;
ub4 secret_data_type = 0;
secret_data = (ub1 *)malloc(secret_data_len*sizeof(ub1));

okvGetSecretData(env, &uid[0], &secret_data_type, &secret_data[0],
&secret_data_len);

if (okvErrGetNum(env))
{
    printf("Error while getting the secret data\n");
}

/* Free "secret_data" */
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.

- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.18 okvGetTemplate

`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.

Category

KMIP API

Purpose

`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.

The template is a list of attributes, which can be interpreted using the Oracle Key Vault utility or Oracle Key Vault KMIP extension functions. For the specified unique identifier of the template, the attributes of the template object are returned.

Syntax

```
OKVErrNo okvGetTemplate(OKVEnv *env, oratext *uid,
                       OKVTTLV **attrs_template);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier of the template (can be NULL for Batching).
<code>attrs_template</code>	OUT	Attributes of the template.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS</code> (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

For each create or register operation that uses retrieved attributes of the template object, `okvGetTemplate` should be used before that operation.

Example

```
/* Create a template for example and get its unique
   identifier as part of its creation in 'uid' */
...
OKVTTLV *template = (OKVTTLV *) NULL;
okvGetTemplate(env, uid, &template);

if (okvErrGetNum(env))
{
    printf("Error while getting the template\n");
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.

- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.19 okvLocate

`okvLocate` implements the KMIP Locate operation.

Category

KMIP API

Purpose

`okvLocate` implements the KMIP Locate operation.

The locate operation will look up all the objects in Oracle Key Vault that match the attributes specified in the `locate_attrs`.

Syntax

```
OKVErrNo okvLocate(OKVEnv *env,
                  ub4 uid_max, ub4 storage_status, OKVTTLV *locate_attrs,
                  ub4 *uid_cnt, oratext **uids);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid_max</code>	IN	Maximum number of unique identifiers expected.
<code>storage_status</code>	IN	Look for archived or online objects.
<code>locate_attrs</code>	IN	Attributes that define the locate search.
<code>uid_cnt</code>	OUT	Number of unique identifiers returned by the server.

Parameter	IN/OUT	Description
uids	OUT	Unique identifiers that match the locate attributes and storage status criteria.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The caller has to allocate sufficient memory for the unique identifiers `uids` returned by this function.

Prior to Oracle Key Vault 21.7 release, Oracle Key Vault server returned all the object unique identifiers that matched the conditions in the `Locate` operation request irrespective of whether the maximum number of requested items field (`uid_max`) are present or not in the request. Starting with Oracle Key Vault 21.7 release, the Oracle Key Vault server now supports the maximum Items field (`uid_max`) for `Locate` operation, that is only requested number (or up to maximum of '`uid_max`') of object Unique ID's is returned by the server. If you want to skip this field in the `locate` operation, then please use constant '`OKV_NO_MAX_ITEMS`' in place of '`uid_max`' parameter. As of today, Storage Status Mask (`storage_status`) field is not supported by the Oracle Key Vault server and hence any values passed into this field is not taken into account by the server during `locate` operation.

Example

```

/* Set up the environment handle 'env' and also the memory and connection
   management as shown in previous sections. Create a key with a name
   attribute value "MyNewKey" for example and get its unique
   identifier as part of its creation in 'uid'. Locate operation can be done as
   shown below. */
...
ub4      locate_count = 0;
ub4      uid_max = 1;
OKVTTLV *loc_attrs = (OKVTTLV *)NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;
oratext **locate_uids = (oratext **) malloc(uid_max * sizeof(oratext *));
ub4      itr = 0;

for (itr = 0; itr < uid_max; itr++)
{
    locate_uids[itr] = (oratext *) malloc(OKV_UNIQUE_ID_MAXLEN * sizeof(oratext));
}

loc_attrs = okvEnvGetOpRequestObj(env);
attr_in = okvAddAttributeObject(env, loc_attrs, OKVAttrName, (ub4) 0);

/* Add name attribute value to name attribute object */

```

```
okvAttrAddName(env, attr_in, (oratest *) "MyNewKey", strlen("MyNewKey"), 1);
okvLocate(env, uid_max, 1, loc_attrs, &locate_count, locate_uids);

if (okvErrGetNum(env))
{
    printf("Error while Locating the Key: MyNewKey\n");
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.

- [okvRekey](#)
okvRekey implements the KMIP Rekey operation.
- [okvRevoke](#)
okvRevoke implements the KMIP Revoke operation.

11.1.20 okvModifyAttribute

okvModifyAttribute implements the KMIP Modify attribute operation.

Category

KMIP API

Purpose

okvModifyAttribute implements the KMIP Modify attribute operation. It modifies an attribute of the KMIP Object specified by the unique identifier.

Syntax

```
OKVErrNo okvModifyAttribute(OKVEnv *env, oratext *uid,
                             OKVTTLV **attr);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
uid	IN	Unique identifier (can be NULL for batching).
attr	IN	Attribute of the KMIP object that needs to be modified.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
/* Create the KMIP object, say Key for example and get its unique identifier
   as part of its creation in 'uid', we can add an attribute and modify it
   as shown shown below */
```

```
OKVTTLV *templ = (OKVTTLV *) NULL;
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_temp = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *) NULL;
```

```
oratext *contact = (oratext *)"9123456789";
ub4      contactl = strlen((char *) contact);
oratext *new_contact = (oratext *)"abc.xyz@com";
ub4 new_contactl = strlen((char *) new_contact);
templ = okvEnvGetOpRequestObj(env);
attr_temp = okvAddAttributeObject(env, templ, OKVAttrContactInfo, (ub4) 0);

okvAttrAddContactInfo(env, attr_temp, contact, contactl);
okvAddAttribute(env, &uid[0], &attr_temp);

/* Now let's modify the contact info attribute */
req = okvEnvGetOpRequestObj(env);
attr_in = okvAddAttributeObject(env, req, OKVAttrContactInfo, (ub4) 0);
okvAttrAddContactInfo(env, attr_in, new_contact, new_contactl);
okvModifyAttribute(env, &uid[0], &attr_in);

if (okvErrGetNum(env))
{
    printf("Error while modifying the contact info attribute of the object\n");
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.

- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.21 okvQueryCapability

`okvQueryCapability` implements the KMIP Query operation.

Category

KMIP API

Purpose

`okvQueryCapability` implements the KMIP Query operation.

KMIP query operation returns the Oracle Key Vault server supported items such as KMIP operations, objects, server information. Items can also be retrieved one at a time. Query function specifies which items should be returned. The supported values of query functions are

- `OKVDEF_QUERY_OPERATIONS`
- `OKVDEF_QUERY_OBJECTS`
- `OKVDEF_QUERY_SERVER_INFO`

The count of the item not requested in the query function will be zero. If server information is not requested then `server_information` can be `NULL`.

Syntax

```
OKVErrNo okvQueryCapability(OKVEnv *env,  
                           ub4 query_function_cnt, ub4 *query_function,  
                           ub4 *operation_cnt, OKVOpsNo *operation,  
                           ub4 *object_type_cnt, OKVObjNo *object_type,  
                           OKVServerInformation *server_information);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
query_function_cnt	IN	Count of KMIP functions requested.
query_function	IN	KMIP functions requested.
operation_cnt	OUT	Count of KMIP operations supported.
operation	OUT	KMIP operations supported.
object_type_cnt	OUT	Count of KMIP managed objects supported.
object_type	OUT	KMIP managed objects supported.
server_information	OUT	Oracle Key Vault server specific information.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```

/* Set up the environment handle 'env' and also the memory and
   connection management as shown in previous sections. */
...
OKVServerInformation s;
ub4 query_function[1];
ub4 operation_cnt = 30;
OKVOpsNo operation[30];
ub4 object_type_cnt = 30;
OKVObjNo object_type[30];
query_function[0] = 3;

okvQueryCapability(env,1, query_function, &operation_cnt, operation,
                  &object_type_cnt, object_type, &s);

if (okvErrGetNum(env))
{
    printf("Error while executing okvQueryCapability");
}

```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.

- `okvRevoke`
`okvRevoke` implements the KMIP Revoke operation.

11.1.22 okvRegCertificate

`okvRegCertificate` implements the KMIP Register operation for the KMIP certificate object.

Category

KMIP API

Purpose

`okvRegCertificate` implements the KMIP Register operation for the KMIP certificate object.

The certificate of a specific type is registered with Oracle Key Vault Server. The unique identifier of the certificate object generated by the Oracle Key Vault server is returned as `oid`.

The maximum length of the unique ID for Oracle Key Vault SDK is defined by `OKV_UNIQUE_ID_MAXLEN`.

The new certificate being registered can take in additional attributes specified with the help of attributes or also with the template names. The attributes, and also the template names if specified, will be the template attribute added to KMIP register operation.

Syntax

```
OKVErrNo okvRegCertificate(OKVEnv *env,
                          ub4 certificate_type, ub4 certificate_subtype,
                          ub1 *certificate, ub4 certificatel,
                          ub4 mask, OKVTTLV *template_names_attrs,
                          oratext *private_key_uid,
                          ub4 private_key_uidl,
                          oratext *wallet_name, ub4 wallet_name1,
                          oratext *oid, ub4 *oidl);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>certificate_type</code>	IN	Certificate type.
<code>certificate_subtype</code>	IN	Certificate sub-type.
<code>certificate</code>	IN	Certificate.
<code>certificatel</code>	IN	Certificate length.
<code>mask</code>	IN	Cryptographic usage mask of the certificate.
<code>template_names_attrs</code>	IN	Template names or attributes that will form the template-attribute.
<code>private_key_uid</code>	IN	Unique identifier of the private key associated with the certificate (optional).
<code>private_key_uidl</code>	IN	Unique identifier length of the private key associated with the certificate (optional).
<code>wallet_name</code>	IN	Wallet name value.

Parameter	IN/OUT	Description
wallet_name1	IN	Length of the wallet name value.
oid	OUT	Unique identifier of the registered certificate.
oid1	OUT	Unique identifier length of the registered certificate.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

It is recommended to add a KMIP name attribute to certificate object to help identify it in future.

The caller has to allocate the memory for the unique identifier returned by this function. The length of allocated memory is passed in via the length of the unique identifier argument `oid1`. Sufficient memory to store the returned unique identifier should be allocated.

The certificate being registered can optionally be associated with a private key by providing the UID of the private key (`private_key_uid`). Validate the existence of `private_key_uid` by performing a locate operation (using `okvLocate` API) before passing it as an argument to this API.

Allowed values of the `certificate_subtype` argument:

- `OKV_CERT_SUBTYPE_USER_CERT`: represents User Certificate.
- `OKV_CERT_SUBTYPE_TRUSTPOINT`: represents Trustpoint.

The certificate is registered with Oracle Key Vault server in wallet `wallet_name` if specified else it is registered in the default wallet if present with the endpoint.

If `mask` is set to zero 0, then a default value of certificate's cryptographic usage mask (`verify`) is assigned during certificate registration.

Example

```
/* X.509 Certificate type */
ub4    cert_type = OKVDEF_CERT_TYPE_X509;

/* Certificate Subtype */
ub4    cert_subtype = OKV_CERT_SUBTYPE_USER_CERT;

/* Usage mask */
ub4    cert_mask = CRYPTO_MASK_VERIFY;
```

```

ub1      cert[] = "-----BEGIN CERTIFICATE-----
MIIEvQIBADANBgkqhkiG9w0BAQE.....
-----END CERTIFICATE-----";
ub4      certl = strlen((const char *)cert);
oratext  uid[OKV_UNIQUE_ID_MAXLEN + 1];
ub4      uidl = sizeof(uid);
OKVTTLV *template = (OKVTTLV *)NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;

/* Set up the environment handle 'env' and also the memory and
   connection management as shown in previous sections */
memset(uid, 0, uidl);
template = okvEnvGetOpRequestObj(env);

/* Add name attribute object to request handle */
attr_in = okvAddAttributeObject(env, template, OKVAttrName, (ub4) 0);

/* Add name attribute value to name attribute object */
okvAttrAddName(env, attr_in, (oratext *)"My Certificate for Register operation",
               strlen("My Certificate for Register operation"), 1);

okvRegCertificate(env, cert_type, cert_subtype,
                  cert, certl,
                  cert_mask, template,
                  (oratext *)NULL, (ub4)0,
                  OKV_NO_WALLET, OKV_NO_WALLET_LEN,
                  uid, &uidl);

uid[*uidl] = '\0';

if (okvErrGetNum(env))
{
    printf("Error while registering the certificate\n");
}

```

Related Topics

- [okvActivate](#)
okvActivate implements the KMIP Activate operation.
- [okvAddAttribute](#)
okvAddAttribute implements the KMIP Add attribute operation.
- [okvCreateKey](#)
okvCreateKey implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
okvDeleteAttribute implements the KMIP Delete attribute operation.
- [okvDestroy](#)
okvDestroy implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
okvGetAttributeList implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
okvGetAttributes implements KMIP Get attribute operation.
- [okvGetCertificate](#)
okvGetCertificate implements the KMIP Get operation for the Certificate object.

- [okvGetCertificateRequest](#)
`okvGetCertificateRequest` implements the KMIP Get operation for the Certificate request object.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetPrivateKey](#)
`okvGetPrivateKey` implements the KMIP Get operation for the KMIP private key object.
- [okvGetPublicKey](#)
`okvGetPublicKey` implements the KMIP Get operation for the KMIP public key object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegCertificateRequest](#)
`okvRegCertificateRequest` implements the KMIP Register operation for the certificate request object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegPrivateKey](#)
`okvRegPrivateKey` implements the KMIP Register operation for the KMIP private key object.
- [okvRegPublicKey](#)
`okvRegPublicKey` implements the KMIP Register operation for the KMIP public key object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.

- [okvRegKey](#)
okvRegKey implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRevoke](#)
okvRevoke implements the KMIP Revoke operation.

11.1.23 okvRegCertificateRequest

okvRegCertificateRequest implements the KMIP Register operation for the certificate request object.

Category

KMIP API

Purpose

okvRegCertificateRequest implements the KMIP Register operation for the certificate request object.

The certificate request object is registered as an opaque object with Oracle Key Vault Server. The unique identifier of the certificate request object generated by the Oracle Key Vault server is returned as `oid`.

The maximum length of the unique ID for Oracle Key Vault SDK is defined by `OKV_UNIQUE_ID_MAXLEN`.

The new certificate request being registered can take in additional attributes specified with the help of attributes or also with the template names. The attributes, and also the template names if specified, will be the template attribute added to KMIP register operation.

Syntax

```
OKVErrNo okvRegCertificateRequest(OKVEnv *env,
    ub4 certificate_request_type,
    ub1 *certificate_request,
    ub4 certificate_requestl,
    OKVTTLV *template_names_attrs,
    oratext *private_key_uid,
    ub4 private_key_uidl,
    oratext *wallet_name, ub4 wallet_name_l,
    oratext *oid, ub4 *oidl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
certificate_request_type	IN	Certificate request type.
certificate_request	IN	Certificate request.
certificate_requestl	IN	Certificate request length.
template_names_attrs	IN	Template names or attributes that will form the template-attribute.

Parameter	IN/OUT	Description
private_key_uid	IN	Unique identifier of the private key associated with the certificate request (mandatory).
private_key_uidl	IN	Unique identifier length of the private key associated with the certificate request (mandatory).
wallet_name	IN	Wallet name value.
wallet_name_l	IN	Length of the wallet name value.
oid	OUT	Unique identifier of the registered certificate request.
oidl	OUT	Unique identifier length of the registered certificate request.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

It is recommended to add a KMIP name attribute to certificate request object to help identify it in future.

The caller has to allocate the memory for the unique identifier returned by this function. The length of allocated memory is passed in via the length of the unique identifier argument `oidl`. Sufficient memory to store the returned unique identifier should be allocated.

The certificate request being registered should be associated with a private key by providing the UID of the private key (`private_key_uid`). Validate the existence of `private_key_uid` by performing a locate operation (using `okvLocate` API) before passing it as an argument to this API.

The certificate request is registered with Oracle Key Vault server in wallet `wallet_name` if specified else it is registered in the default wallet if present with the endpoint.

Example

```
/* Certificate Request type */
ub4 cert_req_type = OKVDEF_CERT_REQ_TYPE_PEM;
ub1 cert_req[] = "-----BEGIN CERTIFICATE REQUEST-----
MIIEvQIBADANBgkqhkiG9w0BAQE.....
-----END CERTIFICATE REQUEST-----";
ub4 cert_req_l = strlen((const char *)cert_req);
```

```
oratest uid[OKV_UNIQUE_ID_MAXLEN + 1];
ub4     uidl = sizeof(uid);
OKVTTLV *template = (OKVTTLV *)NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;

/* Please make sure to pass a valid Private Key UID */
oratest *private_key_uid = "64281937-768D-4F78-BF39-EBD5985BFAB2";
ub4     private_key_uidl = strlen((const char *)private_key_uid);

/* Set up the environment handle 'env' and also the memory and
   connection management as shown in previous sections */
memset(uid, 0, uidl);
template = okvEnvGetOpRequestObj(env);

/* Add name attribute object to request handle */
attr_in = okvAddAttributeObject(env, template, OKVAttrName, (ub4) 0);

/* Add name attribute value to name attribute object */
okvAttrAddName(env, attr_in, (oratest *)"My Certificate Request for Register
operation",
               strlen("My Certificate Request for Register operation"), 1);

okvRegCertificateRequest(env, cert_req_type,
                        cert_req, cert_reql, template,
                        private_key_uid, private_key_uidl,
                        OKV_NO_WALLET, OKV_NO_WALLET_LEN,
                        uid, &uidl);

uid[*uidl] = '\0';

if (okvErrGetNum(env))
{
    printf("Error while registering the certificate request\n");
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetCertificate](#)
`okvGetCertificate` implements the KMIP Get operation for the Certificate object.

- [okvGetCertificateRequest](#)
`okvGetCertificateRequest` implements the KMIP Get operation for the Certificate request object.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetPrivateKey](#)
`okvGetPrivateKey` implements the KMIP Get operation for the KMIP private key object.
- [okvGetPublicKey](#)
`okvGetPublicKey` implements the KMIP Get operation for the KMIP public key object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegCertificate](#)
`okvRegCertificate` implements the KMIP Register operation for the KMIP certificate object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegPrivateKey](#)
`okvRegPrivateKey` implements the KMIP Register operation for the KMIP private key object.
- [okvRegPublicKey](#)
`okvRegPublicKey` implements the KMIP Register operation for the KMIP public key object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.

- [okvRegKey](#)
okvRegKey implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRevoke](#)
okvRevoke implements the KMIP Revoke operation.

11.1.24 okvRegOpaqueData

okvRegOpaqueData implements the KMIP Register operation for the KMIP opaque data object.

Category

KMIP API

Purpose

okvRegOpaqueData implements the KMIP register operation for the KMIP opaque data object.

The opaque data is a byte string. A text file, text string, binary file, or key can also be uploaded as an opaque data.

The unique identifier of the opaque data object created in the Oracle Key Vault server for the registered opaque data is returned as `oid`.

The maximum length of the unique ID for Oracle Key Vault SDK is defined by `OKV_UNIQUE_ID_MAXLEN`.

The new opaque data created can take in additional attributes specified with the help of attributes or also with the template names. The attributes, and also the template names if specified, will be the template attribute added to KMIP Register operation.

Syntax

```
OKVErrNo okvRegOpaqueData(OKVEnv *env,
                          ub4 opaque_data_type, ub1 *opaque_data,
                          ub4 opaque_data1,
                          OKVTTLV *template_names_attrs,
                          oratext *wallet_name, ub4 wallet_name1,
                          oratext *oid, ub4 *oid1);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>opaque_data_type</code>	IN	Type of opaque object being registered.
<code>opaque_data</code>	IN	Opaque object being registered.
<code>opaque_data1</code>	IN	Length of opaque object being registered.
<code>template_names_attrs</code>	IN	Template names or attributes that will form the template-attribute.
<code>wallet_name</code>	IN	Wallet name value.
<code>wallet_name1</code>	IN	Length of the wallet name value.
<code>oid</code>	OUT	Unique identifier of the registered opaque object.
<code>oid1</code>	OUT	Unique identifier length of the registered opaque object.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

It is recommended to add a KMIP name attribute to opaque data object to help identify it in future.

The caller has to allocate the memory for the unique identifier returned by this function. The length of allocated memory is passed in via the length of the unique identifier argument `oidl`. Sufficient memory to store the returned unique identifier should be allocated.

An opaque data of a specific type is registered with Oracle Key Vault server in wallet `wallet_name` if specified else it is registered in the default wallet if present with the endpoint. The size of the opaque data is limited by the maximum size of the object handled by the Oracle Key Vault server.

Example

```
oratext *opaque_data = (oratext *)"MyNewData";
ub4 opaque_data1 = strlen("MyNewData");
oratext uid[OKV_UNIQUE_ID_MAXLEN + 1];
ub4      uid1 = sizeof(uid);

/* Set up the environment handle 'env' and also the memory and
   connection management as shown in previous sections */
memset(uid, 0, uid1);

/* Register Opaque Data */
printf("\tRegistering opaque data\n");

okvRegOpaqueData(env, OKVDEF_TAG_OPAQUE_DATA_TYPE,
                 opaque_data, opaque_data1,
                 (OKVTTLV *)NULL, (oratext *)NULL, (ub4)0,
                 &uid[0], uid1);

if (okvErrGetNum(env))
{
    printf("Error while registering the opaque data\n");
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.

- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.25 okvRegKey

`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.

Category

KMIP API

Purpose

`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.

The unique identifier of the symmetric key object created by the Oracle Key Vault server is returned as `oid`.

The maximum length of the unique ID for Oracle Key Vault SDK is defined by `OKV_UNIQUE_ID_MAXLEN`.

The new key created can take in additional attributes specified with the help of attributes or also with the template names. The attributes, and also the template names if specified, will be the template attribute added to KMIP register operation.

Syntax

```
OKVErrNo okvRegKey(OKVEnv *env,
                  OKVType key_alg, ub4 key_len, ub1 *key, ub4 keyl,
                  ub4 mask, OKVTTLV *template_names_attrs,
                  oratext *wallet_name, ub4 wallet_name1,
                  oratext *oid, ub4 *oidl);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>key_alg</code>	IN	Symmetric key algorithm.
<code>key_len</code>	IN	Key length of the symmetric key.
<code>key</code>	IN	Symmetric key.
<code>keyl</code>	IN	Symmetric key length.
<code>mask</code>	IN	Cryptographic usage mask of the symmetric key.
<code>template_names_attrs</code>	IN	Template names or attributes that will form the template-attribute.
<code>wallet_name</code>	IN	Wallet name value.
<code>wallet_name1</code>	IN	Length of the wallet name value.
<code>oid</code>	OUT	Unique identifier of the registered key.
<code>oidl</code>	OUT	Unique identifier length of the registered key.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

It is recommended to add a KMIP name attribute to symmetric key object to help identify it in future.

The caller has to allocate the memory for the unique identifier returned by this function. The length of allocated memory is passed in via the length of the unique identifier argument `uidl`. Sufficient memory to store the returned unique identifier should be allocated.

A symmetric key of the specified length for a specified algorithm and use (cryptographic usage mask) is registered with Oracle Key Vault server in wallet `wallet_name` if specified else it is registered in the default wallet if present with the endpoint.

If `mask` is set to zero 0, then a default value of symmetric key's cryptographic usage mask (encrypt, decrypt, wrap_key, and unwrap_key) is assigned during symmetric key registration.

Example

```
/* Tag for Cryptographic Algorithm AES */
OKVType  algo = CRYPTO_ALG_AES;

/* Key length 128, because AES keys are 128, 192 or 256 bits in length*/
ub4      key_len = 128;
ub4      usage_mask = CRYPTO_MASK_ENCRYPT | CRYPTO_MASK_DECRYPT;

/* Key */
ub1      key[] = "770A8A65DA156D24";

/* Length of symmetric key */
ub4      keyl = strlen((const char *)key);
oracext  uid[OKV_UNIQUE_ID_MAXLEN + 1];
ub4      uidl = sizeof(uid);
OKVTTLV *template = (OKVTTLV *)NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;

/* Set up the environment handle 'env' and also the memory
   and connection management as shown in previous sections */
memset(uid, 0, uidl);
template = okvEnvGetOpRequestObj(env);

/* Add name attribute object to request handle */
attr_in = okvAddAttributeObject(env, template, OKVAttrName, (ub4) 0);

/* Add name attribute value to name attribute object */
okvAttrAddName(env, attr_in, (oracext *)"My Key for Register operation",
               strlen("My Key for Register operation"), 1);
okvRegKey(env, algo, key_len, &key[0], keyl, usage_mask, template,
          (oracext *)NULL, (ub4)0, uid, &uidl);

if (okvErrGetNum(env))
{
    printf("Error while registering the key\n");
}
```

Related Topics

- [okvActivate](#)
okvActivate implements the KMIP Activate operation.

- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.26 okvRegPrivateKey

`okvRegPrivateKey` implements the KMIP Register operation for the KMIP private key object.

Category

KMIP API

Purpose

`okvRegPrivateKey` implements the KMIP Register operation for the KMIP private key object.

The unique identifier of the private key object registered by the Oracle Key Vault server is returned as `oid`. The maximum length of the unique ID for Oracle Key Vault SDK is defined by `OKV_UNIQUE_ID_MAXLEN`.

The new private key being registered can take in additional attributes specified with the help of attributes or also with the template names. The attributes, and also the template names if specified, will be the template attribute added to KMIP register operation.

Syntax

```
OKVErrNo okvRegPrivateKey(OKVEnv *env,
                          OKVType private_key_alg, ub4 private_key_len,
                          ub1 *private_key, ub4 private_keyl,
                          ub4 mask, OKVTTLV *template_names_attrs,
                          oratext *wallet_name, ub4 wallet_name1,
                          oratext *oid, ub4 *oidl);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>private_key_alg</code>	IN	Private key algorithm.
<code>private_key_len</code>	IN	Key length of the private key.
<code>private_key</code>	IN	Private key.
<code>private_keyl</code>	IN	Private key length.
<code>mask</code>	IN	Cryptographic usage mask of the private key.
<code>template_names_attrs</code>	IN	Template names or attributes that will form the template-attribute.
<code>wallet_name</code>	IN	Wallet name value.
<code>wallet_name1</code>	IN	Length of the wallet name value.
<code>oid</code>	OUT	Unique identifier of the registered private key.
<code>oidl</code>	OUT	Unique identifier length of the registered private key.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

It is recommended to add a KMIP name attribute to private key object to help identify it in future.

The caller has to allocate the memory for the unique identifier returned by this function. The length of allocated memory is passed in via the length of the unique identifier argument `oidl`. Sufficient memory to store the returned unique identifier should be allocated.

A private key of the specified length for a specified algorithm and use (cryptographic usage mask) is registered with Oracle Key Vault server in wallet `wallet_name` if specified else it is registered in the default wallet if present with the endpoint.

If `mask` is set to zero 0, then a default value of private key's cryptographic usage mask (sign, decrypt, wrap_key, and unwrap_key) is assigned during its registration.

Example

```

/* Key Algorithm */
OKVType private_key_algo = CRYPTO_ALG_RSA;

/* Key Size */
ub4 private_key_len = 2048;
ub1 private_key[] = "45687942323587.....";
ub4 private_keyl = strlen((const char *)private_key);

/* Usage mask */
ub4 private_key_mask = CRYPTO_MASK_DECRYPT;
oratext uid[OKV_UNIQUE_ID_MAXLEN + 1];
ub4 uidl = sizeof(uid);
OKVTTLV *template = (OKVTTLV *)NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;

/* Set up the environment handle 'env' and also the memory and
connection management as shown in previous sections */
memset(uid, 0, uidl);
template = okvEnvGetOpRequestObj(env);

/* Add name attribute object to request handle */
attr_in = okvAddAttributeObject(env, template, OKVAttrName, (ub4) 0);

/* Add name attribute value to name attribute object */
okvAttrAddName(env, attr_in, (oratext *)"My Private Key for Register operation",
strlen("My Private Key for Register operation"), 1);

```

```
okvRegPrivateKey(env, private_key_algo, private_key_len,  
                private_key, private_keyl,  
                private_key_mask, template,  
                OKV_NO_WALLET, OKV_NO_WALLET_LEN,  
                uid, &uidl);  
  
uid[*uidl] = '\0';  
  
if (okvErrGetNum(env))  
{  
    printf("Error while registering the private key\n");  
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetCertificate](#)
`okvGetCertificate` implements the KMIP Get operation for the Certificate object.
- [okvGetCertificateRequest](#)
`okvGetCertificateRequest` implements the KMIP Get operation for the Certificate request object.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetPrivateKey](#)
`okvGetPrivateKey` implements the KMIP Get operation for the KMIP private key object.
- [okvGetPublicKey](#)
`okvGetPublicKey` implements the KMIP Get operation for the KMIP public key object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.

- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegCertificate](#)
`okvRegCertificate` implements the KMIP Register operation for the KMIP certificate object.
- [okvRegCertificateRequest](#)
`okvRegCertificateRequest` implements the KMIP Register operation for the certificate request object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegPublicKey](#)
`okvRegPublicKey` implements the KMIP Register operation for the KMIP public key object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.27 `okvRegPublicKey`

`okvRegPublicKey` implements the KMIP Register operation for the KMIP public key object.

Category

KMIP API

Purpose

`okvRegPublicKey` implements the KMIP Register operation for the KMIP public key object.

The unique identifier of the public key object registered by the Oracle Key Vault server is returned as `oid`.

The maximum length of the unique ID for Oracle Key Vault SDK is defined by `OKV_UNIQUE_ID_MAXLEN`.

The new public key being registered can take in additional attributes specified with the help of attributes or also with the template names. The attributes, and also the template names if specified, will be the template attribute added to KMIP register operation.

Syntax

```
OKVErrNo okvRegPublicKey(OKVEnv *env,
                        OKVType public_key_alg, ub4 public_key_len,
                        ub1 *public_key, ub4 public_keyl,
                        ub4 mask, OKVTTLV *template_names_attrs,
                        oratext *private_key_uid, ub4 private_key_uidl,
                        oratext *wallet_name, ub4 wallet_name_l,
                        oratext *oid, ub4 *oidl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
public_key_alg	IN	Public key algorithm.
public_key_len	IN	Key length of the public key.
public_key	IN	Public key.
public_keyl	IN	Public key length.
mask	IN	Cryptographic usage mask of the public key.
template_names_attrs	IN	Template names or attributes that will form the template-attribute.
private_key_uid	IN	Unique identifier of the private key associated with the public key (optional).
private_key_uidl	IN	Unique identifier length of the private key associated with the public key (optional).
wallet_name	IN	Wallet name value.
wallet_name_l	IN	Length of the wallet name value.
oid	OUT	Unique identifier of the registered public key.
oidl	OUT	Unique identifier length of the registered public key.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: <code>OKV_SUCCESS</code> (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

It is recommended to add a KMIP name attribute to public key object to help identify it in future.

The caller has to allocate the memory for the unique identifier returned by this function. The length of allocated memory is passed in via the length of the unique identifier argument `uid1`. Sufficient memory to store the returned unique identifier should be allocated.

A public key of the specified length for a specified algorithm and use (cryptographic usage mask) is registered with Oracle Key Vault server in wallet `wallet_name` if specified else it is registered in the default wallet if present with the endpoint.

The public key being registered can be optionally associated with a private key by providing the UID of the private key (`private_key_uid`). Validate the existence of `private_key_uid` by performing a locate operation (using `okvLocate` API) before passing it as an argument to this API.

If `mask` is set to zero 0, then a default value of public key's cryptographic usage mask (verify, encrypt, and unwrap_key) is assigned during its registration.

Example

```

/* Key Algorithm */
OKVType  public_key_algo = CRYPTO_ALG_RSA;

/* Key Size */
ub4      public_key_len = 2048;
ub1      public_key[] = "7698767245345566789823428.....";
ub4      public_keyl = strlen((const char *)public_key);

/* Usage mask */
ub4      public_key_mask = CRYPTO_MASK_ENCRYPT;
oratext  uid[OKV_UNIQUE_ID_MAXLEN + 1];
ub4      uid1 = sizeof(uid);
OKVTTLV *template = (OKVTTLV *)NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;

/* Set up the environment handle 'env' and also the memory and
   connection management as shown in previous sections */
memset(uid, 0, uid1);
template = okvEnvGetOpRequestObj(env);

/* Add name attribute object to request handle */
attr_in = okvAddAttributeObject(env, template, OKVAttrName, (ub4) 0);

/* Add name attribute value to name attribute object */
okvAttrAddName(env, attr_in, (oratext *)"My Public Key for Register operation",
               strlen("My Public Key for Register operation"), 1);

okvRegPublicKey(env, public_key_algo, public_key_len,
                public_key, public_keyl,
                public_key_mask, template,
                (oratext *)NULL, (ub4)0,
                OKV_NO_WALLET, OKV_NO_WALLET_LEN,
                uid, &uid1);

uid[*uid1] = '\0';

```

```
if (okvErrGetNum(env))
{
    printf("Error while registering the public key\n");
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetCertificate](#)
`okvGetCertificate` implements the KMIP Get operation for the Certificate object.
- [okvGetCertificateRequest](#)
`okvGetCertificateRequest` implements the KMIP Get operation for the Certificate request object.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetPrivateKey](#)
`okvGetPrivateKey` implements the KMIP Get operation for the KMIP private key object.
- [okvGetPublicKey](#)
`okvGetPublicKey` implements the KMIP Get operation for the KMIP public key object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.

- [okvRegCertificate](#)
`okvRegCertificate` implements the KMIP Register operation for the KMIP certificate object.
- [okvRegCertificateRequest](#)
`okvRegCertificateRequest` implements the KMIP Register operation for the certificate request object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegPrivateKey](#)
`okvRegPrivateKey` implements the KMIP Register operation for the KMIP private key object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.28 okvRegSecretData

`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.

Category

KMIP API

Purpose

`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.

Secret data is usually a password or a string.

The unique identifier of the secret data object created in the Oracle Key Vault server for the registered secret data is returned as `oid`.

The maximum length of the unique ID for Oracle Key Vault SDK is defined by `OKV_UNIQUE_ID_MAXLEN`.

The new secret data created can take in additional attributes specified with the help of attributes or also with the template names. The attributes, and also the template names if specified, will be the template attribute added to KMIP register operation.

Syntax

```
OKVErrNo okvRegSecretData(OKVEnv *env,
                          ub4 secret_data_type, ub1 *secret_data,
                          ub4 secret_data1, ub4 mask,
                          OKVTTLV *template_names_attrs,
                          oratext *wallet_name, ub4 wallet_name1,
                          oratext *oid, ub4 *oid1);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
secret_data_type	IN	Type of secret data being registered.
secret_data	IN	Secret data being registered.
secret_data1	IN	Length of secret data being registered.
mask	IN	Cryptographic usage mask of the secret.
template_names_attrs	IN	Template names or attributes that will form the template-attribute.
wallet_name	IN	Wallet name value.
wallet_name1	IN	Length of the wallet name value.
oid	OUT	Unique identifier of the registered secret data.
oid1	OUT	Unique identifier length of the registered secret data.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

It is recommended to add a KMIP name attribute to secret data object to help identify it in future.

The caller has to allocate the memory for the unique identifier returned by this function. The length of allocated memory is passed in via the length of the unique identifier (`oid1`) argument. Sufficient memory to store the returned unique identifier should be allocated.

A secret data of a specific type is registered with Oracle Key Vault server in wallet (`wallet_name`) if specified else it is registered in the default wallet if present with the endpoint.

The size of the secret data is limited by the maximum size of the object handled by the Oracle Key Vault server.

If `mask` is set to zero 0, then a default value of secret data cryptographic usage mask (`derive_key`) is assigned during its registration.

Example

```
/* Parameters for registering secret data */
/* Tag for secret data type */
OKVType   type = OKVDEF_SECRET_DATA_TYPE_PASSWORD;
ub4       usage_mask = CRYPTO_MASK_DERIVE_KEY;
oracext   *secret = (oracext *)"MyNewSecret";
ub4       secretl = strlen("MyNewSecret");
oracext   uid[OKV_UNIQUE_ID_MAXLEN + 1];
ub4       uidl = sizeof(uid);

/* Set up the environment handle 'env' and also the memory and
   connection management as shown in previous sections */
memset(uid, 0, uidl);

/* Register Secret data */
printf("\tRegistering the secret data\n");

okvRegSecretData(env, type, secret, secretl,
                 usage_mask, (OKVTTLV *)NULL,
                 (oracext *)NULL, (ub4)0,
                 &uid[0], uidl);

if (okvErrGetNum(env))
{
    printf("Error while registering the secret data\n");
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.

- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.29 okvRegTemplate

`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.

Category

KMIP API

Purpose

`okvRegTemplate` implements the KMIP Register operation for the KMIP template object (not to be confused with KMIP template-attribute object).

A template object is a collection of attributes.

The unique identifier of the template object created with the specified attributes in Oracle Key Vault for the registered template is returned as `oid`.

The maximum length of the unique identifier for Oracle Key Vault SDK is defined by `OKV_UNIQUE_ID_MAXLEN`.

Syntax

```
OKVErrNo okvRegTemplate(OKVEnv *env,  
                        OKVTTLV *attrs_template,  
                        oratext *wallet_name, ub4 wallet_name_l,  
                        oratext *oid, ub4 *oid_l);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
attrs_template	IN	Attributes of the template.
wallet_name	IN	Wallet name value.
wallet_name1	IN	Length of the wallet name value.
oid	OUT	Unique identifier of the registered template.
oid1	OUT	Unique identifier length of the registered template.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The caller has to allocate the memory for the unique identifier returned by this function. The length of allocated memory is passed in via the length of the unique identifier (`oid1`) argument. Sufficient memory to store the returned unique identifier should be allocated.

The template will be registered with the wallet specified in `wallet_name` argument else it will be registered with the default wallet associated with the endpoint in case the default wallet exists.

Example

```
oratest uid[OKV_UNIQUE_ID_MAXLEN + 1];
ub4     uid1 = sizeof(uid);

/* Set up the environment handle 'env' also the memory and connection
   management as shown in previous sections */
memset(uid, 0, uid1);
okvRegTemplate(env, (OKVTTLV *)NULL, (oratest *)NULL, (ub4)0, &uid[0], &uid1);

if (okvErrGetNum(env))
{
    printf("Error while registering the Template\n");
}
```

Related Topics

- [okvActivate](#)
okvActivate implements the KMIP Activate operation.
- [okvAddAttribute](#)
okvAddAttribute implements the KMIP Add attribute operation.

- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.
- [okvRevoke](#)
`okvRevoke` implements the KMIP Revoke operation.

11.1.30 `okvRekey`

`okvRekey` implements the KMIP Rekey operation.

Category

KMIP API

Purpose

`okvRekey` implements the KMIP Rekey operation.

The rekey operation requires the unique identifier of the symmetric key that needs to be re-keyed. Most of the attributes are carried over from the old key. Some attributes are modified per KMIP defined rules.

The unique identifier of the new symmetric key object generated by the Oracle Key Vault server is returned as `oid`.

The maximum length of the unique ID for Oracle Key Vault SDK is defined by `OKV_UNIQUE_ID_MAXLEN`.

Syntax

```
OKVErrNo okvRekey(OKVEnv *env, oratext *uid,
                  ub4 offset, OKVTTLV *template_names_attrs,
                  oratext *oid, ub4 *oidl);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier of the key being rekeyed (can be NULL for Batching).
<code>offset</code>	IN	Time interval between initialization (creation) date and activation date.
<code>template_names_attrs</code>	IN	Template names or attributes that will form the template-attribute for rekey.
<code>oid</code>	OUT	Unique identifier of the newly generated symmetric key.
<code>oidl</code>	OUT	Unique identifier length of the newly generated symmetric key.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The caller has to allocate the memory for the unique identifier of the new symmetric key returned by this function. The length of allocated memory is passed in via the length of the unique identifier (`oidl`) argument.

Prior to Oracle Key Vault release 21.7, rekey operation was allowed more than once on the same key. Starting with Oracle Key Vault release 21.7, rekey operation is allowed only once on a given key.

The API has the below exception when used with Oracle Key Vault server:

- If a template is passed for rekey, the template attributes are not added for the new key. As a workaround, this can be added post rekey using `okvAddAttribute`.

Example

```
/* Set up the environment handle 'env' and also the memory and
   connection management as shown in previous sections. Create
   a key for example and get its unique identifier as part of
   its creation in 'uid'. Rekey can done as shown below */
...
oratest rekey_uid[OKV_UNIQUE_ID_MAXLEN + 1];
ub4     rekey_uidl = sizeof(rekey_uid);

memset(rekey_uid, 0, rekey_uidl);
okvRekey(env, uid, (ub4)0, (OKVTTLV *)NULL, &rekey_uid[0], &rekey_uidl);

if (okvErrGetNum(env))
{
    printf("Error while Re-Keying the Key\n");
}
```

Related Topics

- [okvActivate](#)
`okvActivate` implements the KMIP Activate operation.
- [okvAddAttribute](#)
`okvAddAttribute` implements the KMIP Add attribute operation.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
`okvDeleteAttribute` implements the KMIP Delete attribute operation.
- [okvDestroy](#)
`okvDestroy` implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
`okvGetAttributeList` implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
`okvGetAttributes` implements KMIP Get attribute operation.
- [okvGetKey](#)
`okvGetKey` implements the KMIP Get operation for the KMIP symmetric key object.
- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.

- [okvLocate](#)
okvLocate implements the KMIP Locate operation.
- [okvModifyAttribute](#)
okvModifyAttribute implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
okvQueryCapability implements the KMIP Query operation.
- [okvRegKey](#)
okvRegKey implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
okvRegOpaqueData implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
okvRegSecretData implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
okvRegTemplate implements the KMIP Register operation for the KMIP template object.
- [okvRevoke](#)
okvRevoke implements the KMIP Revoke operation.

11.1.31 okvRevoke

okvRevoke implements the KMIP Revoke operation.

Category

KMIP API

Purpose

okvRevoke implements the KMIP Revoke operation. It revokes the KMIP object specified by the unique identifier with a revocation reason and the date when the object was compromised.

Syntax

```
OKVErrNo okvRevoke(OKVEnv *env, oratext *uid,
                  ub4 revocation_reason,
                  oratext *revocation_msg,
                  ub8 comp_occurrence_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
uid	IN	Unique identifier (can be NULL for batching).
revocation_reason	IN	Revocation reason for revoking the KMIP object.

Parameter	IN/OUT	Description
revocation_msg	IN	Revocation message for revoking the KMIP object.
comp_occurrence_date	IN	Date when the KMIP object compromise occurred.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
/* Create the KMIP object, say Key for example and get its unique identifier
   as part of its creation in 'uid', activate it and then revoke it as below */

okvRevoke(env, &uid[0], (ub4)1, (oratest *)"Retiring the key",
          (ub8)time((time_t *)NULL));

if (okvErrGetNum(env))
{
    printf("Error while revoking the object\n");
}
```

Related Topics

- [okvActivate](#)
okvActivate implements the KMIP Activate operation.
- [okvAddAttribute](#)
okvAddAttribute implements the KMIP Add attribute operation.
- [okvCreateKey](#)
okvCreateKey implements the KMIP Create operation for the KMIP symmetric key object.
- [okvDeleteAttribute](#)
okvDeleteAttribute implements the KMIP Delete attribute operation.
- [okvDestroy](#)
okvDestroy implements the KMIP Destroy operation.
- [okvGetAttributeList](#)
okvGetAttributeList implements KMIP Get attribute list operation.
- [okvGetAttributes](#)
okvGetAttributes implements KMIP Get attribute operation.
- [okvGetKey](#)
okvGetKey implements the KMIP Get operation for the KMIP symmetric key object.

- [okvGetOpaqueData](#)
`okvGetOpaqueData` implements the KMIP Get operation for the KMIP opaque data object.
- [okvGetSecretData](#)
`okvGetSecretData` implements the KMIP Get operation for the KMIP secret data object.
- [okvGetTemplate](#)
`okvGetTemplate` implements the KMIP Get operation for the KMIP template object.
- [okvLocate](#)
`okvLocate` implements the KMIP Locate operation.
- [okvModifyAttribute](#)
`okvModifyAttribute` implements the KMIP Modify attribute operation.
- [okvQueryCapability](#)
`okvQueryCapability` implements the KMIP Query operation.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvRegOpaqueData](#)
`okvRegOpaqueData` implements the KMIP Register operation for the KMIP opaque data object.
- [okvRegSecretData](#)
`okvRegSecretData` implements the KMIP Register operation for the KMIP secret data object.
- [okvRegTemplate](#)
`okvRegTemplate` implements the KMIP Register operation for the KMIP template object.
- [okvRekey](#)
`okvRekey` implements the KMIP Rekey operation.

11.1.32 okvSign

`okvSign` implements the KMIP Sign operation.

Category

KMIP API

Purpose

`okvSign` performs the sign operation on the provided data using a KMIP object.

Syntax

```
OKVErrNo okvSign(OKVEnv *env, oratext *uid,  
                ub1 *data, ub4 data1, ub4 data_type,  
                OKVCryptoContext *crypto_context,  
                OKVSignResponse *sign_response);
```

Parameters

Table 11-1 Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
uid	IN	Unique identifier (can be NULL for batching).
data	IN	Data to be signed.
data1	IN	Length of the data to be signed.
data_type	IN	Type of the data to be signed, either <code>OKV_DATA_TYPE_RAW</code> or <code>OKV_DATA_TYPE_DIGEST</code> .
crypto_context	IN	Cryptographic context contains required parameters for signing like the cryptographic algorithm and hashing algorithm.
sign_response	OUT	Contains the sign operation response details.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

`crypto_context` can be created and freed using `okvCryptoContextCreate` and `okvCryptoContextFree` helper APIs. It contains the required parameters for signing and the user will need to set it explicitly by making use of helper APIs like `okvCryptoContextSetCryptoAlgo`, `okvCryptoContextSetHashingAlgo`, `okvCryptoContextSetPadding`, and `okvCryptoContextSetDigitalSignAlgo`. The user can also get the respective parameter values that was set in `crypto_context` using helper APIs `okvCryptoContextGetCryptoAlgo`, `okvCryptoContextGetHashingAlgo`, `okvCryptoContextGetPadding`, and `okvCryptoContextGetDigitalSignAlgo`.

`sign_response` will need to explicitly be allocated using helper API `okvSignResponseCreate` before passing it as an OUT parameter to `okvSign` API. Once the sign operation is completed, we can get the signature data details from `sign_response` using helper API `okvCryptoResponseGetSignatureData`. `sign_response` needs to be freed using `okvSignResponseFree` helper API.

Example

```
OKVCryptoContext *crypto_context = (OKVCryptoContext *)NULL;
OKVSignResponse *sign_response = (OKVSignResponse *)NULL;
ub1 data[] = "OKV signature operations demo.";
ub4 datal = strlen((const char *) data);
ub1 signature_data[OKV_OBJECT_MAXLEN];
ub4 signature_datal = sizeof(signature_data);

/* Sign */
crypto_context = okvCryptoContextCreate(env, OKVOpSign);
okvCryptoContextSetCryptoAlgo(env, crypto_context, CRYPTO_ALG_RSA);
okvCryptoContextSetHashingAlgo(env, crypto_context, HASH_ALG_SHA_256);
okvCryptoContextSetPadding(env, crypto_context, PADDING_PKCS1_V1_5);
sign_response = okvSignResponseCreate(env);
okvSign(env, private_key_unique_id, data, datal, OKV_DATA_TYPE_RAW,
        crypto_context, sign_response);

memset(signature_data, 0, signature_datal);
okvCryptoResponseGetSignatureData(env, sign_response, signature_data,
                                  &signature_datal);
```

Related Topics

- [okvCryptoContextCreate](#)
`okvCryptoContextCreate` creates the cryptographic context required for cryptographic operations.
- [okvCryptoContextFree](#)
`okvCryptoContextFree` frees the memory allocated to cryptographic context structure.
- [okvCryptoContextSetCryptoAlgo](#)
`okvCryptoContextSetCryptoAlgo` sets the cryptographic algorithm parameter value in the cryptographic context structure.
- [okvCryptoContextSetHashingAlgo](#)
`okvCryptoContextSetHashingAlgo` sets the hashing algorithm parameter value in the cryptographic context structure.
- [okvCryptoContextSetPadding](#)
`okvCryptoContextSetPadding` sets the padding parameter value in the cryptographic context structure.
- [okvCryptoResponseGetSignatureData](#)
`okvCryptoResponseGetSignatureData` gets the signature data value from the sign response structure.
- [okvSignResponseCreate](#)
`okvSignResponseCreate` creates the sign response structure to hold the sign operation response details.
- [okvSignResponseFree](#)
`okvSignResponseFree` frees the memory allocated to the sign response structure.
- [okvSignVerify](#)
`okvSignVerify` implements the KMIP Signature Verify operation.

11.1.33 okvSignVerify

`okvSignVerify` implements the KMIP Signature Verify operation.

Category

KMIP API

Purpose

`okvSignVerify` performs the signature verify operation on the provided data and signature using a KMIP object.

Syntax

```
OKVErrNo okvSignVerify(OKVEnv *env, oratext *uid,
                       ub1 *data, ub4 datal, ub4 data_type,
                       ub1 *signature_data, ub4 signature_datal,
                       OKVCryptoContext *crypto_context,
                       OKVSignVerifyResponse *sign_verify_response);
```

Parameters

Table 11-2 Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>uid</code>	IN	Unique identifier (can be NULL for batching).
<code>data</code>	IN	The data that was signed.
<code>datal</code>	IN	Length of the data that was signed.
<code>data_type</code>	IN	Type of the data that was signed, either <code>OKV_DATA_TYPE_RAW</code> or <code>OKV_DATA_TYPE_DIGEST</code> .
<code>signature_data</code>	IN	Signature to be verified.
<code>signature_datal</code>	IN	Length of the signature.
<code>crypto_context</code>	IN	Cryptographic context contains required parameters for signature verification like the cryptographic algorithm and hashing algorithm.
<code>sign_verify_response</code>	OUT	Contains the sign operation response details.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

`crypto_context` can be created and freed using `okvCryptoContextCreate` and `okvCryptoContextFree` helper APIs. It contains the required parameters for verifying a signature and the user will need to set it explicitly by making use of helper APIs like `okvCryptoContextSetCryptoAlgo`, `okvCryptoContextSetHashingAlgo`, `okvCryptoContextSetPadding`, and `okvCryptoContextSetDigitalSignAlgo`. The user can also get the respective parameter values that was set in `crypto_context` using helper APIs `okvCryptoContextGetCryptoAlgo`, `okvCryptoContextGetHashingAlgo`, `okvCryptoContextGetPadding`, and `okvCryptoContextGetDigitalSignAlgo`. `sign_verify_response` will need to explicitly be allocated using helper API `okvSignVerifyResponseCreate` before passing it as an OUT parameter to `okvSignVerify` API. Once the signature verify operation is completed, we can get the verification details from `sign_verify_response` using helper APIs `okvCryptoResponseGetValidity` and `okvCryptoResponseGetRecoveredData`. `sign_verify_response` needs to be freed using `okvSignVerifyResponseFree` helper API.

Example

```
OKVCryptoContext *crypto_context = (OKVCryptoContext *)NULL;
OKVSignResponse *sign_response = (OKVSignResponse *)NULL;
OKVSignVerifyResponse *verify_response = (OKVSignVerifyResponse *)NULL;
ub1 data[] = "OKV signature operations demo.";
ub4 datal = strlen((const char *) data);
ub4 iter = 0;
ub1 signature_data[OKV_OBJECT_MAXLEN];
ub4 signature_datal = sizeof(signature_data);
ub4 validity = 0;

/* Sign */
crypto_context = okvCryptoContextCreate(env, OKVOpSign);
okvCryptoContextSetCryptoAlgo(env, crypto_context, CRYPTO_ALG_RSA);
okvCryptoContextSetHashingAlgo(env, crypto_context, HASH_ALG_SHA_256);
okvCryptoContextSetPadding(env, crypto_context, PADDING_PKCS1_V1_5);
sign_response = okvSignResponseCreate(env);
okvSign(env, private_key_unique_id, data, datal, OKV_DATA_TYPE_RAW,
crypto_context, sign_response);
memset(signature_data, 0, signature_datal);
okvCryptoResponseGetSignatureData(env, sign_response, signature_data,
&signature_datal);

printf("Successfully signed the data\n");
```

```
printf("\tSignature Data Length: %d\n", signature_data1);
printf("\tSignature Data: ");
for (iter = 0; iter < signature_data1; iter++)
{
    printf("%02X", signature_data[iter]);
}
printf("\n");

okvCryptoContextFree(env, &crypto_context);
okvSignResponseFree(env, &sign_response);

/* Verify */
crypto_context = okvCryptoContextCreate(env, OKVOpSignVerify);
okvCryptoContextSetCryptoAlgo(env, crypto_context, CRYPTO_ALG_RSA);
okvCryptoContextSetHashingAlgo(env, crypto_context, HASH_ALG_SHA_256);
okvCryptoContextSetPadding(env, crypto_context, PADDING_PKCS1_V1_5);
verify_response = okvSignVerifyResponseCreate(env);
okvSignVerify(env, public_key_unique_id, data, data1, OKV_DATA_TYPE_RAW,
signature_data, signature_data1, crypto_context, verify_response);
okvCryptoResponseGetValidity(env, verify_response, &validity);

if (validity == OKVDEF_VALIDITY_VALID)
{
    printf("Signature is valid\n\n");
}
else if (validity == OKVDEF_VALIDITY_INVALID)
{
    printf("Signature is invalid\n\n");
}
else
{
    printf("Signature validity is unknown\n\n");
}

okvCryptoContextFree(env, &crypto_context);
okvSignVerifyResponseFree(env, &verify_response);
```

Related Topics

- [okvCryptoContextCreate](#)
`okvCryptoContextCreate` creates the cryptographic context required for cryptographic operations.
- [okvCryptoContextFree](#)
`okvCryptoContextFree` frees the memory allocated to cryptographic context structure.
- [okvCryptoContextSetCryptoAlgo](#)
`okvCryptoContextSetCryptoAlgo` sets the cryptographic algorithm parameter value in the cryptographic context structure.
- [okvCryptoContextSetHashingAlgo](#)
`okvCryptoContextSetHashingAlgo` sets the hashing algorithm parameter value in the cryptographic context structure.
- [okvCryptoContextSetPadding](#)
`okvCryptoContextSetPadding` sets the padding parameter value in the cryptographic context structure.
- [okvCryptoResponseGetSignatureData](#)
`okvCryptoResponseGetSignatureData` gets the signature data value from the sign response structure.

- [okvSignResponseCreate](#)
`okvSignResponseCreate` creates the sign response structure to hold the sign operation response details.
- [okvSignResponseFree](#)
`okvSignResponseFree` frees the memory allocated to the sign response structure.
- [okvSign](#)
`okvSign` implements the KMIP Sign operation.
- [okvCryptoResponseGetValidity](#)
`okvCryptoResponseGetValidity` gets the validity value from the signature verify response structure.
- [okvSignVerifyResponseCreate](#)
`okvSignVerifyResponseCreate` creates the signature verify response structure to hold the signature verify operation response details.
- [okvSignVerifyResponseFree](#)
`okvSignVerifyResponseFree` frees the memory allocated to the signature verify response structure.

11.1.34 okvCreateKeyPair

`okvCreateKeyPair` implements the KMIP Create Key Pair operation.

Category

KMIP API

Purpose

`okvCreateKeyPair` implements the KMIP Create Pair operation. The unique identifiers of the generated key pair by the Oracle Key Vault server is returned as `private_key_uid` and `public_key_uid`. The maximum length of the unique ID for Oracle Key Vault SDK is defined by `OKV_UNIQUE_ID_MAXLEN`.

Syntax

```
OKVErrNo okvCreateKeyPair(OKVEnv *env,
                          OKVType alg, ub4 len,
                          ub4 private_key_mask, ub4 public_key_mask,
                          OKVTTLV *common_template_names_attrs,
                          OKVTTLV *private_key_template_names_attrs,
                          OKVTTLV *public_key_template_names_attrs,
                          oratext *wallet_name, ub4 wallet_name_len,
                          oratext *private_key_uid, ub4 *private_key_uid_len,
                          oratext *public_key_uid, ub4 *public_key_uid_len);
```

Parameters

Table 11-3 Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>alg</code>	IN	Asymmetric key algorithm.

Table 11-3 (Cont.) Parameters

Parameter	IN/OUT	Description
len	IN	Key length of the asymmetric key algorithm.
private_key_mask	IN	Cryptographic usage mask of the private key.
public_key_mask	IN	Cryptographic usage mask of the public key.
common_template_names_attrs	IN	Template names or attributes that are common to both public and private keys and will form the common template-attribute.
private_key_template_names_attrs	IN	Template names or attributes of private key and will form the private key template-attribute.
public_key_template_names_attrs	IN	Template names or attributes of public key that will form the public key template-attribute.
wallet_name	IN	Wallet name value.
wallet_name_len	IN	Length of the wallet name value.
private_key_uid	OUT	Unique identifier of the generated private key.
private_key_uid_len	OUT	Unique identifier length of the generated private key.
public_key_uid	OUT	Unique identifier of the generated public key.
public_key_uid_len	OUT	Unique identifier length of the generated public key.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

It is recommended to add a KMIP custom or name attribute to both the private and public key objects to help identify it in future. The caller has to allocate the memory for the unique identifiers returned by this function. The length of allocated memory is passed in via the length of the unique identifier arguments `private_key_uid_len` and `public_key_uid_len`. A public and private key pair of the specified length for the specified algorithm and for a specific use

(cryptographic usage mask) is generated in wallet `wallet_name` if specified else it is generated in the default wallet if present with the endpoint.

If `private_key_mask` is set to zero 0, then a default value of private key's cryptographic usage mask (sign, decrypt, wrap_key, and unwrap_key) is assigned during private key creation.

If `public_key_mask` is set to zero 0, then a default value of public key's cryptographic usage mask (verify, encrypt, and unwrap_key) is assigned during public key creation.

Example

```
/* Parameters to create key pair */

OKVType   algo = CRYPTO_ALG_RSA;
ub4       key_len = 2048;
ub4       pri_key_usage_mask = CRYPTO_MASK_SIGN;
ub4       pub_key_usage_mask = CRYPTO_MASK_VERIFY;

OKVTTLV   *request = (OKVTTLV *)NULL;
OKVTTLV   *pri_key_attr = (OKVTTLV *)NULL;
OKVTTLV   *pub_key_attr = (OKVTTLV *)NULL;
OKVTTLV   *pri_key_attr_name_template = (OKVTTLV *)NULL;
OKVTTLV   *pub_key_attr_name_template = (OKVTTLV *)NULL;
oratext   pri_key_unique_id[OKV_UNIQUE_ID_MAXLEN + 1];
ub4       pri_key_unique_id_len = sizeof(pri_key_unique_id);
oratext   pub_key_unique_id[OKV_UNIQUE_ID_MAXLEN + 1];
ub4       pub_key_unique_id_len = sizeof(pub_key_unique_id);

/* Set up the environment handle 'env' and also the memory and
connection management as shown in previous sections */

memset(pri_key_unique_id, 0, pri_key_unique_id_len);
memset(pub_key_unique_id, 0, pub_key_unique_id_len);

request = okvEnvGetOpRequestObj(env);

/* Add name attribute object to both private and public template
attribute */

pri_key_attr_name_template = okvTTLVAddToObject(env, request,
OKVDEF_TAG_PRIVATE_KEY_TEMPLATE_ATTR_ST, OKVDEF_ITEM_TYPE_STRUCT,
(void *)NULL, (ub4)0);
pri_key_attr = okvAddAttributeObject(env, pri_key_attr_name_template,
OKVAttrName, (ub4)0);
okvAttrAddName(env, pri_key_attr, (oratext *) "Private Key",
strlen("Private Key"), 1);

pub_key_attr_name_template = okvTTLVAddToObject(env, request,
OKVDEF_TAG_PUBLIC_KEY_TEMPLATE_ATTR_ST, OKVDEF_ITEM_TYPE_STRUCT, (void
*)NULL, (ub4)0);
pub_key_attr = okvAddAttributeObject(env, pub_key_attr_name_template,
OKVAttrName, (ub4)0);
```

```
okvAttrAddName(env, pub_key_attr, (oratext *) "Public Key", strlen("Public
Key"), 1);

printf("\nCreating a Key Pair on Oracle Key Vault server\n");

okvCreateKeyPair(env, algo, key_len, pri_key_usage_mask, pub_key_usage_mask,
(OKVTTLV *)NULL, pri_key_attr_name_template, pub_key_attr_name_template,
OKV_NO_WALLET, OKV_NO_WALLET_LEN, pri_key_unique_id, &pri_key_unique_id_len,
pub_key_unique_id, &pub_key_unique_id_len);
pri_key_unique_id[pri_key_unique_id_len] = '\0';
pub_key_unique_id[pub_key_unique_id_len] = '\0';

if (okvErrGetNum(env))
{
    printf("Error while creating the key pair\n");
}
```

Related Topics

- [okvRegPrivateKey](#)
`okvRegPrivateKey` implements the KMIP Register operation for the KMIP private key object.
- [okvRegPublicKey](#)
`okvRegPublicKey` implements the KMIP Register operation for the KMIP public key object.
- [okvRegKey](#)
`okvRegKey` implements the KMIP Register operation for the KMIP symmetric key object.
- [okvCreateKey](#)
`okvCreateKey` implements the KMIP Create operation for the KMIP symmetric key object.

11.2 Oracle Key Vault Client SDK Batch APIs

This section describes the interfaces for the Oracle Key Vault KMIP batch functions.

- [okvBatchCreate](#)
`okvBatchCreate` will mark the start of Oracle Key Vault batching.
- [okvBatchExecute](#)
`okvBatchExecute` will execute the batched Oracle Key Vault functions.
- [okvBatchFree](#)
`okvBatchFree` will mark the end of Oracle Key Vault batching.
- [okvGetBatchOperationCount](#)
`okvGetBatchOperationCount` gets the count of batched Oracle Key Vault operations.
- [okvGetBatchOperationName](#)
`okvGetBatchOperationName` returns the KMIP operation name of the respective batch job number that is passed with this function.

11.2.1 okvBatchCreate

`okvBatchCreate` will mark the start of Oracle Key Vault batching.

Category

KMIP Batch API

Purpose

`okvBatchCreate` will mark the start of Oracle Key Vault batching. All Oracle Key Vault functions after this command will be batched.

Syntax

```
OKVErrNo okvBatchCreate(OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
/* Set up the environment handle 'env' and also the memory and
   connection management as shown in previous sections. */

printf("Start preparing batch operations\n");
okvBatchCreate(env);

if (okvErrGetNum(env))
{
    printf("Error while initiating the Batch");
}
...
/* All Oracle Key Vault APIs from this point will be batched */
```

Related Topics

- [okvBatchExecute](#)
`okvBatchExecute` will execute the batched Oracle Key Vault functions.

- [okvBatchFree](#)
`okvBatchFree` will mark the end of Oracle Key Vault batching.
- [okvGetBatchOperationCount](#)
`okvGetBatchOperationCount` gets the count of batched Oracle Key Vault operations.
- [okvGetBatchOperationName](#)
`okvGetBatchOperationName` returns the KMIP operation name of the respective batch job number that is passed with this function.

11.2.2 okvBatchExecute

`okvBatchExecute` will execute the batched Oracle Key Vault functions.

Category

KMIP Batch API

Purpose

`okvBatchExecute` will execute the batched Oracle Key Vault functions. The batched Oracle Key Vault functions are functions between `okvBatchCreate` and `okvBatchExecute`. If there are errors, then the errors for all the batched Oracle Key Vault functions should be checked to verify which operations failed and which were successful.

Syntax

```
OKVErrNo okvBatchExecute(OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

To check for individual operations in the batch after its execution, these APIs can be made use of: `okvErrGetNumForBatch`, `okvErrGetDepthForBatch`, and `okvErrGetNumAtDepthForBatch`. The errors for individual batch operations can be checked only before freeing the batch context, that is, before calling `okvBatchFree`.

Example

```
/* Set up the environment handle 'env' and also the memory and
   connection management as shown in previous sections. */
printf("Start preparing batch operations\n");
```

```
okvBatchCreate(env);
...
/* All Oracle Key Vault KMIP APIs from this point will be batched */
...
printf("Executing batch operation\n");
okvBatchExecute(env);

if (okvErrGetNum(env))
{
    printf("Error while executing the batch");
}
```

Related Topics

- [okvBatchCreate](#)
`okvBatchCreate` will mark the start of Oracle Key Vault batching.
- [okvBatchFree](#)
`okvBatchFree` will mark the end of Oracle Key Vault batching.
- [okvErrGetDepthForBatch](#)
`okvErrGetDepthForBatch` is used to return the depth of the error stack for the provided batch job number otherwise 0 is returned.
- [okvErrGetNumAtDepthForBatch](#)
`okvErrGetNumAtDepthForBatch` returns the error number at the specified depth of the error stack for the provided batch job number.
- [okvErrGetNumForBatch](#)
`okvErrGetNumForBatch` returns the error number on top of the error stack for the provided batch job number.
- [okvGetBatchOperationCount](#)
`okvGetBatchOperationCount` gets the count of batched Oracle Key Vault operations.
- [okvGetBatchOperationName](#)
`okvGetBatchOperationName` returns the KMIP operation name of the respective batch job number that is passed with this function.

11.2.3 okvBatchFree

`okvBatchFree` will mark the end of Oracle Key Vault batching.

Category

KMIP Batch API

Purpose

`okvBatchFree` will mark the end of Oracle Key Vault batching. Essentially the memory allocated for complex arguments will be released. Subsequent Oracle Key Vault functions will not be batched unless `okvBatchCreate` is called again.

Syntax

```
OKVErrNo okvBatchFree (OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The errors for individual batch operations can be checked only before freeing the batch context, that is, before calling `okvBatchFree`.

Example

```

/* Set up the environment handle 'env' and also the memory and
   connection management as shown in previous sections. */
printf("Start preparing batch operations\n");
okvBatchCreate(env);
...
/* All Oracle Key Vault KMIP APIs from this point will be batched */
...
printf("Executing batch operation\n");
okvBatchExecute(env);
...
/* Check for Individual Batch Operation errors */
...
printf("Ending batch operations\n\n");
okvBatchFree(env);

if (okvErrGetNum(env))
{
    printf("Error while ending the batch");
}

```

Related Topics

- [okvBatchCreate](#)
`okvBatchCreate` will mark the start of Oracle Key Vault batching.
- [okvBatchExecute](#)
`okvBatchExecute` will execute the batched Oracle Key Vault functions.
- [okvGetBatchOperationCount](#)
`okvGetBatchOperationCount` gets the count of batched Oracle Key Vault operations.
- [okvGetBatchOperationName](#)
`okvGetBatchOperationName` returns the KMIP operation name of the respective batch job number that is passed with this function.

11.2.4 okvGetBatchOperationCount

`okvGetBatchOperationCount` gets the count of batched Oracle Key Vault operations.

Category

KMIP Batch API

Purpose

`okvGetBatchOperationCount` gets the count of batched Oracle Key Vault operations.

Syntax

```
ub4 okvGetBatchOperationCount(OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
<code>ub4</code>	Count of the batched operations. Success: A valid positive non-zero number is returned. Failure: Zero.

Comments

This function should be called before calling `okvBatchFree` else it will return zero.

Example

```
ub4 batch_cnt = 0;

/* Set up the environment handle 'env' and also the memory and
   connection management as shown in previous sections. */
printf("\t\tStart preparing batch operations\n");
okvBatchCreate(env);
...
* All Oracle Key Vault KMIP APIs from this point will be batched */
...
printf("\t\tExecuting batch operation\n");
okvBatchExecute(env);
...
/* Check for Individual Batch Operation errors */
...
batch_cnt = okvGetBatchOperationCount(env);
printf("Count of the KMIP operations that are batched: %d", batch_cnt);
```

Related Topics

- [okvBatchCreate](#)
`okvBatchCreate` will mark the start of Oracle Key Vault batching.
- [okvBatchExecute](#)
`okvBatchExecute` will execute the batched Oracle Key Vault functions.
- [okvBatchFree](#)
`okvBatchFree` will mark the end of Oracle Key Vault batching.
- [okvGetBatchOperationName](#)
`okvGetBatchOperationName` returns the KMIP operation name of the respective batch job number that is passed with this function.

11.2.5 okvGetBatchOperationName

`okvGetBatchOperationName` returns the KMIP operation name of the respective batch job number that is passed with this function.

Category

KMIP Batch API

Purpose

`okvGetBatchOperationName` returns the KMIP operation name of the respective batch job number that is passed with this function.

Syntax

```
oratest *okvGetBatchOperationName(OKVEnv *env, ubl batch_job_no);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>batch_job_no</code>	IN	Batch job number.

Return Values

Return Value	Description
<code>oratest *</code>	KMIP operation name that was batched. Success: A pointer to batch job operation name is returned. Failure: NULL pointer is returned.

Comments

This function should be called before calling `okvBatchFree` else it will return a pointer to NULL.

`batch_job_no` is the number in which the operations are batched. For example, if the user wants to create a key, activate a key, revoke it, and then destroy it, all of these operations are batched in the same order, that is, `batch_job_no` for create a key is 1, `batch_job_no` for activate a key is 2, `batch_job_no` for revoke is 3, and `batch_job_no` for destroy is 4.

Example

```
ub4 batch_cnt = 0;
ub4 batch_job_num = 0;

/* Set up the environment handle 'env' also the memory and
   connection management as shown in previous sections. */
printf("\t\tStart preparing batch operations\n");
okvBatchCreate(env);
...
/* All Oracle Key Vault KMIP APIs from this point will be batched */
...
printf("\t\tExecuting batch operation\n");
okvBatchExecute(env);
...
/* Check for Individual Batch Operation errors */
...
batch_cnt = okvGetBatchOperationCount(env);
printf("Batch Operations count is: %d\n", batch_cnt);

if (batch_cnt)
{
    for(batch_job_num=1; batch_job_num<=batch_cnt; batch_job_num++)
    {
        printf("\t\t\t%d: %s\n", batch_job_num, okvGetBatchOperationName(env,
batch_job_num));
    }
}
```

Related Topics

- [okvBatchCreate](#)
`okvBatchCreate` will mark the start of Oracle Key Vault batching.
- [okvBatchExecute](#)
`okvBatchExecute` will execute the batched Oracle Key Vault functions.
- [okvBatchFree](#)
`okvBatchFree` will mark the end of Oracle Key Vault batching.
- [okvGetBatchOperationCount](#)
`okvGetBatchOperationCount` gets the count of batched Oracle Key Vault operations.

12

Oracle Key Vault Client SDK KMIP Attributes and Custom Attributes APIs

This section describes the interfaces that help create and interpret both KMIP attributes and KMIP custom attributes.

- [Oracle Key Vault Client SDK KMIP Attribute APIs](#)
Oracle Key Vault client SDK provides a set of APIs to manage KMIP attributes.
- [Oracle Key Vault Client SDK KMIP Custom Attribute APIs](#)
The KMIP Custom Attribute APIs are listed in this section.

12.1 Oracle Key Vault Client SDK KMIP Attribute APIs

Oracle Key Vault client SDK provides a set of APIs to manage KMIP attributes.

- [About the Oracle Key Vault KMIP Attribute APIs](#)
This section describes the interfaces that help create and interpret Oracle Key Vault KMIP attributes.
- [Attribute Index and Element Index](#)
Element index can be used to retrieve child TTLV objects from the parent TTLV object and attribute index is the property of a KMIP Attribute.
- [okvAttrAddArchiveDate](#)
`okvAttrAddArchiveDate` adds an archive date attribute to an OKVTTLV object.
- [okvAddAttributeObject](#)
`okvAddAttributeObject` adds an attribute object to the parent TTLV object.
- [okvAttrAddActivationDate](#)
`okvAttrAddActivationDate` adds the activation date attribute to an OKVTTLV object.
- [okvAttrAddCertLen](#)
`okvAttrAddCertLen` adds a certificate length attribute to an OKVTTLV object.
- [okvAttrAddCertType](#)
`okvAttrAddCertType` adds a certificate type attribute to an OKVTTLV object.
- [okvAttrAddCompromiseDate](#)
`okvAttrAddCompromiseDate` adds a compromise date attribute to an OKVTTLV object.
- [okvAttrAddCompromiseOccurrenceDate](#)
`okvAttrAddCompromiseOccurrenceDate` adds a compromise occurrence date attribute to an OKVTTLV object.
- [okvAttrAddContactInfo](#)
`okvAttrAddContactInfo` adds a contact information attribute to an OKVTTLV object.
- [okvAttrAddCryptoAlgo](#)
`okvAttrAddCryptoAlgo` adds a cryptographic algorithm attribute to an OKVTTLV object.
- [okvAttrAddCryptoLen](#)
`okvAttrAddCryptoLen` adds a cryptographic length attribute to an OKVTTLV object.

- [okvAttrAddCryptoParams](#)
`okvAttrAddCryptoParams` adds cryptographic parameters to an OKVTTLV object.
- [okvAttrAddCryptoUsageMask](#)
`okvAttrAddCryptoUsageMask` adds a cryptographic usage mask attribute to an OKVTTLV object.
- [okvAttrAddDeactivationDate](#)
`okvAttrAddDeactivationDate` adds a deactivation date attribute to an OKVTTLV object.
- [okvAttrAddDestroyDate](#)
`okvAttrAddDestroyDate` adds a destroy date attribute to an OKVTTLV object.
- [okvAttrAddDigest](#)
`okvAttrAddDigest` adds a digest attribute to an OKVTTLV object.
- [okvAttrAddDigitalSignAlgo](#)
`okvAttrAddDigitalSignAlgo` adds a digital signature algorithm attribute to an OKVTTLV object.
- [okvAttrAddExtractable](#)
`okvAttrAddExtractable` adds an extractable attribute to an OKVTTLV object.
- [okvAttrAddFresh](#)
`okvAttrAddFresh` adds a fresh attribute to an OKVTTLV object.
- [okvAttrAddInitialDate](#)
`okvAttrAddInitialDate` adds an initial date attribute to an OKVTTLV object.
- [okvAttrAddLastChangeDate](#)
`okvAttrAddLastChangeDate` adds a last change date attribute to an OKVTTLV object.
- [okvAttrAddLeaseTime](#)
`okvAttrAddLeaseTime` adds a lease time attribute to an OKVTTLV object.
- [okvAttrAddName](#)
`okvAttrAddName` adds a name attribute to an OKVTTLV object.
- [okvAttrAddNeverExtractable](#)
`okvAttrAddNeverExtractable` adds a never extractable attribute to an OKVTTLV object.
- [okvAttrAddObjectGroup](#)
`okvAttrAddObjectGroup` adds an object group attribute to an OKVTTLV object.
- [okvAttrAddObjectType](#)
`okvAttrAddObjectType` adds an object type attribute to an OKVTTLV object.
- [okvAttrAddProcessStartDate](#)
`okvAttrAddProcessStartDate` adds a process start date attribute to an OKVTTLV object.
- [okvAttrAddProtectStopDate](#)
`okvAttrAddProtectStopDate` adds a protect stop date attribute to an OKVTTLV object.
- [okvAttrAddRevocationReason](#)
`okvAttrAddRevocationReason` adds the revocation reason attribute to an OKVTTLV object.

- [okvAttrAddState](#)
`okvAttrAddState` adds a state attribute to an OKVTTLV object.
- [okvAttrAddUniqueID](#)
`okvAttrAddUniqueID` adds a unique identifier attribute to an OKVTTLV object.
- [okvAttrAddUsageLimits](#)
`okvAttrAddUsageLimits` adds a usage limits attribute to an OKVTTLV object.
- [okvAttrAddX509CertId](#)
`okvAttrAddX509CertId` adds an issuer and serial number which forms the X.509 Certificate ID attribute to an OKVTTLV object.
- [okvAttrAddX509CertIss](#)
`okvAttrAddX509CertIss` adds a X.509 Certificate Issuer distinguished name attribute to an OKVTTLV object.
- [okvAttrAddX509CertIssAltName](#)
`okvAttrAddX509CertIssAltName` adds a X.509 Certificate Issuer Alternate name attribute to an OKVTTLV object.
- [okvAttrAddX509CertSubj](#)
`okvAttrAddX509CertSubj` adds a X.509 Certificate Subject distinguished name attribute to an OKVTTLV object.
- [okvAttrAddX509CertSubjAltName](#)
`okvAttrAddX509CertSubjAltName` adds a X.509 Certificate Subject Alternate name attribute to an OKVTTLV object.
- [okvAttrGetActivationDate](#)
`okvAttrGetActivationDate` gets the activation date attribute value from an OKVTTLV object.
- [okvAttrGetArchiveDate](#)
`okvAttrGetArchiveDate` gets the archive date attribute value from an OKVTTLV object.
- [okvAttrGetCertLen](#)
`okvAttrGetCertLen` gets the certificate length attribute value from an OKVTTLV object.
- [okvAttrGetCertType](#)
`okvAttrGetCertType` gets the certificate type attribute value from an OKVTTLV object.
- [okvAttrGetCompromiseDate](#)
`okvAttrGetCompromiseDate` gets the compromise date attribute value from an OKVTTLV object.
- [okvAttrGetCompromiseOccurrenceDate](#)
`okvAttrGetCompromiseOccurrenceDate` gets the compromise occurrence date attribute value from an OKVTTLV object.
- [okvAttrGetContactInfo](#)
`okvAttrGetContactInfo` gets the contact information attribute value from an OKVTTLV object.
- [okvAttrGetContactInfoLen](#)
`okvAttrGetContactInfoLen` gets the length of the contact information value of the contact information attribute.
- [okvAttrGetCryptoAlgo](#)
`okvAttrGetCryptoAlgo` gets the cryptographic algorithm attribute value from an OKVTTLV object.

- [okvAttrGetCryptoLen](#)
`okvAttrGetCryptoLen` gets the cryptographic length attribute value from an OKVTTLV object.
- [okvAttrGetCryptoParams](#)
`okvAttrGetCryptoParams` gets the cryptographic parameters attribute found at or after element index `elem_index`.
- [okvAttrGetCryptoUsageMask](#)
`okvAttrGetCryptoUsageMask` gets the cryptographic usage mask attribute value from an OKVTTLV object.
- [okvAttrGetDeactivationDate](#)
`okvAttrGetDeactivationDate` gets the deactivation date attribute value from an OKVTTLV object.
- [okvAttrGetDestroyDate](#)
`okvAttrGetDestroyDate` gets the destroy date attribute value from an OKVTTLV object.
- [okvAttrGetDigest](#)
`okvAttrGetDigest` gets the digest attribute found at or after element index `elem_index`.
- [okvAttrGetDigestLen](#)
`okvAttrGetDigestLen` gets the length of the digest value of the digest attribute found at or after element index `elem_index`.
- [okvAttrGetDigitalSignAlgo](#)
`okvAttrGetDigitalSignAlgo` gets the digital signature algorithm attribute value from an OKVTTLV object.
- [okvAttrGetExtractable](#)
`okvAttrGetExtractable` gets the extractable attribute value from an OKVTTLV object.
- [okvAttrGetFresh](#)
`okvAttrGetFresh` gets the fresh attribute value from an OKVTTLV object.
- [okvAttrGetInitialDate](#)
`okvAttrGetInitialDate` gets the initial date attribute value from an OKVTTLV object.
- [okvAttrGetLastChangeDate](#)
`okvAttrGetLastChangeDate` gets the last change date attribute value from an OKVTTLV object.
- [okvAttrGetLeaseTime](#)
`okvAttrGetLeaseTime` gets the lease time attribute value from an OKVTTLV object.
- [okvAttrGetName](#)
`okvAttrGetName` gets the name value, attribute index, and name type of the name attribute found at or after element index `elem_index`.
- [okvAttrGetNameValueLen](#)
`okvAttrGetNameValueLen` gets the length of the name value of the name attribute found at or after element index `elem_index`.

- [okvAttrGetNeverExtractable](#)
`okvAttrGetNeverExtractable` gets the never extractable attribute value from an OKVTTLV object.
- [okvAttrGetObjectGroup](#)
`okvAttrGetObjectGroup` gets the object group value of the object group attribute found at or after element index `elem_index`.
- [okvAttrGetObjectGroupLen](#)
`okvAttrGetObjectGroupLen` gets the length of the object group value of the object group attribute found at or after element index `elem_index`.
- [okvAttrGetObjectType](#)
`okvAttrGetObjectType` gets the object type attribute value from an OKVTTLV object.
- [okvAttrGetProcessStartDate](#)
`okvAttrGetProcessStartDate` gets the process start date attribute value from an OKVTTLV object.
- [okvAttrGetProtectStopDate](#)
`okvAttrGetProtectStopDate` gets the protect stop date attribute value from an OKVTTLV object.
- [okvAttrGetRevocationReason](#)
`okvAttrGetRevocationReason` gets the revocation reason attribute value from an OKVTTLV object.
- [okvAttrGetRevocationReasonMessageLen](#)
`okvAttrGetRevocationReasonMessageLen` gets the length of the revocation message value of the revocation reason attribute.
- [okvAttrGetState](#)
`okvAttrGetState` gets the state attribute value from an OKVTTLV object.
- [okvAttrGetUniqueID](#)
`okvAttrGetUniqueID` gets the unique identifier attribute value from an OKVTTLV object.
- [okvAttrGetUniqueIDLen](#)
`okvAttrGetUniqueIDLen` gets the length of the unique identifier value of the unique identifier attribute.
- [okvAttrGetUsageLimits](#)
`okvAttrGetUsageLimits` gets the usage limits attribute value from an OKVTTLV object.
- [okvAttrGetX509CertId](#)
`okvAttrGetX509CertId` gets the X.509 Certificate ID attribute value from an OKVTTLV object.
- [okvAttrGetX509CertIdIssuerLen](#)
`okvAttrGetX509CertIdIssuerLen` gets the length of the certificate issuer value of the X.509 Certificate ID attribute from an OKVTTLV object.
- [okvAttrGetX509CertIdSerialNoLen](#)
`okvAttrGetX509CertIdSerialNoLen` gets the length of the certificate serial number value of the X.509 Certificate ID attribute from an OKVTTLV object.
- [okvAttrGetX509CertIss](#)
`okvAttrGetX509CertIss` gets the X.509 Certificate Issuer distinguished name attribute value from an OKVTTLV object.

- [okvAttrGetX509CertIssAltName](#)
`okvAttrGetX509CertIssAltName` gets the X.509 Certificate Issuer alternate name attribute value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertIssAltNameLen](#)
`okvAttrGetX509CertIssAltNameLen` gets the length of the X.509 Certificate Issuer Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertIssDNLen](#)
`okvAttrGetX509CertIssDNLen` gets the length of the X.509 Certificate Issuer distinguished name value from an OKVTTLV object.
- [okvAttrGetX509CertSubj](#)
`okvAttrGetX509CertSubj` gets the X.509 Certificate Subject distinguished name attribute value from an OKVTTLV object.
- [okvAttrGetX509CertSubjAltName](#)
`okvAttrGetX509CertSubjAltName` gets the X.509 Certificate Subject alternate name attribute value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertSubjAltNameLen](#)
`okvAttrGetX509CertSubjAltNameLen` gets the length of the X.509 Certificate Subject Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertSubjDNLen](#)
`okvAttrGetX509CertSubjDNLen` gets the length of the X.509 Certificate Subject distinguished name value from an OKVTTLV object.
- [okvGetAttributeObject](#)
`okvGetAttributeObject` gets the attribute, its name, and index from the parent attribute found at element index `elem_index`.

12.1.1 About the Oracle Key Vault KMIP Attribute APIs

This section describes the interfaces that help create and interpret Oracle Key Vault KMIP attributes.

For the functions in this section, all of the functions with arguments `env` and `ttlv` have the following meaning:

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault Environment handle.
<code>ttlv</code>	IN	TTLV parent object.

For the functions in this section that return the TTLV object (`OKVTTLV *`), the return value has the following interpretation:

- On success, a valid TTLV object for the attribute is returned.
- On failure, a NULL pointer is returned.

For the functions in this section that return the length of the retrieved object, the return value has the following interpretation:

- On success, the length of the buffer is returned.
- On failure, zero (0) is returned.

For the functions in this section that return the Oracle Key Vault error number, the return value has the following interpretation:

- On success, `OKV_SUCCESS` is returned.
- On failure, a valid error number is returned for the error on top of the error stack.

Oracle Key Vault functions defined in this section add and retrieve attributes of a specific KMIP data type to and from the OKVTTLV object. The functions have the following construction in general:

- `okvAttrAddAttr`: Adds the attribute to the OKVTTLV parent object.
- `okvAttrGetAttrLen`: Gets the value length of the attribute in OKVTTLV parent object for KMIP Attributes that don't have fixed length.
- `okvAttrGetAttrElementLen`: Gets the value length of the element of the attribute in the OKVTTLV parent object for STRUCTURE attributes that have child values with variable length. An example is the name value of the `name` attribute.
- `okvAttrGetAttr`: Gets the attribute in the OKVTTLV parent object.

Note:

For the functions in this section that are used to set the attributes of type date-time, do not set the time value to epoch time (January 1st, 1970 at UTC). In Oracle Key Vault, setting the date-time attributes (such as, `ActivationDate`, `DeactivationDate`, `ProcessStartDate`, and `ProtectStopDate`) for a security object to the epoch time has the same effect of not setting the attribute at all. For example, if you set the `ActivationDate` attribute of a security object to the epoch time to immediately activate the object, then the object remains in the Pre-Active state. This is because Oracle Key Vault treats the epoch value of the attribute as if the attribute is not set at all.

12.1.2 Attribute Index and Element Index

Element index can be used to retrieve child TTLV objects from the parent TTLV object and attribute index is the property of a KMIP Attribute.

An OKVTTLV parent object can have a number of child OKVTTLV objects. The child objects usually have different KMIP tags. Some of the child objects like, multi-instance attributes can be repeated, so there can be a few child objects with the same tag.

The immediate child objects of an OKVTTLV object can be thought of as an indexed list. The child OKVTTLV objects can be retrieved one by one from the parent object by specifying the index. This index is the element index of the child TTLV object.

`okvTTLVGetChild` should be used to retrieve the child by specifying the element index.

In most cases however, the child being looked up is known. The child is usually identified by a tag. But what is not known is the index of the child TTLV object.

`okvTTLVGetChildByTag` is used to lookup the child with a given tag.

With this API we generally guess that the child is found at particular index. The API will look for the first occurrence of the child from this index onwards and will return the actual index where the child was found.

Usually we should start with index 0, to get the first occurrence of the child with a given tag. The returned element index will specify where the child was found.

The element index can be incremented by one and `okvTTLVGetChildByTag` can be called again to get the second occurrence of the child with the same tag.

The first occurrence of child with a given tag can also be done by using `okvTTLVGetFirstChildByTag`.

This behavior is true for any Oracle Key Vault function that takes element index as an argument.

As an example using the OKVTTLV Parent Object table below, calling `okvTTLVGetChildByTag("Name", &elem_index)` with `elem_index` set to 1 will return object with Ref# C, and set the `elem_index` to 2. Again calling `okvTTLVGetChildByTag("Object Group", &elem_index)` with `elem_index` set to 4 will return object with Ref# E, and set the `elem_index` to 4.

Table 12-1 OKVTTLV Parent Object

Ref #	Attribute Object	Element Index	Attribute Index
A	Name	0	1
B	Object Group	1	1
C	Name	2	3
D	Name	3	2
E	Object Group	4	2

Attribute index is the property of a KMIP Attribute. Oracle Key Vault returns the attribute index to the endpoint program when requested or the endpoint program can add one when modifying or adding an attribute. Oracle Key Vault does not do any special processing for the attribute index and does not use it for lookup operations.

12.1.3 okvAttrAddArchiveDate

`okvAttrAddArchiveDate` adds an archive date attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddArchiveDate` adds an archive date attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddArchiveDate(OKVEnv *env, OKVTTLV *ttlV,
                                ub8 archive_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to OKVTTLV object.
archive_date	IN	Archive date.

Return Values

Return Value	Description
OKVTTLV *	<p>Pointer to OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with archive date attribute value added.</p> <p>Failure: NULL Pointer.</p>

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
time_t current_time = time((time_t *)NULL);
okvAttrAddArchiveDate(env, ttlv, (ub8) current_time + 10000);
```

Related Topics

- [okvAttrGetArchiveDate](#)
okvAttrGetArchiveDate gets the archive date attribute value from an OKVTTLV object.

12.1.4 okvAddAttributeObject

okvAddAttributeObject adds an attribute object to the parent TTLV object.

Category

KMIP attribute API

Purpose

okvAddAttributeObject adds an attribute object to the parent TTLV object. The actual attribute value can be added using the functions defined in this section.

Syntax

```
OKVTTLV* okvAddAttributeObject(OKVEnv *env, OKVTTLV *ttl,
                               OKVAttrNo attrno, ub4 attr_index);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault Environment handle.
ttlv	IN	Pointer to parent OKVTTLV object.
attrno	IN	Attribute number of the attribute being added.
attr_index	IN	Attribute index of the attribute.

Return Values

Return Value	Description
OKVTTLV *	<p>Pointer to OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with attribute object TTLV indicated by argument <code>attrno</code> added.</p> <p>Failure: NULL pointer.</p>

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

The API can be used to add attribute TTLVs to the parent TTLV object. The below example shows how a contact info attribute can be added to the parent TTLV object.

Example

```
oratext *contact = (oratext *)"sample contact info";
ub4      contactl = strlen((char *) contact);
OKVTTLV *resultttl;

resultttl = okvAddAttributeObject(env, ttlv, OKVAttrContactInfo, (ub4) 0);
okvAttrAddContactInfo(env, resultttl, contact, contactl);
```

Related Topics

- [okvGetAttributeObject](#)
`okvGetAttributeObject` gets the attribute, its name, and index from the parent attribute found at element index `elem_index`.

12.1.5 okvAttrAddActivationDate

`okvAttrAddActivationDate` adds the activation date attribute to an OKVTTLV object.

Catetry

KMIP attribute API

Purpose

`okvAttrAddActivationDate` adds the activation date attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddActivationDate(OKVEnv *env, OKVTTLV *ttl,
                                   ub8 activation_date);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to parent OKVTTLV object.
<code>activation_date</code>	IN	Activation date.

Return Values

Return Value	Description
<code>OKVTTLV *</code>	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with activation date attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
time_t current_time = time((time_t *)NULL);
...
okvAttrAddActivationDate(env, attr_in, (ub8) current_time + 10000);
```

Related Topics

- [okvAttrGetActivationDate](#)
`okvAttrGetActivationDate` gets the activation date attribute value from an OKVTTLV object.

12.1.6 okvAttrAddCertLen

`okvAttrAddCertLen` adds a certificate length attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddCertLen` adds a certificate length attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddCertLen(OKVEnv *env, OKVTTLV *ttl,
                           ub4 cert_len);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to OKVTTLV object.
cert_len	IN	Certificate length.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with certificate length attribute value added. Failure: NULL pointer.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the `OKVTTLV` object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
okvAttrAddCertLen(env, ttl, (ub4)500);
```

Related Topics

- [okvAttrAddCertType](#)
`okvAttrAddCertType` adds a certificate type attribute to an OKVTTLV object.
- [okvAttrGetCertType](#)
`okvAttrGetCertType` gets the certificate type attribute value from an OKVTTLV object.
- [okvAttrGetCertLen](#)
`okvAttrGetCertLen` gets the certificate length attribute value from an OKVTTLV object.

12.1.7 okvAttrAddCertType

`okvAttrAddCertType` adds a certificate type attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddCertType` adds a certificate type attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddCertType(OKVEnv *env, OKVTTLV *ttl,
                             ub4 cert_typ);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV object.
<code>cert_typ</code>	IN	Certificate type.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with certificate type attribute value added. Failure: NULL pointer.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the `OKVTTLV` object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
okvAttrAddCertType(env, ttl, OKVDEF_CERT_TYPE_X509);
```

Related Topics

- [okvAttrAddCertLen](#)
`okvAttrAddCertLen` adds a certificate length attribute to an OKVTTLV object.
- [okvAttrGetCertLen](#)
`okvAttrGetCertLen` gets the certificate length attribute value from an OKVTTLV object.

- [okvAttrGetCertType](#)
okvAttrGetCertType gets the certificate type attribute value from an OKVTTLV object.

12.1.8 okvAttrAddCompromiseDate

okvAttrAddCompromiseDate adds a compromise date attribute to an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrAddCompromiseDate adds a compromise date attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddCompromiseDate(OKVEnv *env, OKVTTLV *ttl,
                                   ub8 comp_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to OKVTTLV object.
comp_date	IN	Compromise date.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with compromise date attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
time_t current_time = time((time_t *)NULL);
OKVTTLV *resultttl;
resultttl = okvAttrAddCompromiseDate(env, ttl, (ub8) current_time + 24*3600);
```

Related Topics

- [okvAttrGetCompromiseDate](#)
okvAttrGetCompromiseDate gets the compromise date attribute value from an OKVTTLV object.

12.1.9 okvAttrAddCompromiseOccurrenceDate

`okvAttrAddCompromiseOccurrenceDate` adds a compromise occurrence date attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddCompromiseOccurrenceDate` adds a compromise occurrence date attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddCompromiseOccurrenceDate(OKVEnv *env, OKVTTLV *ttl,
                                             ub8 comp_occr_date);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to parent OKVTTLV object.
<code>comp_occr_date</code>	IN	Compromise occurrence date.

Return Values

Return Value	Description
<code>OKVTTLV *</code>	<p>Pointer to OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with compromise occurrence date attribute value added.</p> <p>Failure: NULL pointer.</p>

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
ub8 comp_date;
ctime(&comp_date);
resultttl = okvAttrAddCompromiseOccurrenceDate(env, ttl, comp_date);
```

Related Topics

- [okvAttrGetCompromiseOccurrenceDate](#)
`okvAttrGetCompromiseOccurrenceDate` gets the compromise occurrence date attribute value from an OKVTTLV object.

12.1.10 okvAttrAddContactInfo

`okvAttrAddContactInfo` adds a contact information attribute to an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrAddContactInfo` adds a contact information attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddContactInfo(OKVEnv *env, OKVTTLV *ttl,
                                oratext *contact_info, ub4 contact_infol);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to parent OKVTTLV object.
<code>contact_info</code>	IN	Contact information.
<code>contact_infol</code>	IN	Length of contact information.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with contact info attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
OKVTTLV *resultttl;
oratext *new_contact = (oratext *)"abc.xyz@com";
ub4 new_contactl = strlen((char *) new_contact);
resultttl = okvAttrAddContactInfo(env, attr_in, new_contact, new_contactl);
```

Related Topics

- [okvAttrGetContactInfoLen](#)
`okvAttrGetContactInfoLen` gets the length of the contact information value of the contact information attribute.

- [okvAttrGetContactInfo](#)
`okvAttrGetContactInfo` gets the contact information attribute value from an OKVTTLV object.

12.1.11 okvAttrAddCryptoAlgo

`okvAttrAddCryptoAlgo` adds a cryptographic algorithm attribute to an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrAddCryptoAlgo` adds a cryptographic algorithm attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddCryptoAlgo(OKVEnv *env, OKVTTLV *ttl,
                               ub4 crypto_alg);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to parent OKVTTLV object.
<code>crypto_alg</code>	IN	Cryptographic algorithm.

Return Values

Return Value	Description
<code>OKVTTLV *</code>	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with cryptographic algorithm attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
attr = okvAddAttributeObject(env, templ, OKVAttrCryptoAlg, 0);
okvAttrAddCryptoAlgo(env, attr, (ub4)CRYPTO_ALG_AES);
```

Related Topics

- [okvAttrGetCryptoAlgo](#)
`okvAttrGetCryptoAlgo` gets the cryptographic algorithm attribute value from an OKVTTLV object.

- [okvAttrAddCryptoLen](#)
`okvAttrAddCryptoLen` adds a cryptographic length attribute to an OKVTTLV object.
- [okvAttrGetCryptoLen](#)
`okvAttrGetCryptoLen` gets the cryptographic length attribute value from an OKVTTLV object.
- [okvAttrAddCryptoParams](#)
`okvAttrAddCryptoParams` adds cryptographic parameters to an OKVTTLV object.
- [okvAttrGetCryptoParams](#)
`okvAttrGetCryptoParams` gets the cryptographic parameters attribute found at or after element index `elem_index`.

12.1.12 okvAttrAddCryptoLen

`okvAttrAddCryptoLen` adds a cryptographic length attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddCryptoLen` adds a cryptographic length attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddCryptoLen(OKVEnv *env, OKVTTLV *ttl,
                             ub4 crypto_len);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to parent OKVTTLV object.
<code>crypto_len</code>	IN	Cryptographic length.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with cryptographic length attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
attr = okvAddAttributeObject(env, templ, OKVAttrCryptoLen, 0);
okvAttrAddCryptoLen(env, attr, (ub4)128);
```

Related Topics

- [okvAttrAddCryptoAlgo](#)
okvAttrAddCryptoAlgo adds a cryptographic algorithm attribute to an OKVTTLV object.
- [okvAttrGetCryptoAlgo](#)
okvAttrGetCryptoAlgo gets the cryptographic algorithm attribute value from an OKVTTLV object.
- [okvAttrGetCryptoLen](#)
okvAttrGetCryptoLen gets the cryptographic length attribute value from an OKVTTLV object.
- [okvAttrAddCryptoParams](#)
okvAttrAddCryptoParams adds cryptographic parameters to an OKVTTLV object.
- [okvAttrGetCryptoParams](#)
okvAttrGetCryptoParams gets the cryptographic parameters attribute found at or after element index elem_index.

12.1.13 okvAttrAddCryptoParams

okvAttrAddCryptoParams adds cryptographic parameters to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrAddCryptoParams adds cryptographic parameters to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddCryptoParams(OKVEnv *env, OKVTTLV *ttl,
                                ub4 block_cipher_mode, ub4 padding_method,
                                ub4 hashing_algorithm, ub4 key_role_type);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to parent TTLV.
block_cipher_mode	IN	Block cipher mode.
padding_method	IN	Padding method.
hashing_algorithm	IN	Hashing algorithm.
key_role_type	IN	Key role type.

Return Values

Return Value	Description
OKVTTLV *	<p>Pointer to OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with cryptographic parameters added.</p> <p>Failure: NULL pointer.</p>

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
okvAttrAddCryptoParams(env, ttlv, BLK_CIPHER_ECB, PADDING_SSL3,
                      HASH_ALG_MD4, KEY_ROLE_CVK);
```

Related Topics

- [okvAttrAddCryptoAlgo](#)
`okvAttrAddCryptoAlgo` adds a cryptographic algorithm attribute to an OKVTTLV object.
- [okvAttrGetCryptoAlgo](#)
`okvAttrGetCryptoAlgo` gets the cryptographic algorithm attribute value from an OKVTTLV object.
- [okvAttrAddCryptoLen](#)
`okvAttrAddCryptoLen` adds a cryptographic length attribute to an OKVTTLV object.
- [okvAttrGetCryptoLen](#)
`okvAttrGetCryptoLen` gets the cryptographic length attribute value from an OKVTTLV object.
- [okvAttrGetCryptoParams](#)
`okvAttrGetCryptoParams` gets the cryptographic parameters attribute found at or after element index `elem_index`.

12.1.14 okvAttrAddCryptoUsageMask

`okvAttrAddCryptoUsageMask` adds a cryptographic usage mask attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddCryptoUsageMask` adds a cryptographic usage mask attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddCryptoUsageMask(OKVEnv *env, OKVTTLV *ttl,
                                     ub4 mask);
```

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to parent OKVTTLV Object.
mask	IN	Cryptographic usage mask.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with cryptographic usage mask attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
OKVTTLV *resultttl;
resultttl = okvAttrAddCryptoUsageMask(env, ttl, (ub4)12);
```

Related Topics

- [okvAttrGetCryptoUsageMask](#)
okvAttrGetCryptoUsageMask gets the cryptographic usage mask attribute value from an OKVTTLV object.

12.1.15 okvAttrAddDeactivationDate

okvAttrAddDeactivationDate adds a deactivation date attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrAddDeactivationDate adds a deactivation date attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddDeactivationDate(OKVEnv *env, OKVTTLV *ttl,
                                     ub8 deactivation_date);
```


Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to parent OKVTTLV object.
deactivation_date	IN	Deactivation date

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with deactivation date attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
time_t  current_time = time((time_t *)NULL);
...
okvAttrAddDeactivationDate(env, ttlv, (ub8) current_date + 1800);
```

Related Topics

- [okvAttrGetDeactivationDate](#)
okvAttrGetDeactivationDate gets the deactivation date attribute value from an OKVTTLV object.

12.1.16 okvAttrAddDestroyDate

okvAttrAddDestroyDate adds a destroy date attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrAddDestroyDate adds a destroy date attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddDestroyDate(OKVEnv *env, OKVTTLV *ttl,
                                ub8 destroy_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to parent OKVTTLV Object.
destroy_date	IN	Destroy date.

Return Values

Return Value	Description
OKVTTLV *	<p>Pointer to OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with destroy date attribute value added.</p> <p>Failure: NULL pointer.</p>

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
time_t current_time = time((time_t *)NULL);
...
okvAttrAddDestroyDate(env, attr_in, (ub8) current_time + 24*3*3600);
```

Related Topics

- [okvAttrGetDestroyDate](#)
okvAttrGetDestroyDate gets the destroy date attribute value from an OKVTTLV object.

12.1.17 okvAttrAddDigest

okvAttrAddDigest adds a digest attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrAddDigest adds a digest attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddDigest(OKVEnv *env, OKVTTLV *ttl,
                           ub4 hash_algo, ub4 key_format_type,
                           oratext *digest, ub4 digestl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlvs	IN	Pointer to parent OKVTTLV Object.
hash_algo	IN	Hash algorithm.
key_format_type	IN	Key format type.
digest	IN	Digest value.
digestl	IN	Digest value length.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with digest attribute values added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
oracertext digest[] = "Sample_Digest";
okvAddAttributeObject(env, ttlvs, OKVAttrDigest, 1);
resultttlvs = okvAttrAddDigest(env, ttlvs, HASH_ALG_SHA_1, OKVDEF_KEY_FMT_OPAQUE,
                               &digest[0], sizeof(digest));
```

Related Topics

- [okvAttrGetDigest](#)
okvAttrGetDigest gets the digest attribute found at or after element index elem_index.
- [okvAttrGetDigestLen](#)
okvAttrGetDigestLen gets the length of the digest value of the digest attribute found at or after element index elem_index.

12.1.18 okvAttrAddDigitalSignAlgo

okvAttrAddDigitalSignAlgo adds a digital signature algorithm attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddDigitalSignAlgo` adds a digital signature algorithm attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddDigitalSignAlgo(OKVEnv *env, OKVTTLV *ttl,
                                     ub4 digital_sign_alg);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV object.
<code>digital_sign_alg</code>	IN	Digital Signature Algorithm.

Return Values

Return Value	Description
OKVTTLV *	<p>Pointer to OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with digital signature algorithm attribute value added.</p> <p>Failure: NULL Pointer.</p>

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
okvAttrAddDigitalSignAlgo(env, ttl, SIGN_ALG_SHA256_W_RSA);
```

Related Topics

- [okvAttrGetDigitalSignAlgo](#)
`okvAttrGetDigitalSignAlgo` gets the digital signature algorithm attribute value from an OKVTTLV object.

12.1.19 okvAttrAddExtractable

`okvAttrAddExtractable` adds an extractable attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddExtractable` adds an extractable attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddExtractable(OKVEnv *env, OKVTTLV *ttl, ub8 extractable);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV object.
<code>extractable</code>	IN	Extractable attribute value.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with extractable attribute value added. Failure: NULL Pointer.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
okvAttrAddExtractable(env, ttl, (ub8)1);
```

Related Topics

- [okvAttrGetExtractable](#)
`okvAttrGetExtractable` gets the extractable attribute value from an OKVTTLV object.

12.1.20 okvAttrAddFresh

`okvAttrAddFresh` adds a fresh attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddFresh` adds a fresh attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddFresh(OKVEnv *env, OKVTTLV *ttl, ub8 fresh);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to parent OKVTTLV Object.
<code>fresh</code>	IN	Fresh attribute.

Return Values

Return Value	Description
<code>OKVTTLV *</code>	<p>Pointer to OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with fresh attribute value added.</p> <p>Failure: NULL pointer.</p>

Comments

The fresh attribute can take values 0 or 1 for false or true respectively.

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
OKVTTLV *resultttl;
resultttl = okvAttrAddFresh(env, attr_in, (ub8) 1);
```

Related Topics

- [okvAttrGetFresh](#)
`okvAttrGetFresh` gets the fresh attribute value from an OKVTTLV object.

12.1.21 okvAttrAddInitialDate

`okvAttrAddInitialDate` adds an initial date attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddInitialDate` adds an initial date attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddInitialDate(OKVEnv *env, OKVTTLV *ttl,
                               ub8 initial_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to OKVTTLV object.
initial_date	IN	Initial date.

Return Values

Return Value	Description
OKVTTLV *	<p>Pointer to OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with initial date attribute value added.</p> <p>Failure: NULL Pointer.</p>

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
time_t current_time = time((time_t *)NULL);
okvAttrAddInitialDate(env, ttl, (ub8) current_time + 10000);
```

Related Topics

- [okvAttrGetInitialDate](#)
okvAttrGetInitialDate gets the initial date attribute value from an OKVTTLV object.

12.1.22 okvAttrAddLastChangeDate

okvAttrAddLastChangeDate adds a last change date attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrAddLastChangeDate adds a last change date attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddLastChangeDate(OKVEnv *env, OKVTTLV *ttl,
                                   ub8 last_change_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to OKVTTLV object.
last_change_date	IN	Last Change date.

Return Values

Return Value	Description
OKVTTLV *	<p>Pointer to OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with last change date attribute value added.</p> <p>Failure: NULL Pointer.</p>

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
time_t current_time = time((time_t *)NULL);
okvAttrAddLastChangeDate(env, ttl, (ub8) current_time + 10000);
```

Related Topics

- [okvAttrGetLastChangeDate](#)
okvAttrGetLastChangeDate gets the last change date attribute value from an OKVTTLV object.

12.1.23 okvAttrAddLeaseTime

okvAttrAddLeaseTime adds a lease time attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrAddLeaseTime adds a lease time attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddLeaseTime(OKVEnv *env, OKVTTLV *ttl,
                             ub4 lease_time);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to parent OKVTTLV Object.
lease_time	IN	Lease time.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with lease time attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
OKVTTLV *resultttl;
resultttl = okvAttrAddLeaseTime(env, ttl, (ub4)100);
```

Related Topics

- [okvAttrGetLeaseTime](#)
okvAttrGetLeaseTime gets the lease time attribute value from an OKVTTLV object.

12.1.24 okvAttrAddName

okvAttrAddName adds a name attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrAddName adds a name attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddName(OKVEnv *env, OKVTTLV *ttl,
                        oratext *name, ub4 name1, ub4 typ);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to parent OKVTTLV Object.
name	IN	Name value of the name attribute.
name1	IN	Length of name value of the name attribute.
typ	IN	Type of the name attribute.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with name attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
oratext[] name_value = "sample name";
ub4 name_value1 = strlen((const char *)name_value);
okvAttrAddName(env, attr_in, (oratext *) name_value, name_value1, 1);
```

Related Topics

- [okvAttrGetName](#)
okvAttrGetName gets the name value, attribute index, and name type of the name attribute found at or after element index elem_index.
- [okvAttrGetNameValueLen](#)
okvAttrGetNameValueLen gets the length of the name value of the name attribute found at or after element index elem_index.

12.1.25 okvAttrAddNeverExtractable

`okvAttrAddNeverExtractable` adds a never extractable attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddNeverExtractable` adds a never extractable attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddNeverExtractable(OKVEnv *env, OKVTTLV *ttl,
                                     ub8 never_extractable);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV object.
<code>never_extractable</code>	IN	Never extractable attribute value.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with never extractable attribute value added. Failure: NULL Pointer.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
okvAttrAddNeverExtractable(env, ttl, (ub8)1);
```

Related Topics

- [okvAttrGetNeverExtractable](#)
okvAttrGetNeverExtractable gets the never extractable attribute value from an OKVTTLV object.

12.1.26 okvAttrAddObjectGroup

okvAttrAddObjectGroup adds an object group attribute to an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrAddObjectGroup adds an object group attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddObjectGroup(OKVEnv *env, OKVTTLV *ttl,
                                oratext *object_group,
                                ub4 object_group1);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to parent OKVTTLV Object.
object_group	IN	Object group of the object group attribute.
object_group1	IN	Length of object group of the object group attribute.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with object group attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
OKVTTLV *resultttl;
oratext obj_grp[] = "Object_Group";
resultttl = okvAttrAddObjectGroup(env, ttl, &obj_grp[0], strlen(obj_grp));
```

Related Topics

- [okvAttrGetObjectGroup](#)
okvAttrGetObjectGroup gets the object group value of the object group attribute found at or after element index elem_index.
- [okvAttrGetObjectGroupLen](#)
okvAttrGetObjectGroupLen gets the length of the object group value of the object group attribute found at or after element index elem_index.

12.1.27 okvAttrAddObjectType

okvAttrAddObjectType adds an object type attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrAddObjectType adds an object type attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddObjectType(OKVEnv *env, OKVTTLV *ttl,
                               OKVObjNo typ);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to parent OKVTTLV Object.
typ	IN	Type of the object type attribute.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with object type attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
okvAttrAddObjectType(env, req, OKVObjSymmetric);
```

Related Topics

- [okvAttrGetObjectType](#)
okvAttrGetObjectType gets the object type attribute value from an OKVTTLV object.

12.1.28 okvAttrAddProcessStartDate

okvAttrAddProcessStartDate adds a process start date attribute to an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrAddProcessStartDate adds a process start date attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddProcessStartDate(OKVEnv *env, OKVTTLV *ttl,
                                     ub8 process_start_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to parent OKVTTLV Object.
process_start_date	IN	Process start date.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with process start date attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
time_t current_time = time((time_t *)NULL);
...
okvAttrAddProcessStartDate(env, attr_temp, (ub8) current_time + 1000);
```

Related Topics

- [okvAttrGetProcessStartDate](#)
okvAttrGetProcessStartDate gets the process start date attribute value from an OKVTTLV object.

12.1.29 okvAttrAddProtectStopDate

`okvAttrAddProtectStopDate` adds a protect stop date attribute to an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrAddProtectStopDate` adds a protect stop date attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddProtectStopDate(OKVEnv *env, OKVTTLV *ttl,
                                     ub8 protect_stop_date);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to parent OKVTTLV Object.
<code>protect_stop_date</code>	IN	Protect stop date.

Return Values

Return Value	Description
<code>OKVTTLV *</code>	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with protect stop date attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
time_t current_time = time((time_t *)NULL);
...
okvAttrAddProtectStopDate(env, attr_in, (ub8) current_time + 24*3600);
```

Related Topics

- [okvAttrGetProtectStopDate](#)
`okvAttrGetProtectStopDate` gets the protect stop date attribute value from an OKVTTLV object.

12.1.30 okvAttrAddRevocationReason

`okvAttrAddRevocationReason` adds the revocation reason attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddRevocationReason` adds the revocation reason attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddRevocationReason(OKVEnv *env, OKVTTLV *ttl,
                                     ub4 code, oratext *msg, ub4 msgl);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to parent OKVTTLV object.
<code>code</code>	IN	Revocation code.
<code>msg</code>	IN	Revocation message.
<code>msgl</code>	IN	Revocation message length.

Return Values

Return Value	Description
<code>OKVTTLV *</code>	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with revocation attribute values added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
oratext msg[] = "Object_Compromised";
OKVTTLV *resultttl;
resultttl = okvAttrAddRevocationReason(env, ttl, OKVDEF_REV_CODE_KEY_COMP, &msg[0],
                                       sizeof(msg));
```

Related Topics

- [okvAttrGetRevocationReason](#)
`okvAttrGetRevocationReason` gets the revocation reason attribute value from an OKVTTLV object.

- [okvAttrGetRevocationReasonMessageLen](#)
`okvAttrGetRevocationReasonMessageLen` gets the length of the revocation message value of the revocation reason attribute.

12.1.31 okvAttrAddState

`okvAttrAddState` adds a state attribute to an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrAddState` adds a state attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddState(OKVEnv *env, OKVTTLV *ttl, ub4 state);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV object.
<code>state</code>	IN	State.

Return Values

Return Value	Description
<code>OKVTTLV *</code>	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with state attribute value added. Failure: NULL Pointer.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
okvAttrAddState(env, ttl, (ub4)1);
```

Related Topics

- [okvAttrGetState](#)
`okvAttrGetState` gets the state attribute value from an OKVTTLV object.

12.1.32 okvAttrAddUniqueID

okvAttrAddUniqueID adds a unique identifier attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrAddUniqueID adds a unique identifier attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddUniqueID(OKVEnv *env, OKVTTLV *ttl,
                             oratext *uid, ub4 uidl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to parent OKVTTLV object.
uid	IN	Unique identifier.
uidl	IN	Unique identifier length.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with the unique identifier attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
OKVTTLV *resultttl;
oratext uidval[] = "12345678901234567890";
resultttl = okvAttrAddUniqueID(env, ttl, &uidval[0], strlen(uidval));
```

Related Topics

- [okvAttrGetUniqueID](#)
okvAttrGetUniqueID gets the unique identifier attribute value from an OKVTTLV object.
- [okvAttrGetUniqueIDLen](#)
okvAttrGetUniqueIDLen gets the length of the unique identifier value of the unique identifier attribute.

12.1.33 okvAttrAddUsageLimits

`okvAttrAddUsageLimits` adds a usage limits attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddUsageLimits` adds a usage limits attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddUsageLimits(OKVEnv *env, OKVTTLV *ttl,
                                ub8 total, ub8 count, ub4 unit);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to parent OKVTTLV object.
<code>total</code>	IN	Usage limits total.
<code>count</code>	IN	Usage limits count.
<code>unit</code>	IN	Usage limits type.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with usage limits attribute value added. Failure: NULL pointer.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
OKVTTLV *resultttl;
resultttl = okvAttrAddUsageLimits(env, ttl, (ub8) 256, (ub8) 256, (ub4) 1);
```

Related Topics

- [okvAttrGetUsageLimits](#)
`okvAttrGetUsageLimits` gets the usage limits attribute value from an OKVTTLV object.

12.1.34 okvAttrAddX509CertId

`okvAttrAddX509CertId` adds an issuer and serial number which forms the X.509 Certificate ID attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddX509CertId` adds an issuer and serial number which forms the X.509 Certificate ID attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddX509CertId(OKVEnv *env, OKVTTLV *ttl,
                               oratext *issuer, ub4 issuerl,
                               oratext *serialno, ub4 serialnol);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV object.
<code>issuer</code>	IN	Certificate issuer.
<code>issuerl</code>	IN	Certificate issuer length.
<code>serialno</code>	IN	Certificate serial number.
<code>serialnol</code>	IN	Certificate serial number length.

Return Values

Return Value	Description
<code>OKVTTLV *</code>	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with X.509 certificate id attribute value added. Failure: NULL pointer.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
oratext issuer[] = " DN
CN=sample_issuer,OU=demo,O=Software,L=Redwood_City,ST=California,C=us";
oratext serialno[] = "0x01";
okvAttrAddX509CertId(env, ttlv, &issuer[0], strlen(issuer),
                    &serialno[0], strlen(serialno));
```

Related Topics

- [okvAttrGetX509CertId](#)
okvAttrGetX509CertId gets the X.509 Certificate ID attribute value from an OKVTTLV object.
- [okvAttrGetX509CertIdIssuerLen](#)
okvAttrGetX509CertIdIssuerLen gets the length of the certificate issuer value of the X.509 Certificate ID attribute from an OKVTTLV object.
- [okvAttrGetX509CertIdSerialNoLen](#)
okvAttrGetX509CertIdSerialNoLen gets the length of the certificate serial number value of the X.509 Certificate ID attribute from an OKVTTLV object.

12.1.35 okvAttrAddX509CertIss

okvAttrAddX509CertIss adds a X.509 Certificate Issuer distinguished name attribute to an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrAddX509CertIss adds a X.509 Certificate Issuer distinguished name attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddX509CertIss(OKVEnv *env, OKVTTLV *ttlv,
                               oratext *dn, ub4 dn1);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to OKVTTLV object.
dn	IN	Certificate issuer distinguished name.
dn1	IN	Certificate issuer distinguished name length.

Return Values

Return Value	Description
OKVTTLV *	<p>Pointer to OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with X.509 certificate issuer distinguished name attribute value added.</p> <p>Failure: NULL Pointer.</p>

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```

oratext dn[] = "DN
CN=sample_issuer,OU=demo,O=Software,L=Redwood_City,ST=California,C=us";
ub4 dnl = strlen((const char *)dn);

okvAttrAddX509CertIss(env, ttlv, &dn[0], dnl);

```

Related Topics

- [okvAttrAddX509CertIssAltName](#)
okvAttrAddX509CertIssAltName adds a X.509 Certificate Issuer Alternate name attribute to an OKVTTLV object.
- [okvAttrGetX509CertIss](#)
okvAttrGetX509CertIss gets the X.509 Certificate Issuer distinguished name attribute value from an OKVTTLV object.
- [okvAttrGetX509CertIssAltName](#)
okvAttrGetX509CertIssAltName gets the X.509 Certificate Issuer alternate name attribute value from an OKVTTLV object found at or after the element index elem_index.
- [okvAttrGetX509CertIssAltNameLen](#)
okvAttrGetX509CertIssAltNameLen gets the length of the X.509 Certificate Issuer Alternate name value from an OKVTTLV object found at or after the element index elem_index.
- [okvAttrGetX509CertIssDNLen](#)
okvAttrGetX509CertIssDNLen gets the length of the X.509 Certificate Issuer distinguished name value from an OKVTTLV object.

12.1.36 okvAttrAddX509CertIssAltName

`okvAttrAddX509CertIssAltName` adds a X.509 Certificate Issuer Alternate name attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddX509CertIssAltName` adds a X.509 Certificate Issuer Alternate name attribute to an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrAddX509CertIssAltName(OKVEnv *env, OKVTTLV *ttl,
                                       oratext *alt_name, ub4 alt_name1);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV object.
<code>alt_name</code>	IN	Certificate issuer alternate name.
<code>alt_name1</code>	IN	Certificate issuer alternate name length.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
oratext alt_name[] = "www.example.com";
ub4 alt_name1 = strlen((const char *)dn);

okvAttrAddX509CertIssAltName(env, ttl, &alt_name[0], alt_name1);
```

Related Topics

- [okvAttrAddX509CertIss](#)
`okvAttrAddX509CertIss` adds a X.509 Certificate Issuer distinguished name attribute to an OKVTTLV object.
- [okvAttrGetX509CertIss](#)
`okvAttrGetX509CertIss` gets the X.509 Certificate Issuer distinguished name attribute value from an OKVTTLV object.
- [okvAttrGetX509CertIssAltName](#)
`okvAttrGetX509CertIssAltName` gets the X.509 Certificate Issuer alternate name attribute value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertIssAltNameLen](#)
`okvAttrGetX509CertIssAltNameLen` gets the length of the X.509 Certificate Issuer Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertIssDNLen](#)
`okvAttrGetX509CertIssDNLen` gets the length of the X.509 Certificate Issuer distinguished name value from an OKVTTLV object.

12.1.37 okvAttrAddX509CertSubj

`okvAttrAddX509CertSubj` adds a X.509 Certificate Subject distinguished name attribute to an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrAddX509CertSubj` adds a X.509 Certificate Subject distinguished name attribute to an OKVTTLV object.

Syntax

```
OKVTTLV *okvAttrAddX509CertSubj(OKVEnv *env, OKVTTLV *ttl,
                                oratext *dn, ub4 dn1);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV object.
<code>dn</code>	IN	Certificate subject distinguished name.
<code>dn1</code>	IN	Certificate subject distinguished name length.

Return Values

Return Value	Description
OKVTTLV *	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with X.509 certificate subject distinguished name attribute value added. Failure: NULL pointer.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs

Example

```
oratest dn[] = "DN
CN=sample_subject,OU=demo,O=Software,L=Redwood_City,ST=California,C=us";
ub4 dnl = strlen((const char *)dn);
okvAttrAddX509CertSubj(env, ttlv, &dn[0], dnl);
```

Related Topics

- [okvAttrAddX509CertSubjAltName](#)
`okvAttrAddX509CertSubjAltName` adds a X.509 Certificate Subject Alternate name attribute to an OKVTTLV object.
- [okvAttrGetX509CertSubj](#)
`okvAttrGetX509CertSubj` gets the X.509 Certificate Subject distinguished name attribute value from an OKVTTLV object.
- [okvAttrGetX509CertSubjAltName](#)
`okvAttrGetX509CertSubjAltName` gets the X.509 Certificate Subject alternate name attribute value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertSubjAltNameLen](#)
`okvAttrGetX509CertSubjAltNameLen` gets the length of the X.509 Certificate Subject Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertSubjDNLen](#)
`okvAttrGetX509CertSubjDNLen` gets the length of the X.509 Certificate Subject distinguished name value from an OKVTTLV object.

12.1.38 okvAttrAddX509CertSubjAltName

`okvAttrAddX509CertSubjAltName` adds a X.509 Certificate Subject Alternate name attribute to an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrAddX509CertSubjAltName` adds a X.509 Certificate Subject Alternate name attribute to an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrAddX509CertSubjAltName(OKVEnv *env, OKVTTLV *ttl,
                                         oratext *alt_name, ub4 alt_name1);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV object.
<code>alt_name</code>	IN	Certificate subject alternate name.
<code>alt_name1</code>	IN	Certificate subject alternate name length.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

This API does only the client side processing to build the OKVTTLV object that needs to be sent to the Oracle Key Vault server. It does not do any server operation like the KMIP APIs.

Example

```
oratext alt_name[] = "www.example.com";
ub4 alt_name1 = strlen((const char *)dn);
okvAttrAddX509CertSubjAltName(env, ttl, &alt_name[0], alt_name1);
```

Related Topics

- [okvAttrAddX509CertSubjAltName](#)
`okvAttrAddX509CertSubjAltName` adds a X.509 Certificate Subject Alternate name attribute to an OKVTTLV object.
- [okvAttrGetX509CertSubj](#)
`okvAttrGetX509CertSubj` gets the X.509 Certificate Subject distinguished name attribute value from an OKVTTLV object.
- [okvAttrGetX509CertSubjAltName](#)
`okvAttrGetX509CertSubjAltName` gets the X.509 Certificate Subject alternate name attribute value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertSubjAltNameLen](#)
`okvAttrGetX509CertSubjAltNameLen` gets the length of the X.509 Certificate Subject Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertSubjDNLen](#)
`okvAttrGetX509CertSubjDNLen` gets the length of the X.509 Certificate Subject distinguished name value from an OKVTTLV object.

12.1.39 okvAttrGetActivationDate

`okvAttrGetActivationDate` gets the activation date attribute value from an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrGetActivationDate` gets the activation date attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetActivationDate(OKVEnv *env, OKVTTLV *ttl,
                                   ub8 *activation_date);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to parent OKVTTLV Object.
<code>activation_date</code>	OUT	Activation date.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub8 act_date;
okvAttrGetActivationDate(env, ttlv, &act_date);
```

Related Topics

- [okvAttrAddActivationDate](#)
okvAttrAddActivationDate adds the activation date attribute to an OKVTTLV object.

12.1.40 okvAttrGetArchiveDate

okvAttrGetArchiveDate gets the archive date attribute value from an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrGetArchiveDate gets the archive date attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetArchiveDate(OKVEnv *env, OKVTTLV *ttlv,
                                ub8 *archive_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to parent OKVTTLV Object.
archive_date	OUT	Archive date.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub8 archive_date;
okvAttrGetArchiveDate(env, ttlv, &archive_date);
```

12.1.41 okvAttrGetCertLen

okvAttrGetCertLen gets the certificate length attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetCertLen gets the certificate length attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetCertLen(OKVEnv *env, OKVTTLV *ttlv,
                           ub4 *cert_len);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to the OKVTTLV object.
cert_len	OUT	Certificate length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
ub4 cert_len = 0;
okvAttrGetCertLen(env, ttlv, &cert_len);
```

Related Topics

- [okvAttrAddCertLen](#)
okvAttrAddCertLen adds a certificate length attribute to an OKVTTLV object.
- [okvAttrAddCertType](#)
okvAttrAddCertType adds a certificate type attribute to an OKVTTLV object.
- [okvAttrGetCertType](#)
okvAttrGetCertType gets the certificate type attribute value from an OKVTTLV object.

12.1.42 okvAttrGetCertType

okvAttrGetCertType gets the certificate type attribute value from an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrGetCertType gets the certificate type attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetCertType(OKVEnv *env, OKVTTLV *ttlv,
                             ub4 *cert_typ);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to the OKVTTLV object.
cert_typ	OUT	Certificate type.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
ub4 cert_type = 0;  
okvAttrGetCertType(env, ttlv, &cert_type);
```

Related Topics

- [okvAttrAddCertLen](#)
`okvAttrAddCertLen` adds a certificate length attribute to an OKVTTLV object.
- [okvAttrAddCertType](#)
`okvAttrAddCertType` adds a certificate type attribute to an OKVTTLV object.
- [okvAttrGetCertLen](#)
`okvAttrGetCertLen` gets the certificate length attribute value from an OKVTTLV object.

12.1.43 okvAttrGetCompromiseDate

`okvAttrGetCompromiseDate` gets the compromise date attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrGetCompromiseDate` gets the compromise date attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetCompromiseDate(OKVEnv *env, OKVTTLV *ttlv,  
                                   ub8 *comp_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to the OKVTTLV object.
comp_date	OUT	Compromise date.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub8 comp_date;
okvAttrGetCompromiseDate(env, ttlv, &comp_date);
```

Related Topics

- [okvAttrAddCompromiseDate](#)
okvAttrAddCompromiseDate adds a compromise date attribute to an OKVTTLV object.

12.1.44 okvAttrGetCompromiseOccurrenceDate

okvAttrGetCompromiseOccurrenceDate gets the compromise occurrence date attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetCompromiseOccurrenceDate gets the compromise occurrence date attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetCompromiseOccurrenceDate(OKVEnv *env, OKVTTLV *ttl,
                                             ub8 *comp_occr_date);
```


Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault Environment handle.
ttlv	IN	Pointer to the OKVTTLV object.
comp_occ_date	OUT	Compromise occurrence date.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub8 comp_occ_date;
OKVTTLV *resultttl;
resultttl = okvAttrGetCompromiseOccurrenceDate(env, ttlv, &comp_occ_date);
```

Related Topics

- [okvAttrAddCompromiseOccurrenceDate](#)
okvAttrAddCompromiseOccurrenceDate adds a compromise occurrence date attribute to an OKVTTLV object.

12.1.45 okvAttrGetContactInfo

okvAttrGetContactInfo gets the contact information attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetContactInfo gets the contact information attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetContactInfo(OKVEnv *env, OKVTTLV *ttl,
                                oratext *contact_info, ub4 *contact_info);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault Environment handle
ttlv	IN	Pointer to the parent OKVTTLV Object
contact_info	OUT	Contact information
contact_infoLen	OUT	Length of contact information

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The memory for the argument `contact_info` must be allocated before you execute the `okvAttrGetContactInfo` function call. You can find the size by using `okvAttrGetContactInfoLen`.

Example

```
ub4 contactl;
contactl = okvAttrGetContactInfoLen(env, ttlv);
contact = calloc(contactl, sizeof(oratext));
okvAttrGetContactInfo(env, ttlv, contact, &contactl);
```

Related Topics

- [okvAttrAddContactInfo](#)
`okvAttrAddContactInfo` adds a contact information attribute to an OKVTTLV object.
- [okvAttrGetContactInfoLen](#)
`okvAttrGetContactInfoLen` gets the length of the contact information value of the contact information attribute.

12.1.46 okvAttrGetContactInfoLen

`okvAttrGetContactInfoLen` gets the length of the contact information value of the contact information attribute.

Category

KMIP attribute API

Purpose

`okvAttrGetContactInfoLen` gets the length of the contact information value of the contact information attribute.

Syntax

```
ub4 okvAttrGetContactInfoLen(OKVEnv *env, OKVTTLV *ttl);
```

Parameters

Parameters	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault Environment handle
ttl	IN	Pointer to parent OKVTTLV Object

Return Values

Return Value	Description
ub4	Length of the attribute value. Success: Length of the contact information attribute value. Failure: 0.

Comments

None.

Example

```
ub4 cinfo;
cinfo = okvAttrGetContactInfoLen(env, ttl);
```

Related Topics

- [okvAttrAddContactInfo](#)
okvAttrAddContactInfo adds a contact information attribute to an OKVTTLV object.
- [okvAttrGetContactInfo](#)
okvAttrGetContactInfo gets the contact information attribute value from an OKVTTLV object.

12.1.47 okvAttrGetCryptoAlgo

okvAttrGetCryptoAlgo gets the cryptographic algorithm attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetCryptoAlgo gets the cryptographic algorithm attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetCryptoAlgo(OKVEnv *env, OKVTTLV *ttl,
                              ub4 *crypto_alg);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault Environment handle.
ttl	IN	Pointer to the OKVTTLV object.
crypto_alg	OUT	Cryptographic algorithm.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub4 alg = 0;
okvAttrGetCryptoAlgo(env, ttl, &alg);
```

Related Topics

- [okvAttrAddCryptoAlgo](#)
okvAttrAddCryptoAlgo adds a cryptographic algorithm attribute to an OKVTTLV object.
- [okvAttrAddCryptoLen](#)
okvAttrAddCryptoLen adds a cryptographic length attribute to an OKVTTLV object.
- [okvAttrGetCryptoLen](#)
okvAttrGetCryptoLen gets the cryptographic length attribute value from an OKVTTLV object.
- [okvAttrAddCryptoParams](#)
okvAttrAddCryptoParams adds cryptographic parameters to an OKVTTLV object.
- [okvAttrGetCryptoParams](#)
okvAttrGetCryptoParams gets the cryptographic parameters attribute found at or after element index elem_index.

12.1.48 okvAttrGetCryptoLen

`okvAttrGetCryptoLen` gets the cryptographic length attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrGetCryptoLen` gets the cryptographic length attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetCryptoLen(OKVEnv *env, OKVTTLV *ttl,
                             ub4 *crypto_len);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle
<code>ttl</code>	IN	Pointer to the OKVTTLV object
<code>crypto_len</code>	OUT	Cryptographic length

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub4 len = 0;
okvAttrGetCryptoLen(env, ttl, &len);
```

Related Topics

- [okvAttrAddCryptoAlgo](#)
`okvAttrAddCryptoAlgo` adds a cryptographic algorithm attribute to an OKVTTLV object.
- [okvAttrGetCryptoAlgo](#)
`okvAttrGetCryptoAlgo` gets the cryptographic algorithm attribute value from an OKVTTLV object.

- [okvAttrAddCryptoLen](#)
okvAttrAddCryptoLen adds a cryptographic length attribute to an OKVTTLV object.
- [okvAttrAddCryptoParams](#)
okvAttrAddCryptoParams adds cryptographic parameters to an OKVTTLV object.
- [okvAttrGetCryptoParams](#)
okvAttrGetCryptoParams gets the cryptographic parameters attribute found at or after element index elem_index.

12.1.49 okvAttrGetCryptoParams

okvAttrGetCryptoParams gets the cryptographic parameters attribute found at or after element index elem_index.

Category

KMIP attribute API

Purpose

okvAttrGetCryptoParams gets the cryptographic parameters attribute found at or after element index elem_index in the parent TTLV.

Syntax

```
OKVErrNo okvAttrGetCryptoParams(OKVEnv *env, OKVTTLV *ttl,
                                ub4 *elem_index,
                                ub4 *block_cipher_mode, ub4 *padding_method,
                                ub4 *hashing_algorithm, ub4 *key_role_type);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to parent TTLV object.
elem_index	IN/OUT	Element index.
block_cipher_mode	OUT	Block cipher mode.
padding_method	OUT	Padding method.
hashing_algorithm	OUT	Hashing algorithm.
key_role_type	OUT	Key role type.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub4 bcm, pm, ha, krt, ind;
okvAttrGetCryptoParams(env, ttlv, &ind, &bcm, &pm, &ha, &krt);
```

Related Topics

- [okvAttrAddCryptoAlgo](#)
okvAttrAddCryptoAlgo adds a cryptographic algorithm attribute to an OKVTTLV object.
- [okvAttrAddCryptoLen](#)
okvAttrAddCryptoLen adds a cryptographic length attribute to an OKVTTLV object.
- [okvAttrAddCryptoParams](#)
okvAttrAddCryptoParams adds cryptographic parameters to an OKVTTLV object.
- [okvAttrGetCryptoAlgo](#)
okvAttrGetCryptoAlgo gets the cryptographic algorithm attribute value from an OKVTTLV object.
- [okvAttrGetCryptoLen](#)
okvAttrGetCryptoLen gets the cryptographic length attribute value from an OKVTTLV object.

12.1.50 okvAttrGetCryptoUsageMask

okvAttrGetCryptoUsageMask gets the cryptographic usage mask attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetCryptoUsageMask gets the cryptographic usage mask attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetCryptoUsageMask(OKVEnv *env, OKVTTLV *ttl,
                                     ub4 *mask);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle
ttl	IN	Pointer to parent OKVTTLV object
mask	OUT	Cryptographic usage mask

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub4 mask = 0;
okvAttrGetCryptoUsageMask(env, ttlv, &mask);
```

Related Topics

- [okvAttrAddCryptoUsageMask](#)
okvAttrAddCryptoUsageMask adds a cryptographic usage mask attribute to an OKVTTLV object.

12.1.51 okvAttrGetDeactivationDate

okvAttrGetDeactivationDate gets the deactivation date attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetDeactivationDate gets the deactivation date attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetDeactivationDate(OKVEnv *env, OKVTTLV *ttlv,
                                     ub8 *deactivation_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle
ttlv	IN	Pointer to OKVTTLV object
deactivation_date	OUT	Deactivation date

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub8 deact_date;
okvAttrGetDeactivationDate(env, ttlv, &deact_date);
```

Related Topics

- [okvAttrAddDeactivationDate](#)
okvAttrAddDeactivationDate adds a deactivation date attribute to an OKVTTLV object.

12.1.52 okvAttrGetDestroyDate

okvAttrGetDestroyDate gets the destroy date attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetDestroyDate gets the destroy date attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetDestroyDate(OKVEnv *env, OKVTTLV *ttlv,
                                ub8 *destroy_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle
ttlv	IN	Pointer to OKVTTLV object
destroy_date	OUT	Destroy date

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub8 destroy_date;
okvAttrGetDestroyDate(env, ttlv, &destroy_date);
```

12.1.53 okvAttrGetDigest

okvAttrGetDigest gets the digest attribute found at or after element index elem_index.

Category

KMIP attribute API

Purpose

okvAttrGetDigest gets the digest parameters for the OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetDigest(OKVEnv *env, OKVTTLV *ttlv,
                          ub4 *elem_index,
                          ub4 *hash_algo, ub4 *key_format_type,
                          oratext *digest, ub4 *digestl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to parent OKVTTLV object.
elem_index	IN/OUT	The API will look for the first occurrence of the child with tag OKVDEF_TAG_DIGEST from this index onwards and will return the actual index where the child was found.
hash_algo	OUT	Hash algorithm.
key_format_type	OUT	Key format type.
digest	OUT	Digest value.
digestl	IN/OUT	Digest value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The memory to store the digest value has to be allocated before this API is called. `okvAttrGetDigestLen` can be used to get the digest length.

Example

```
ub4 ei = 0, digestl = 0, hash_algo, key_format_type;
digestl = okvAttrGetDigestLen(env, ttlv, &ei);
oratext * digest = (oratext *) calloc(digestl ,sizeof(oratext) );
okvAttrGetDigest(env, ttlv, &ei, &hash_algo, &key_format_type,
                 &digest[0], &digestl);
```

Related Topics

- [okvAttrAddDigest](#)
`okvAttrAddDigest` adds a digest attribute to an OKVTTLV object.
- [okvAttrGetDigestLen](#)
`okvAttrGetDigestLen` gets the length of the digest value of the digest attribute found at or after element index `elem_index`.

12.1.54 okvAttrGetDigestLen

`okvAttrGetDigestLen` gets the length of the digest value of the digest attribute found at or after element index `elem_index`.

Category

KMIP attribute API

Purpose

`okvAttrGetDigestLen` gets the length of the digest attribute from the OKVTTLV object.

Syntax

```
ub4 okvAttrGetDigestLen(OKVEnv *env, OKVTTLV *ttlv,
                       ub4 *elem_index);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.

Parameter	IN/OUT	Description
ttlv	IN	Pointer to the OKVTTLV object.
elem_index	IN/OUT	The API will look for the first occurrence of the child with tag OKVDEF_TAG_DIGEST from this index onwards and will return the actual index where the child was found.

Return Values

Return Value	Description
ub4	Length of the attribute value. Success: Length of the digest attribute. Failure: 0.

Comments

None.

Example

```
ub4 ei = 0;
ub4 digestl;
digestl = okvAttrGetDigestLen(env, ttlv, &ei)
```

Related Topics

- [okvAttrAddDigest](#)
okvAttrAddDigest adds a digest attribute to an OKVTTLV object.
- [okvAttrGetDigest](#)
okvAttrGetDigest gets the digest attribute found at or after element index elem_index.

12.1.55 okvAttrGetDigitalSignAlgo

okvAttrGetDigitalSignAlgo gets the digital signature algorithm attribute value from an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrGetDigitalSignAlgo gets the digital signature algorithm attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetDigitalSignAlgo(OKVEnv *env, OKVTTLV *ttl,
                                   ub4 *elem_index,
                                   ub4 *digital_sign_alg);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to the OKVTTLV object.
digital_sign_alg	OUT	Digital Signature Algorithm.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
ub4 digital_sign_algo = 0;
okvAttrGetDigitalSignAlgo(env, ttlv, &digital_sign_algo);
```

Related Topics

- [okvAttrAddDigitalSignAlgo](#)
okvAttrAddDigitalSignAlgo adds a digital signature algorithm attribute to an OKVTTLV object.

12.1.56 okvAttrGetExtractable

okvAttrGetExtractable gets the extractable attribute value from an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

okvAttrGetExtractable gets the extractable attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetExtractable(OKVEnv *env, OKVTTLV *ttl, ub8 *extractable);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlV	IN	Pointer to OKVTTLV object.
extractable	OUT	Extractable attribute value.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub8 extractable;
okvAttrGetExtractable(env, ttlV, &extractable);
```

Related Topics

- [okvAttrAddExtractable](#)
okvAttrAddExtractable adds an extractable attribute to an OKVTTLV object.

12.1.57 okvAttrGetFresh

okvAttrGetFresh gets the fresh attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetFresh gets the fresh attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetFresh(OKVEnv *env, OKVTTLV *ttlV, ub8 *fresh);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle
ttlv	IN	Pointer to the parent OKVTTLV Object
fresh	OUT	Fresh attribute

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub8 fresh_val;
okvAttrGetFresh(env, attr, &fresh_val);
```

Related Topics

- [okvAttrAddFresh](#)
okvAttrAddFresh adds a fresh attribute to an OKVTTLV object.

12.1.58 okvAttrGetInitialDate

okvAttrGetInitialDate gets the initial date attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetInitialDate gets the initial date attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetInitialDate(OKVEnv *env, OKVTTLV *ttl,
                               ub8 *initial_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault Environment handle.

Parameter	IN/OUT	Description
ttl_v	IN	Pointer to OKVTTLV object.
initial_date	OUT	Initial date.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub8 ini_date;
okvAttrGetInitialDate(env, ttl_v, &ini_date);
```

12.1.59 okvAttrGetLastChangeDate

okvAttrGetLastChangeDate gets the last change date attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetLastChangeDate gets the last change date attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetLastChangeDate(OKVEnv *env, OKVTTLV *ttl_v,
                                   ub8 *last_change_date);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl_v	IN	Pointer to OKVTTLV object.
last_change_date	OUT	Last change date.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub8 last_change_date;
okvAttrGetLastChangeDate(env, ttlv, &last_change_date);
```

12.1.60 okvAttrGetLeaseTime

okvAttrGetLeaseTime gets the lease time attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetLeaseTime gets the lease time attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetLeaseTime(OKVEnv *env, OKVTTLV *ttlv,
                             ub4 *lease_time);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault Environment handle.
ttlv	IN	Pointer to the OKVTTLV object.
lease_time	OUT	Lease time.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub4 lease_time;
okvAttrGetLeaseTime(env, ttlv, &lease_time);
```

12.1.61 okvAttrGetName

okvAttrGetName gets the name value, attribute index, and name type of the name attribute found at or after element index elem_index.

Category

KMIP attribute API

Purpose

okvAttrGetName gets the name value, name length, and name type of the name attribute from the OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetName(OKVEnv *env, OKVTTLV *ttlv,
                        ub4 *elem_index,
                        oratext *name, ub4 name1, ub4 *typ);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to the parent TTLV object.
elem_index	IN/OUT	The API will look for the first occurrence of the child with tag OKVDEF_TAG_NAME_ST from this index onwards and will return the actual index where the child was found.
name	OUT	Name value of the name attribute.
name1	IN/OUT	Length of name value of the name attribute.
typ	OUT	Type of the name attribute.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The memory to store the name value should be allocated before the function call.

Example

```
ub4 ei = 0;
ub4 nametyp;
namel = okvAttrGetNameValueLen(env, ttlv, &ei);
oratext * name = (oratext *) calloc(namel, sizeof(oratext));
okvAttrGetName(env, ttlv, &ei, name, namel, &nametyp);
```

Related Topics

- [okvAttrGetNameValueLen](#)
okvAttrGetNameValueLen gets the length of the name value of the name attribute found at or after element index elem_index.
- [okvAttrAddName](#)
okvAttrAddName adds a name attribute to an OKVTTLV object.

12.1.62 okvAttrGetNameValueLen

okvAttrGetNameValueLen gets the length of the name value of the name attribute found at or after element index elem_index.

Category

KMIP attribute API

Purpose

okvAttrGetNameValueLen gets the length of the name attribute from the OKVTTLV object.

Syntax

```
ub4 okvAttrGetNameValueLen(OKVEnv *env, OKVTTLV *ttlv,
                           ub4 *elem_index);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.

Parameter	IN/OUT	Description
<code>ttl_v</code>	IN	Pointer to the OKVTTLV buffer to search the name length.
<code>elem_index</code>	IN/OUT	The API will look for the first occurrence of the child with tag <code>OKVDEF_TAG_NAME_ST</code> from this index onwards and will return the actual index where the child was found.

Return Values

Return Value	Description
<code>ub4</code>	Length of the attribute value. Success: Length of the name attribute. Failure: 0.

Comments

None.

Example

```
ei = 0;
name1 = okvAttrGetNameValueLen(env, ttl_v, &ei);
```

Related Topics

- [okvAttrGetName](#)
`okvAttrGetName` gets the name value, attribute index, and name type of the name attribute found at or after element index `elem_index`.
- [okvAttrAddName](#)
`okvAttrAddName` adds a name attribute to an OKVTTLV object.

12.1.63 okvAttrGetNeverExtractable

`okvAttrGetNeverExtractable` gets the never extractable attribute value from an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrGetNeverExtractable` gets the never extractable attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetNeverExtractable(OKVEnv *env, OKVTTLV *ttl_v,
                                     ub8 *never_extractable);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to OKVTTLV object.
never_extractable	OUT	Never extractable attribute value.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub8 never_extractable;
okvAttrGetNeverExtractable(env, ttl, &never_extractable);
```

Related Topics

- [okvAttrAddNeverExtractable](#)
okvAttrAddNeverExtractable adds a never extractable attribute to an OKVTTLV object.

12.1.64 okvAttrGetObjectGroup

okvAttrGetObjectGroup gets the object group value of the object group attribute found at or after element index elem_index.

Category

KMIP attribute API

Purpose

okvAttrGetObjectGroup gets the object group value of the object group attribute from the OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetObjectGroup(OKVEnv *env, OKVTTLV *ttl,
                                ub4 *elem_index,
                                oratext *object_group, ub4 *object_group1);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to OKVTTLV object.
elem_index	IN/OUT	The API will look for the first occurrence of the child with tag OKVDEF_TAG_OBJ_GROUP from this index onwards and will return the actual index where the child was found.
object_group	OUT	Object group of the object group attribute.
object_group1	IN/OUT	Length of object group of the object group attribute.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The memory for `object_group` must be allocated before you execute the function call. Use `okvAttrGetObjectGroupLen` to find the size of memory to be allocated.

Example

```
ub4 index = 0, obj_grpl;
obj_grpl = okvAttrGetObjectGroupLen(env, ttl, &index);
oratext *obj_group = (oratext *)calloc(obj_grpl, sizeof(oratext));
okvAttrGetObjectGroup(env, ttl, &index, &obj_group, &obj_grpl);
```

Related Topics

- [okvAttrGetObjectGroupLen](#)
`okvAttrGetObjectGroupLen` gets the length of the object group value of the object group attribute found at or after element index `elem_index`.
- [okvAttrAddObjectGroup](#)
`okvAttrAddObjectGroup` adds an object group attribute to an OKVTTLV object.

12.1.65 okvAttrGetObjectGroupLen

`okvAttrGetObjectGroupLen` gets the length of the object group value of the object group attribute found at or after element index `elem_index`.

Category

KMIP attribute API

Purpose

`okvAttrGetObjectGroupLen` gets the length of the object group from the OKVTTLV object.

Syntax

```
ub4 okvAttrGetObjectGroupLen(OKVEnv *env, OKVTTLV *ttl,
                             ub4 *elem_index);
```

Parameters

Parameter	IN/OUT	Element index
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to the OKVTTLV object.
<code>elem_index</code>	IN/OUT	The API will look for the first occurrence of the child with tag <code>OKVDEF_TAG_OBJ_GROUP</code> from this index onwards and will return the actual index where the child was found.

Return Values

Return Value	Description
<code>ub4</code>	Length of the attribute value. Success: Length of the object group attribute value. Failure: 0.

Comments

None.

Example

```
ub4 obj_grpl, index = 0;
obj_grpl = okvAttrGetObjectGroupLen(env, ttl, &index);
```

Related Topics

- [okvAttrAddObjectGroup](#)
`okvAttrAddObjectGroup` adds an object group attribute to an OKVTTLV object.

- [okvAttrGetObjectGroup](#)
okvAttrGetObjectGroup gets the object group value of the object group attribute found at or after element index `elem_index`.

12.1.66 okvAttrGetObjectType

okvAttrGetObjectType gets the object type attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetObjectType gets the object type attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetObjectType(OKVEnv *env, OKVTTLV *ttl,
                               OKVObjNo *typ);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to OKVTTLV object.
typ	OUT	Type of the object type attribute.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub4 typ;
okvAttrGetObjectType(env, ttl, &typ);
```

Related Topics

- [okvAttrAddObjectType](#)
okvAttrAddObjectType adds an object type attribute to an OKVTTLV object.

12.1.67 okvAttrGetProcessStartDate

`okvAttrGetProcessStartDate` gets the process start date attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrGetProcessStartDate` gets the process start date attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetProcessStartDate(OKVEnv *env, OKVTTLV *ttl,
                                     ub8 *process_start_date);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV object.
<code>process_start_date</code>	OUT	Process start date.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub8 pstart_date;
okvAttrGetProcessStartDate(env, ttl, &pstart_date);
```

Related Topics

- [okvAttrAddProcessStartDate](#)
`okvAttrAddProcessStartDate` adds a process start date attribute to an OKVTTLV object.

12.1.68 okvAttrGetProtectStopDate

`okvAttrGetProtectStopDate` gets the protect stop date attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrGetProtectStopDate` gets the protect stop date attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetProtectStopDate(OKVEnv *env, OKVTTLV *ttl,
                                   ub8 *protect_stop_date);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV parent object.
<code>protect_stop_date</code>	OUT	Protect stop date.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub8 pstop_date;
okvAttrGetProtectStopDate(env, ttl, &pstop_date);
```

Related Topics

- [okvAttrAddProtectStopDate](#)
`okvAttrAddProtectStopDate` adds a protect stop date attribute to an OKVTTLV object.

12.1.69 okvAttrGetRevocationReason

`okvAttrGetRevocationReason` gets the revocation reason attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrGetRevocationReason` gets the revocation reason attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetRevocationReason(OKVEnv *env, OKVTTLV *ttl,
                                     oratext *msg, ub4 *msgl, ub4 *code);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to parent OKVTTLV object.
<code>code</code>	OUT	Revocation code.
<code>msg</code>	OUT	Revocation message.
<code>msgl</code>	IN/OUT	Revocation message length.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The memory for the `msg` argument must be allocated before the function call. The size of memory to be allocated can be retrieved by using `okvAttrGetRevocationReasonMessageLen`.

Example

```
ub4 code;
msgl = okvAttrGetRevocationReasonMessageLen(env, ttl);
revoke_reason = calloc(msgl, sizeof(oratext));
okvAttrGetRevocationReason(env, ttl, revoke_reason, &msgl, &code);
```

Related Topics

- [okvAttrAddRevocationReason](#)
okvAttrAddRevocationReason adds the revocation reason attribute to an OKVTTLV object.
- [okvAttrGetRevocationReasonMessageLen](#)
okvAttrGetRevocationReasonMessageLen gets the length of the revocation message value of the revocation reason attribute.

12.1.70 okvAttrGetRevocationReasonMessageLen

okvAttrGetRevocationReasonMessageLen gets the length of the revocation message value of the revocation reason attribute.

Category

KMIP attribute API

Purpose

okvAttrGetRevocationReasonMessageLen gets the length of the revocation message value of the revocation reason attribute.

Syntax

```
ub4 okvAttrGetRevocationReasonMessageLen(OKVEnv *env, OKVTTLV *ttl);
```

Parameters

Parameters	IN/OUT	Description
env	IN	Pointer to Oracle Key Vault environment handle.
ttl	IN	Pointer to the OKVTTLV object.

Return Values

Return Value	Description
ub4	Length of the attribute value. Success: Length of the revocation message. Failure: 0.

Comments

None.

Example

```
ub4 msg1;  
msg1 = okvAttrGetRevocationReasonMessageLen(env, ttl);
```

Related Topics

- [okvAttrAddRevocationReason](#)
`okvAttrAddRevocationReason` adds the revocation reason attribute to an OKVTTLV object.
- [okvAttrGetRevocationReason](#)
`okvAttrGetRevocationReason` gets the revocation reason attribute value from an OKVTTLV object.

12.1.71 okvAttrGetState

`okvAttrGetState` gets the state attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrGetState` gets the state attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetState(OKVEnv *env, OKVTTLV *ttl, ub4 *state);
```

Parameters

Parameter	IN/OUT	State
<code>env</code>	IN	Pointer to parent OKVTTLV object.
<code>ttl</code>	IN	Pointer to OKVTTLV parent object.
<code>state</code>	OUT	State.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub4 val_state;  
okvAttrGetState(env, attr, &val_state);
```

12.1.72 okvAttrGetUniqueID

okvAttrGetUniqueID gets the unique identifier attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetUniqueID gets the unique identifier attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetUniqueID(OKVEnv *env, OKVTTLV *ttl,
                             ub4 *elem_index,
                             oratext *uid, ub4 *uidl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttl	IN	Pointer to the OKVTTLV parent object.
elem_index	IN/OUT	The API will look for the first occurrence of the child with tag OKVDEF_TAG_ID from this index onwards and will store the actual index where the child was found.
uid	OUT	Pointer to memory storing the unique identifier.
uidl	IN/OUT	Unique identifier length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

The memory to store the UID should be allocated before API is called. To fetch the length, execute okvAttrGetUniqueIDLen.

Example

```
ub4 index = 0;
oidl = okvAttrGetUniqueIDLen(env, ttl, &index);
oratext *oid = (oratext *) calloc (oidl, sizeof(oratext));
okvAttrGetUniqueID(env, ttl, &i, &oid[0], &oidl);
```

Related Topics

- [okvAttrAddUniqueID](#)
okvAttrAddUniqueID adds a unique identifier attribute to an OKVTTLV object.
- [okvAttrGetUniqueIDLen](#)
okvAttrGetUniqueIDLen gets the length of the unique identifier value of the unique identifier attribute.

12.1.73 okvAttrGetUniqueIDLen

okvAttrGetUniqueIDLen gets the length of the unique identifier value of the unique identifier attribute.

Category

KMIP attribute API

Purpose

okvAttrGetUniqueIDLen gets the length of the unique identifier value of the unique identifier attribute.

Syntax

```
ub4 okvAttrGetUniqueIDLen(OKVEnv *env, OKVTTLV *ttl,
                          ub4 *elem_index);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttl	IN	TTLV parent object containing the UID.
elem_index	IN/OUT	The API will look for the first occurrence of the child with tag OKVDEF_TAG_ID from this index onwards and will store the actual index where the child was found.

Return Values

Return Value	Description
ub4	Length of the attribute value. Success: Positive integer indicating the length of UID. Failure: 0.

Comments

None.

Example

```

oid1 = okvAttrGetUniqueIDLen(env, ttlv, &index);
okvAttrGetUniqueID(env, ttlv, &index, &oid[0], &oid1);

```

Related Topics

- [okvAttrAddUniqueID](#)
okvAttrAddUniqueID adds a unique identifier attribute to an OKVTTLV object.
- [okvAttrGetUniqueID](#)
okvAttrGetUniqueID gets the unique identifier attribute value from an OKVTTLV object.

12.1.74 okvAttrGetUsageLimits

okvAttrGetUsageLimits gets the usage limits attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetUsageLimits() gets the usage limit attribute value from an OKVTTLV object.

Syntax

```

OKVErrNo okvAttrGetUsageLimits(OKVEnv *env, OKVTTLV *ttlv,
                                ub8 *total, ub8 *count, ub4 *unit);

```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttlv	IN	Oracle TTLV parent object.
total	OUT	Usage limits total.
count	OUT	Usage limits count.
unit	OUT	Usage limits type.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
ub4 utype;
ub8 utotal, ucount;
okvAttrGetUsageLimits(env, ttlv, &utotal, &ucount, &utype);
```

Related Topics

- [okvAttrAddUsageLimits](#)
okvAttrAddUsageLimits adds a usage limits attribute to an OKVTTLV object.

12.1.75 okvAttrGetX509CertId

okvAttrGetX509CertId gets the X.509 Certificate ID attribute value from an OKVTTLV object.

Catortory

KMIP attribute API

Purpose

okvAttrGetX509CertId gets the X.509 Certificate ID attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetX509CertId(OKVEnv *env, OKVTTLV *ttlv,
                               oratext *issuer, ub4 *issuerl,
                               oratext *serialno, ub4 *serialnol);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlv	IN	Pointer to the OKVTTLV object.
issuer	OUT	Certificate issuer.
issuerl	OUT	Certificate issuer length.
serialno	OUT	Certificate serial number.
serialnol	OUT	Certificate serial number length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

The memory to store the X.509 Certificate ID value which consists of issuer and serial number values should be allocated before this API is called.

`okvAttrGetX509CertIdIssuerLen` and `okvAttrGetX509CertIdSerialNoLen` can be used to get the issuer and serial number value lengths respectively.

Example

```
oratest *issuer = (oratest *)NULL;
oratest *serial = (oratest *)NULL;
ub4 issuer_len = okvAttrGetX509CertIdIssuerLen(env, ttlv);
ub4 serial_len = okvAttrGetX509CertIdSerialNoLen(env, ttlv);

issuer = calloc(issuer_len + 1, sizeof(oratest));
serial = calloc(serial_len + 1, sizeof(oratest));

okvAttrGetX509CertId(env, ttlv, issuer, &issuer_len,
                    serial, &serial_len);

/* Free 'issuer' and 'serial' */
```

Related Topics

- [okvAttrAddX509CertId](#)
`okvAttrAddX509CertId` adds an issuer and serial number which forms the X.509 Certificate ID attribute to an OKVTTLV object.
- [okvAttrGetX509CertIdIssuerLen](#)
`okvAttrGetX509CertIdIssuerLen` gets the length of the certificate issuer value of the X.509 Certificate ID attribute from an OKVTTLV object.
- [okvAttrGetX509CertIdSerialNoLen](#)
`okvAttrGetX509CertIdSerialNoLen` gets the length of the certificate serial number value of the X.509 Certificate ID attribute from an OKVTTLV object.

12.1.76 okvAttrGetX509CertIdIssuerLen

`okvAttrGetX509CertIdIssuerLen` gets the length of the certificate issuer value of the X.509 Certificate ID attribute from an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrGetX509CertIdIssuerLen` gets the length of the certificate issuer value of the X.509 Certificate ID attribute from an OKVTTLV object.

Syntax

```
ub4 okvAttrGetX509CertIdIssuerLen(OKVEnv *env, OKVTTLV *ttl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to the OKVTTLV object.

Return Values

Return Value	Description
ub4	Length of the attribute value. Success: Length of the certificate issuer value of the X.509 Certificate ID. Failure: 0

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
ub4 issuerl = 0;
issuerl = okvAttrGetX509CertIdIssuerLen(env, ttl);
```

Related Topics

- [okvAttrAddX509CertId](#)
okvAttrAddX509CertId adds an issuer and serial number which forms the X.509 Certificate ID attribute to an OKVTTLV object.
- [okvAttrGetX509CertId](#)
okvAttrGetX509CertId gets the X.509 Certificate ID attribute value from an OKVTTLV object.
- [okvAttrGetX509CertIdSerialNoLen](#)
okvAttrGetX509CertIdSerialNoLen gets the length of the certificate serial number value of the X.509 Certificate ID attribute from an OKVTTLV object.

12.1.77 okvAttrGetX509CertIdSerialNoLen

okvAttrGetX509CertIdSerialNoLen gets the length of the certificate serial number value of the X.509 Certificate ID attribute from an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrGetX509CertIdSerialNoLen` gets the length of the certificate serial number value of the X.509 Certificate ID attribute from an OKVTTLV object.

Syntax

```
ub4 okvAttrGetX509CertIdSerialNoLen(OKVEnv *env, OKVTTLV *ttl);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to the OKVTTLV object.

Return Values

Return Value	Description
<code>ub4</code>	Length of the attribute value. Success: Length of the certificate serial number value of the X.509 Certificate ID. Failure: 0

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
ub4 serialno1 = 0;
serialno1 = okvAttrGetX509CertIdSerialNoLen(env, ttl);
```

Related Topics

- [okvAttrAddX509CertId](#)
`okvAttrAddX509CertId` adds an issuer and serial number which forms the X.509 Certificate ID attribute to an OKVTTLV object.
- [okvAttrGetX509CertId](#)
`okvAttrGetX509CertId` gets the X.509 Certificate ID attribute value from an OKVTTLV object.
- [okvAttrGetX509CertIdIssuerLen](#)
`okvAttrGetX509CertIdIssuerLen` gets the length of the certificate issuer value of the X.509 Certificate ID attribute from an OKVTTLV object.

12.1.78 okvAttrGetX509CertIss

`okvAttrGetX509CertIss` gets the X.509 Certificate Issuer distinguished name attribute value from an OKVTTLV object.

Catetory

KMIP attribute API

Purpose

`okvAttrGetX509CertIss` gets the X.509 Certificate Issuer distinguished name attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetX509CertIss(OKVEnv *env, OKVTTLV *ttl,
                                oratext *dn, ub4 *dnl);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to the OKVTTLV object.
<code>dn</code>	OUT	Certificate Issuer distinguished name.
<code>dnl</code>	IN/OUT	Certificate Issuer distinguished name length.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

The memory to store the X.509 Certificate Issuer distinguished name value should be allocated before this API is called.

`okvAttrGetX509CertIssDNLen` can be used to get the X.509 Certificate Issuer distinguished name value length.

Example

```
oratext *issuer = (oratext *)NULL;
ub4 issuer_len = okvAttrGetX509CertIssDNLen(env, ttl);
```

```

issuer = calloc(issuer_len + 1, sizeof(oratext));

okvAttrGetX509CertIss(env, ttlv, issuer, &issuer_len);

/* Free 'issuer' */

```

Related Topics

- [okvAttrAddX509CertIss](#)
okvAttrAddX509CertIss adds a X.509 Certificate Issuer distinguished name attribute to an OKVTTLV object.
- [okvAttrAddX509CertIssAltName](#)
okvAttrAddX509CertIssAltName adds a X.509 Certificate Issuer Alternate name attribute to an OKVTTLV object.
- [okvAttrGetX509CertIssAltName](#)
okvAttrGetX509CertIssAltName gets the X.509 Certificate Issuer alternate name attribute value from an OKVTTLV object found at or after the element index elem_index.
- [okvAttrGetX509CertIssAltNameLen](#)
okvAttrGetX509CertIssAltNameLen gets the length of the X.509 Certificate Issuer Alternate name value from an OKVTTLV object found at or after the element index elem_index.
- [okvAttrGetX509CertIssDNLen](#)
okvAttrGetX509CertIssDNLen gets the length of the X.509 Certificate Issuer distinguished name value from an OKVTTLV object.

12.1.79 okvAttrGetX509CertIssAltName

okvAttrGetX509CertIssAltName gets the X.509 Certificate Issuer alternate name attribute value from an OKVTTLV object found at or after the element index elem_index.

Catetory

KMIP attribute API

Purpose

okvAttrGetX509CertIssAltName gets the X.509 Certificate Issuer alternate name attribute value from an OKVTTLV object found at or after the element index elem_index.

Syntax

```

OKVErrNo okvAttrGetX509CertIssAltName(OKVEnv *env, OKVTTLV *ttl,
                                       ub4 *elem_index,
                                       oratext *alt_name, ub4 *alt_name);

```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to the OKVTTLV object.
elem_index	IN/OUT	Index of child OKVTTLV to start the lookup.

Parameter	IN/OUT	Description
alt_name	OUT	Certificate Issuer Alternate name.
alt_nameLen	IN/OUT	Certificate Issuer Alternate name length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

The memory to store the X.509 Certificate Issuer alternate name value should be allocated before the function call.

`okvAttrGetX509CertIssAltNameLen` can be used to get the X.509 Certificate Issuer alternate name value length.

Example

```
orertext *issuer_alt_name = (orertext *)NULL;
ub4 issuer_alt_name_len = okvAttrGetX509CertIssAltNameLen(env, ttlv, 0);
issuer_alt_name = calloc(issuer_alt_name_len + 1, sizeof(orertext));

okvAttrGetX509CertIssAltName(env, ttlv, 0, issuer_alt_name,
                             &issuer_alt_name_len);

/* Free 'issuer_alt_name' */
```

Related Topics

- [okvAttrAddX509CertIss](#)
`okvAttrAddX509CertIss` adds a X.509 Certificate Issuer distinguished name attribute to an OKVTTLV object.
- [okvAttrAddX509CertIssAltName](#)
`okvAttrAddX509CertIssAltName` adds a X.509 Certificate Issuer Alternate name attribute to an OKVTTLV object.
- [okvAttrGetX509CertIss](#)
`okvAttrGetX509CertIss` gets the X.509 Certificate Issuer distinguished name attribute value from an OKVTTLV object.
- [okvAttrGetX509CertIssAltNameLen](#)
`okvAttrGetX509CertIssAltNameLen` gets the length of the X.509 Certificate Issuer Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.

- [okvAttrGetX509CertIssDNLen](#)
okvAttrGetX509CertIssDNLen gets the length of the X.509 Certificate Issuer distinguished name value from an OKVTTLV object.

12.1.80 okvAttrGetX509CertIssAltNameLen

okvAttrGetX509CertIssAltNameLen gets the length of the X.509 Certificate Issuer Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.

Catetory

KMIP attribute API

Purpose

okvAttrGetX509CertIssAltNameLen gets the length of the X.509 Certificate Issuer Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.

Syntax

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttlV</code>	IN	Pointer to the OKVTTLV object.
<code>elem_index</code>	IN/OUT	Index of child OKVTTLV to start the lookup.

Return Values

Return Value	Description
<code>ub4</code>	Length of the attribute value. Success: Length of the X.509 certificate issuer alternate name value. Failure: 0.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
ub4 issuer_alt_name1 = 0;
issuer_alt_name1 = okvAttrGetX509CertIssAltNameLen(env, ttlv, 0);
```


Related Topics

- [okvAttrAddX509CertIss](#)
okvAttrAddX509CertIss adds a X.509 Certificate Issuer distinguished name attribute to an OKVTTLV object.
- [okvAttrAddX509CertIssAltName](#)
okvAttrAddX509CertIssAltName adds a X.509 Certificate Issuer Alternate name attribute to an OKVTTLV object.
- [okvAttrGetX509CertIss](#)
okvAttrGetX509CertIss gets the X.509 Certificate Issuer distinguished name attribute value from an OKVTTLV object.
- [okvAttrGetX509CertIssAltName](#)
okvAttrGetX509CertIssAltName gets the X.509 Certificate Issuer alternate name attribute value from an OKVTTLV object found at or after the element index elem_index.
- [okvAttrGetX509CertIssDNLen](#)
okvAttrGetX509CertIssDNLen gets the length of the X.509 Certificate Issuer distinguished name value from an OKVTTLV object.

12.1.81 okvAttrGetX509CertIssDNLen

okvAttrGetX509CertIssDNLen gets the length of the X.509 Certificate Issuer distinguished name value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

okvAttrGetX509CertIssDNLen gets the length of the X.509 Certificate Issuer distinguished name value from an OKVTTLV object.

Syntax

```
ub4 okvAttrGetX509CertIssDNLen(OKVEnv *env, OKVTTLV *ttl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttl	IN	Pointer to the OKVTTLV object.

Return Values

Return Value	Description
ub4	Length of the attribute value. Success: Length of the X.509 certificate issuer distinguished name value. Failure: 0.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
ub4 issuerl = 0;
issuerl = okvAttrGetX509CertIssDNLen(env, ttlv);
```

Related Topics

- [okvAttrAddX509CertIss](#)
`okvAttrAddX509CertIss` adds a X.509 Certificate Issuer distinguished name attribute to an OKVTTLV object.
- [okvAttrAddX509CertIssAltName](#)
`okvAttrAddX509CertIssAltName` adds a X.509 Certificate Issuer Alternate name attribute to an OKVTTLV object.
- [okvAttrGetX509CertIss](#)
`okvAttrGetX509CertIss` gets the X.509 Certificate Issuer distinguished name attribute value from an OKVTTLV object.
- [okvAttrGetX509CertIssAltName](#)
`okvAttrGetX509CertIssAltName` gets the X.509 Certificate Issuer alternate name attribute value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertIssAltNameLen](#)
`okvAttrGetX509CertIssAltNameLen` gets the length of the X.509 Certificate Issuer Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.

12.1.82 okvAttrGetX509CertSubj

`okvAttrGetX509CertSubj` gets the X.509 Certificate Subject distinguished name attribute value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrGetX509CertSubj` gets the X.509 Certificate Subject distinguished name attribute value from an OKVTTLV object.

Syntax

```
OKVErrNo okvAttrGetX509CertSubj(OKVEnv *env, OKVTTLV *ttl,
                                oratext *dn, ub4 *dnl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Pointer to the Oracle Key Vault environment handle.
ttlV	IN	Pointer to the OKVTTLV object.
dn	OUT	Certificate Subject distinguished name.
dnLen	IN/OUT	Certificate Subject distinguished name length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

The memory to store the X.509 Certificate Subject distinguished name value should be allocated before this API is called.

okvAttrGetX509CertSubjDNLen can be used to get the X.509 Certificate Subject distinguished name value length.

Example

```
oratext *subject = (oratext *)NULL;
ub4 subject_len = okvAttrGetX509CertSubjDNLen(env, ttlV);

subject = calloc(subject_len + 1, sizeof(oratext));

okvAttrGetX509CertSubj(env, ttlV, subject, &subject_len);

/* Free 'subject' */
```

Related Topics

- [okvAttrAddX509CertSubj](#)
okvAttrAddX509CertSubj adds a X.509 Certificate Subject distinguished name attribute to an OKVTTLV object.
- [okvAttrAddX509CertSubjAltName](#)
okvAttrAddX509CertSubjAltName adds a X.509 Certificate Subject Alternate name attribute to an OKVTTLV object.

- [okvAttrGetX509CertSubjAltName](#)
okvAttrGetX509CertSubjAltName gets the X.509 Certificate Subject alternate name attribute value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertSubjAltNameLen](#)
okvAttrGetX509CertSubjAltNameLen gets the length of the X.509 Certificate Subject Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertSubjDNLen](#)
okvAttrGetX509CertSubjDNLen gets the length of the X.509 Certificate Subject distinguished name value from an OKVTTLV object.

12.1.83 okvAttrGetX509CertSubjAltName

okvAttrGetX509CertSubjAltName gets the X.509 Certificate Subject alternate name attribute value from an OKVTTLV object found at or after the element index `elem_index`.

Catetory

KMIP attribute API

Purpose

okvAttrGetX509CertSubjAltName gets the X.509 Certificate Subject alternate name attribute value from an OKVTTLV object found at or after the element index `elem_index`.

Syntax

```
OKVErrNo okvAttrGetX509CertSubjAltName(OKVEnv *env, OKVTTLV *ttl,
                                       ub4 *elem_index,
                                       oratext *alt_name, ub4 *alt_name1);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to the OKVTTLV object.
<code>elem_index</code>	IN/OUT	Index of child OKVTTLV to start the lookup.
<code>alt_name</code>	OUT	Certificate Subject Alternate name.
<code>alt_name1</code>	IN/OUT	Certificate Subject Alternate name length.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

The memory to store the X.509 Certificate Subject alternate name value should be allocated before the function call.

`okvAttrGetX509CertSubjAltNameLen` can be used to get the X.509 Certificate Subject alternate name value length.

Example

```
oratext *subject_alt_name = (oratext *)NULL;
ub4 subject_alt_name_len = okvAttrGetX509CertSubjAltNameLen(env, ttlv, 0);

subject_alt_name = calloc(subject_alt_name_len + 1, sizeof(oratext));

okvAttrGetX509CertSubjAltName(env, ttlv, 0, subject_alt_name,
                              &subject_alt_name_len);

/* Free 'subject_alt_name' */
```

Related Topics

- [okvAttrAddX509CertSubj](#)
`okvAttrAddX509CertSubj` adds a X.509 Certificate Subject distinguished name attribute to an OKVTTLV object.
- [okvAttrAddX509CertSubjAltName](#)
`okvAttrAddX509CertSubjAltName` adds a X.509 Certificate Subject Alternate name attribute to an OKVTTLV object.
- [okvAttrGetX509CertSubj](#)
`okvAttrGetX509CertSubj` gets the X.509 Certificate Subject distinguished name attribute value from an OKVTTLV object.
- [okvAttrGetX509CertSubjAltNameLen](#)
`okvAttrGetX509CertSubjAltNameLen` gets the length of the X.509 Certificate Subject Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertSubjDNLen](#)
`okvAttrGetX509CertSubjDNLen` gets the length of the X.509 Certificate Subject distinguished name value from an OKVTTLV object.

12.1.84 okvAttrGetX509CertSubjAltNameLen

`okvAttrGetX509CertSubjAltNameLen` gets the length of the X.509 Certificate Subject Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.

Catetory

KMIP attribute API

Purpose

`okvAttrGetX509CertSubjAltNameLen` gets the length of the X.509 Certificate Subject Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.

Syntax

```
ub4 okvAttrGetX509CertSubjAltNameLen(OKVEnv *env, OKVTTLV *ttl,
                                     ub4 *elem_index);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to the OKVTTLV object.
<code>elem_index</code>	IN/OUT	Index of child OKVTTLV to start the lookup.

Return Values

Return Value	Description
<code>ub4</code>	Length of the attribute value. Success: Length of the X.509 certificate subject alternate name value. Failure: 0.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
ub4 subj_alt_name1 = 0;
subj_alt_name1 = okvAttrGetX509CertSubjAltNameLen(env, ttl, 0);
```

Related Topics

- [okvAttrAddX509CertSubj](#)
`okvAttrAddX509CertSubj` adds a X.509 Certificate Subject distinguished name attribute to an OKVTTLV object.
- [okvAttrAddX509CertSubjAltName](#)
`okvAttrAddX509CertSubjAltName` adds a X.509 Certificate Subject Alternate name attribute to an OKVTTLV object.
- [okvAttrGetX509CertSubj](#)
`okvAttrGetX509CertSubj` gets the X.509 Certificate Subject distinguished name attribute value from an OKVTTLV object.

- [okvAttrGetX509CertSubjAltName](#)
`okvAttrGetX509CertSubjAltName` gets the X.509 Certificate Subject alternate name attribute value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertSubjDNLen](#)
`okvAttrGetX509CertSubjDNLen` gets the length of the X.509 Certificate Subject distinguished name value from an OKVTTLV object.

12.1.85 okvAttrGetX509CertSubjDNLen

`okvAttrGetX509CertSubjDNLen` gets the length of the X.509 Certificate Subject distinguished name value from an OKVTTLV object.

Category

KMIP attribute API

Purpose

`okvAttrGetX509CertSubjDNLen` gets the length of the X.509 Certificate Subject distinguished name value from an OKVTTLV object.

Syntax

```
ub4 okvAttrGetX509CertSubjDNLen(OKVEnv *env, OKVTTLV *ttl);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to the OKVTTLV object.

Return Values

Return Value	Description
<code>ub4</code>	Length of the attribute value. Success: Length of the X.509 certificate subject distinguished name value. Failure: 0.

Supported Versions

Oracle Key Vault C SDK version 21.2.0.0.0 and later.

Comments

None.

Example

```
ub4 subj1 = 0;
subj1 = okvAttrGetX509CertSubjDNLen(env, ttl);
```

Related Topics

- [okvAttrAddX509CertSubj](#)
`okvAttrAddX509CertSubj` adds a X.509 Certificate Subject distinguished name attribute to an OKVTTLV object.
- [okvAttrAddX509CertSubjAltName](#)
`okvAttrAddX509CertSubjAltName` adds a X.509 Certificate Subject Alternate name attribute to an OKVTTLV object.
- [okvAttrGetX509CertSubj](#)
`okvAttrGetX509CertSubj` gets the X.509 Certificate Subject distinguished name attribute value from an OKVTTLV object.
- [okvAttrGetX509CertSubjAltName](#)
`okvAttrGetX509CertSubjAltName` gets the X.509 Certificate Subject alternate name attribute value from an OKVTTLV object found at or after the element index `elem_index`.
- [okvAttrGetX509CertSubjAltNameLen](#)
`okvAttrGetX509CertSubjAltNameLen` gets the length of the X.509 Certificate Subject Alternate name value from an OKVTTLV object found at or after the element index `elem_index`.

12.1.86 okvGetAttributeObject

`okvGetAttributeObject` gets the attribute, its name, and index from the parent attribute found at element index `elem_index`.

Category

KMIP attribute API

Purpose

`okvGetAttributeObject` gets the attribute, its name and index from the parent attribute found at element index `elem_index`. The actual attribute value can be retrieved using one of the other functions defined in this section.

Syntax

```
OKVErrNo okvGetAttributeObject(OKVEnv *env, OKVTTLV *ttl,
                               ub4 *elem_index,
                               OKVAttrNo *attrno, ub4 *attr_index, OKVTTLV **attr);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Pointer to the Oracle Key Vault environment handle.
<code>ttl</code>	IN	Pointer to OKVTTLV object.
<code>elem_index</code>	IN/OUT	The API will return the attribute number, attribute index and attribute value at the child at index pointed to by <code>elem_index</code> .
<code>attrno</code>	OUT	Oracle Key Vault attribute number.

Parameter	IN/OUT	Description
attr_index	OUT	Attribute index.
attr	OUT	TTLV object containing attribute value.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

This API is useful when it is required to parse the parent TTLV and find the various attribute and their corresponding values. The following example shows how we can use this API to parse a KMIP TTLV for name attribute.

Example

```
ub4 i = 0, ret_name_attrl, attrno, ret_index_name_attr;
OKVTTLV *name_attr_out;
oratext * ret_name_attr;

while(OKV_ATTR_NOT_FOUND !=
      okvGetAttributeObject(env, attr_out_list, &i,
                           &attrno, &ret_index_name_attr, &name_attr_out))
{
    if(attrno == OKVAttrName)
    {
        ret_name_attrl = okvAttrGetNameValueLen(env, name_attr_out, &i);
        ret_name_attr = calloc(ret_name_attrl, sizeof(oratext));
        okvAttrGetName(env, name_attr_out, &i,
                      ret_name_attr, ret_name_attrl, &typ);
        break;
    }
    else
    {
        i++;
    }
}
```

Related Topics

- [okvAddAttributeObject](#)
okvAddAttributeObject adds an attribute object to the parent TTLV object.

12.2 Oracle Key Vault Client SDK KMIP Custom Attribute APIs

The KMIP Custom Attribute APIs are listed in this section.

- [About the KMIP Custom Attributes API](#)
The Oracle Key Vault KMIP custom attributes follow a set of strict guidelines.
- [okvCustomAttrAddBigInteger](#)
`okvCustomAttrAddBigInteger` adds a big integer data to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrAddBoolean](#)
`okvCustomAttrAddBoolean` adds a Boolean data type to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrAddByteString](#)
`okvCustomAttrAddByteString` adds a byte string data type to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrAddDateTime](#)
`okvCustomAttrAddDateTime` adds a date time data type to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrAddEnum](#)
`okvCustomAttrAddEnum` adds an enumeration data type to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrAddInteger](#)
`okvCustomAttrAddInteger` adds an integer data type to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrAddInterval](#)
`okvCustomAttrAddInterval` adds an interval data type to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrAddLongInteger](#)
`okvCustomAttrAddLongInteger` adds a long integer data type to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrAddStructure](#)
`okvCustomAttrAddStructure` adds a TTLV structure to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrAddTextString](#)
`okvCustomAttrAddTextString` adds a text string data type to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrGet](#)
`okvCustomAttrGet` finds any custom attribute at or after element index `elem_ind`.
- [okvCustomAttrGetBigInteger](#)
`okvCustomAttrGetBigInteger` returns the big integer data found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.
- [okvCustomAttrGetBigIntegerLen](#)
`okvCustomAttrGetBigIntegerLen` returns the length of the big integer data found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrGetBoolean](#)
`okvCustomAttrGetBoolean` fetches a Boolean data type found at the element index `elem_ind`.

- **okvCustomAttrGetByName**
`okvCustomAttrGetByName` finds custom attribute with name `name` at or after the element index `elem_ind`.
- **okvCustomAttrGetByteString**
`okvCustomAttrGetByteString` returns the byte string data type found at the element index `elem_ind`.
- **okvCustomAttrGetByteStringLength**
`okvCustomAttrGetByteStringLength` returns the length of the byte string data type found at the element index `elem_ind`.
- **okvCustomAttrGetByType**
`okvCustomAttrGetByType` finds any custom attribute of type `typ` at or after the element index `elem_ind`, and returns the actual element index and length of the name of the custom attribute.
- **okvCustomAttrGetDateTime**
`okvCustomAttrGetDateTime` returns a date time data type found at the element index `elem_ind`.
- **okvCustomAttrGetEnum**
`okvCustomAttrGetEnum` returns an enumeration data type found at the element index `elem_ind`.
- **okvCustomAttrGetInteger**
Returns an integer data type found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.
- **okvCustomAttrGetInterval**
`okvCustomAttrGetInterval` returns an interval data type found at the element index `elem_ind`.
- **okvCustomAttrGetLongInteger**
`okvCustomAttrGetLongInteger` returns a long integer data type found at the element index `elem_ind`.
- **okvCustomAttrGetStructure**
`okvCustomAttrGetStructure` returns a TTLV structure data type found at element index `elem_ind`.
- **okvCustomAttrGetTextString**
`okvCustomAttrGetTextString` returns the text string data type found at the element index `elem_ind`.
- **okvCustomAttrGetTextStringLength**
`okvCustomAttrGetTextStringLength` returns the length of the text string data type found at the element index `elem_ind`.

12.2.1 About the KMIP Custom Attributes API

The Oracle Key Vault KMIP custom attributes follow a set of strict guidelines.

The custom attributes can have structures but the structures cannot have structures within them.

All client KMIP custom attribute names can begin with `x-` only. Any Oracle Key Vault custom attribute not starting with this prefix will be rejected.

 **Note:**

Do not use the prefix of `x-OKV` with custom attribute names. The custom attributes that start with the `x-OKV` prefix are reserved for use by Oracle Key Vault only.

Functions that return the `OKVTTLV` object have the following interpretation:

- On success, a valid `OKVTTLV` object for the attribute is returned.
- On failure, a `NULL` pointer is returned.

Functions that return the length of the retrieved object have the following interpretation:

- On success, a length of the buffer is returned.
- On failure, zero (0) is returned.

The following Oracle Key Vault functions add and retrieve custom attributes of a specific KMIP Data type from the `OKVTTLV` object. The functions have the following construction in general:

- `okvCustomAttrAddType` adds the custom attribute name and value to the `OKVTTLV` parent object.
- `okvCustomAttrGetTypeLen` gets the length of the custom attribute value from the `OKVTTLV` parent object for KMIP Data Types that don't have fixed length.
- `okvCustomAttrGetType` gets the custom attribute name and value from the `OKVTTLV` parent object.

The attribute index and element index used in the Oracle Key Vault functions have the same meaning as the standard Oracle Key Vault KMIP attribute APIs, but with the following exception:

Custom attributes have iterator functions because the endpoint may not know the type of the custom attribute with a given name. This makes it necessary to iterate over all types of custom attributes. But when a custom attribute with a given name is located, then the element index points that attribute for certain. Therefore, the get functions for the custom attributes do not have to look for the attribute at all and do not have to update the element index passed in.

Related Topics

- [About the Oracle Key Vault KMIP Attribute APIs](#)
This section describes the interfaces that help create and interpret Oracle Key Vault KMIP attributes.

12.2.2 `okvCustomAttrAddBigInteger`

`okvCustomAttrAddBigInteger` adds a big integer data to the custom attribute specified by the `OKVTTLV` parent object.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrAddBigInteger` adds a big integer data to the custom attribute specified by the OKVTTLV parent object.

Syntax

```
OKVTTLV *okvCustomAttrAddBigInteger(OKVEnv *env, OKVTTLV *ttl,
                                     oratext *name, ub4 namel,
                                     ub1 *big_integer,
                                     ub4 big_integerl,
                                     ub4 attr_index);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>ttl</code>	IN	TTLV parent object.
<code>name</code>	IN	Name of the custom attribute.
<code>namel</code>	IN	Length of the name of custom attribute.
<code>big_integer</code>	IN	Big Integer value to be added to the custom attribute.
<code>big_integerl</code>	IN	Big Integer value length.
<code>attr_index</code>	IN	Attribute index of the Big Integer custom attribute.

Return Values

Return Value	Description
<code>OKVTTLV *</code>	Pointer to OKVTTLV object. Success: Pointer to OKVTTLV object with big integer data type added. Failure: NULL.

Supported Versions:

Oracle Key Vault C SDK version 21.8.0.0.0 and later.

Comments

None.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *) NULL;
ub1 big_int[] = {-1, -1, 114, 48, 77, 100, 52, 60};
...
req = okvEnvGetOpRequestObj(env);
attr_in = okvCustomAttrAddBigInteger(env, req, "x-My Big Integer",
```

```

        strlen("x-My Big Integer"),
        big_int,
        strlen(big_int), 0);
    okvAddAttribute(env, uid, &attr_in);

```

Related Topics

- [okvCustomAttrGetBigIntegerLen](#)
`okvCustomAttrGetBigIntegerLen` returns the length of the big integer data found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrGetBigInteger](#)
`okvCustomAttrGetBigInteger` returns the big integer data found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

12.2.3 okvCustomAttrAddBoolean

`okvCustomAttrAddBoolean` adds a Boolean data type to the custom attribute specified by the OKVTTLV parent object.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrAddBoolean` adds a Boolean data type to the custom attribute specified by the OKVTTLV parent object.

Syntax

```

OKVTTLV * okvCustomAttrAddBoolean(OKVEnv *env, OKVTTLV *ttl,
                                   oratext *name, ub4 namel,
                                   ub8 bool_val, ub4 attr_index);

```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle
<code>ttl</code>	IN	TTLV parent object
<code>name</code>	IN	Name of custom attribute
<code>namel</code>	IN	Length of name of custom attribute
<code>bool_val</code>	IN	Boolean value to be added to the custom attribute
<code>attr_index</code>	IN	Attribute index of the Boolean custom attribute

Return Values

Return Value	Description
OKVTTLV *	<p>Pointer to the OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with Boolean data type added.</p> <p>Failure: NULL.</p>

Comments

None.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;
...
req = okvEnvGetOpRequestObj(env);
attr_in = okvCustomAttrAddBoolean(env, req, "x-My Boolean",
                                   strlen("x-My Boolean"),
                                   00000001, 0);
okvAddAttribute(env, uid, &attr_in);
```

Related Topics

- [okvCustomAttrGetBoolean](#)
okvCustomAttrGetBoolean fetches a Boolean data type found at the element index elem_ind.

12.2.4 okvCustomAttrAddByteString

okvCustomAttrAddByteString adds a byte string data type to the custom attribute specified by the OKVTTLV parent object.

Category

KMIP custom attributes API

Purpose

okvCustomAttrAddByteString adds a byte string data type to the custom attribute specified by the OKVTTLV parent object.

Syntax

```
OKVTTLV *okvCustomAttrAddByteString(OKVEnv *env, OKVTTLV *ttl,
                                     oratext *name, ub4 namel,
                                     ub1 *byte, ub4 bytel, ub4 attr_index);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle

Parameter	IN/OUT	Description
ttlV	IN	TTLV parent object
name	IN	Name of custom attribute
nameLen	IN	Length of name of custom attribute
byte	IN	Byte string
byteLen	IN	Length of byte string
attr_index	IN	Attribute index of the byte string custom attribute

Return Values

Return Value	Description
OKVTTLV *	<p>Pointer to the OKVTTLV object.</p> <p>Success: Pointer to OKVTTLV object with byte string added.</p> <p>Failure: NULL.</p>

Comments

None.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;
ub1 *byte = "ByteOne";
...
req = okvEnvGetOpRequestObj(env);
attr_in = okvCustomAttrAddByteString(env, req, "x-My Byte String",
                                     strlen("x-My Byte String"),
                                     byte, strlen(byte), 0);
okvAddAttribute(env, uid, &attr_in);
```

Related Topics

- [okvCustomAttrGetByteStringLength](#)
okvCustomAttrGetByteStringLength returns the length of the byte string data type found at the element index elem_ind.
- [okvCustomAttrGetByteString](#)
okvCustomAttrGetByteString returns the byte string data type found at the element index elem_ind.

12.2.5 okvCustomAttrAddDateTime

okvCustomAttrAddDateTime adds a date time data type to the custom attribute specified by the OKVTTLV parent object.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrAddDateTime` adds a date time data type to the custom attribute specified by the OKVTTLV parent object.

Syntax

```
OKVTTLV * okvCustomAttrAddDateTime(OKVEnv *env, OKVTTLV *ttl,
                                     oratext *name, ub4 namel,
                                     ub8 date_time, ub4 attr_index);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle
<code>ttl</code>	IN	TTLV parent object
<code>name</code>	IN	Name of custom attribute
<code>namel</code>	IN	Length of name of custom attribute
<code>date_time</code>	IN	Date time value to be added to the custom attribute
<code>attr_index</code>	IN	Attribute index of the date time custom attribute

Return Values

Return Value	Description
<code>OKVTTLV *</code>	Pointer to the OKVTTLV object. Success: Pointer to OKVTTLV object with date time custom attribute added. Failure: NULL.

Comments

None.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;
time_t current_time = time((time_t *)NULL);
...
req = okvEnvGetOpRequestObj(env);
attr_in = okvCustomAttrAddDateTime(env, req, "x-My Date Time",
                                   strlen("x-My Date Time"),
                                   (ub8) current_time, 0);
okvAddAttribute(env, uid, &attr_in);
```

Related Topics

- [okvCustomAttrGetDateTime](#)
`okvCustomAttrGetDateTime` returns a date time data type found at the element index `elem_ind`.

12.2.6 okvCustomAttrAddEnum

`okvCustomAttrAddEnum` adds an enumeration data type to the custom attribute specified by the OKVTTLV parent object.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrAddEnum` adds an enumeration data type to the custom attribute specified by the OKVTTLV parent object.

Syntax

```
OKVTTLV * okvCustomAttrAddEnum(OKVEnv *env, OKVTTLV *ttl,
                                oratext *name, ub4 namel,
                                ub4 enumval, ub4 attr_index);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle
<code>ttl</code>	IN	TTLV parent object
<code>name</code>	IN	Name of custom attribute
<code>namel</code>	IN	Length of name of custom attribute
<code>enumval</code>	IN	Enum value to be added to the custom attribute
<code>attr_index</code>	IN	Attribute index of enumeration custom attribute

Return Values

Return Value	Description
<code>OKVTTLV *</code>	Pointer to the OKVTTLV object. Success: Pointer to OKVTTLV object with enumeration values added. Failure: NULL.

Comments

None.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;
...
req = okvEnvGetOpRequestObj(env);
attr_in = okvCustomAttrAddEnum(env, req, "x-My Enumeration",
```

```

        strlen("x-My Enumeration"),
        CRYPTO_ALG_DES, 0);
okvAddAttribute(env, uid, &attr_in);

```

Related Topics

- [okvCustomAttrGetEnum](#)
okvCustomAttrGetEnum returns an enumeration data type found at the element index elem_ind.

12.2.7 okvCustomAttrAddInteger

okvCustomAttrAddInteger adds an integer data type to the custom attribute specified by the OKVTTLV parent object.

Category

KMIP custom attributes API

Purpose

okvCustomAttrAddInteger adds an integer data type to the custom attribute specified by the OKVTTLV parent object.

Syntax

```

OKVTTLV * okvCustomAttrAddInteger(OKVEnv *env, OKVTTLV *ttl,
    oratext *name, ub4 namel,
    ub4 integer, ub4 attr_index);

```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle
ttl	IN	TTLV parent object
name	IN	Name of custom attribute
namel	IN	Length of name of custom attribute
integer	IN	Integer value to be added to the custom attribute
attr_ind	IN	Attribute index of the integer custom attribute

Return Values

Return Value	Description
OKVTTLV *	Pointer to the OKVTTLV object. Success: Pointer to OKVTTLV object with integer data type added. Failure: NULL.

Comments

None.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;
...
req = okvEnvGetOpRequestObj(env);
attr_in = okvCustomAttrAddInteger(env, req, "x-My Integer",
                                strlen("x-My Integer"), 32, 0);
okvAddAttribute(env, uid, &attr_in);
```

Related Topics

- [okvCustomAttrGetInteger](#)
Returns an integer data type found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

12.2.8 okvCustomAttrAddInterval

`okvCustomAttrAddInterval` adds an interval data type to the custom attribute specified by the OKVTTLV parent object.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrAddInterval` adds an interval data type to the custom attribute specified by the OKVTTLV parent object.

Syntax

```
OKVTTLV * okvCustomAttrAddInterval(OKVEnv *env, OKVTTLV *ttl,
                                   oratext *name, ub4 namel,
                                   ub4 interval, ub4 attr_index);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle
<code>ttl</code>	IN	TTLV parent object
<code>name</code>	IN	Name of custom attribute
<code>namel</code>	IN	Length of name of custom attribute
<code>interval</code>	IN	Interval value to be added to the custom attribute
<code>attr_ind</code>	IN	Attribute index of the Interval custom attribute

Return Values

Return Value	Description
OKVTTLV *	Pointer to the OKVTTLV object. Success: Pointer to OKVTTLV object with interval data type added. Failure: NULL.

Comments

None.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;
...
req = okvEnvGetOpRequestObj(env);
attr_in = okvCustomAttrAddInterval(env, req, "x-My Interval",
                                   strlen("x-My Interval"),
                                   5, 0);

okvAddAttribute(env, uid, &attr_in);
```

Related Topics

- [okvCustomAttrGetInterval](#)
okvCustomAttrGetInterval returns an interval data type found at the element index elem_ind.

12.2.9 okvCustomAttrAddLongInteger

okvCustomAttrAddLongInteger adds a long integer data type to the custom attribute specified by the OKVTTLV parent object.

Category

KMIP custom attributes API

Purpose

okvCustomAttrAddLongInteger adds a long integer data type to the custom attribute specified by the OKVTTLV parent object.

Syntax

```
OKVTTLV * okvCustomAttrAddLongInteger(OKVEnv *env, OKVTTLV *ttl,
                                       oratext *name, ub4 name1,
                                       ub8 long_integer, ub4 attr_index);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Parameter	IN/OUT	Description
ttlv	IN	TTLV parent object.
name	IN	Name of custom attribute.
namel	IN	Length of name of custom attribute.
long_integer	IN	Long integer value to be added to the custom attribute.
attr_index	IN	Attribute index of long integer custom attribute.

Return Values

Return Value	Description
OKVTTLV *	Pointer to the OKVTTLV object. Success: Pointer to OKVTTLV object with long integer data type added. Failure: NULL.

Comments

None.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;
...
req = okvEnvGetOpRequestObj(env);
attr_in = okvCustomAttrAddLongInteger(env, req, "x-My Long Integer",
                                     strlen("x-My Long Integer"),
                                     (ub8) 32, 0);
okvAddAttribute(env, uid, &attr_in);
```

Related Topics

- [okvCustomAttrGetLongInteger](#)
`okvCustomAttrGetLongInteger` returns a long integer data type found at the element index `elem_ind`.

12.2.10 okvCustomAttrAddStructure

`okvCustomAttrAddStructure` adds a TTLV structure to the custom attribute specified by the OKVTTLV parent object.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrAddStructure` adds a TTLV structure to the custom attribute specified by the OKVTTLV parent object.

Syntax

```
OKVTTLV * okvCustomAttrAddStructure(OKVEnv *env, OKVTTLV *ttl,
                                   oratext *name, ub4 namel,
                                   OKVTTLV *structure, ub4 attr_index);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttl	IN	TTLV parent object.
name	IN	Name of custom attribute.
namel	IN	Length of name of custom attribute.
structure	IN	TTLV structure to be added to the custom attribute.
attr_index	IN	Attribute index of the structure custom attribute.

Return Values

Return Value	Description
OKVTTLV *	Pointer to the OKVTTLV object. Success: Pointer to OKVTTLV object with TTLV structure added. Failure: NULL.

Comments

None.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *) NULL;
...
/* Construct the structure to be added */
OKVTTLV *req2 = okvEnvGetOpRequestObj(env);
okvAttrAddUniqueID(env, req2, "Unique_ID354", sizeof("Unique_ID354"));

/* Add the structure */
req = okvEnvGetOpRequestObj(env);
attr_in = okvCustomAttrAddStructure(env, req, "x-My Structure",
                                   strlen("x-My Structure"),
                                   req2, 0);
okvAddAttribute(env, uid, &attr_in);
```

Related Topics

- [okvCustomAttrGetStructure](#)
okvCustomAttrGetStructure returns a TTLV structure data type found at element index elem_ind.

12.2.11 okvCustomAttrAddTextString

`okvCustomAttrAddTextString` adds a text string data type to the custom attribute specified by the OKVTTLV parent object.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrAddTextString` adds a text string data type to the custom attribute specified by the OKVTTLV parent object.

Syntax

```
OKVTTLV *okvCustomAttrAddTextString(OKVEnv *env, OKVTTLV *ttl,
                                     oratext *name, ub4 name1,
                                     oratext *text, ub4 text1, ub4 attr_index);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>ttl</code>	IN	TTLV parent object.
<code>name</code>	IN	Name of custom attribute.
<code>name1</code>	IN	Length of name of custom attribute.
<code>text</code>	IN	Text string.
<code>text1</code>	IN	Length of text string.
<code>attr_index</code>	IN	Attribute index of the text string custom attribute.

Return Values

Return Value	Description
<code>OKVTTLV *</code>	Pointer to the OKVTTLV object. Success: Pointer to OKVTTLV object with text string data type added. Failure: NULL.

Comments

None.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *) NULL;
oratext *text = "Text Message";
...
```



```

req = okvEnvGetOpRequestObj(env);
attr_in = okvCustomAttrAddTextString(env, req, "x-My Text String", strlen("x-My
Text String"),
                                text, strlen(text), 0);
okvAddAttribute(env, uid, &attr_in);

```

Related Topics

- [okvCustomAttrGetTextString](#)
okvCustomAttrGetTextString returns the text string data type found at the element index elem_ind.
- [okvCustomAttrGetTextStringLen](#)
okvCustomAttrGetTextStringLen returns the length of the text string data type found at the element index elem_ind.

12.2.12 okvCustomAttrGet

okvCustomAttrGet finds any custom attribute at or after element index elem_ind.

Category

KMIP custom attributes API

Purpose

okvCustomAttrGet finds any custom attribute at or after element index elem_ind. The actual element index and length of the name of the custom attribute are also returned.

Syntax

```

OKVErrNo okvCustomAttrGet(OKVEnv *env, OKVTTLV *ttl,
                          ub4 *elem_ind, OKVType *typ, ub4 *name_len);

```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttl	IN	TTLV parent object.
elem_ind	IN/OUT	Element index.
typ	IN	Type of the custom attribute.
name_len	OUT	Length of the name of the custom attribute.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```

OKVTTLV *ttl = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Custom Attribute";
ub4 elem_ind = 0;
ub1 typ = 0;
ub4 name_len = 0;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &ttl);

/* We need the type of the custom attribute */
okvCustomAttrGetByName(env, ttl, &elem_ind, attr_name_list[0],
                      strlen((char *) attr_name_list[0]), &typ);
okvCustomAttrGet(env, ttl, &elem_ind, &typ, &name_len);
printf ("%d %d", elem_ind, name_len);

```

Related Topics

- [okvCustomAttrGetByName](#)
okvCustomAttrGetByName finds custom attribute with name `name` at or after the element index `elem_ind`.
- [okvCustomAttrGetByType](#)
okvCustomAttrGetByType finds any custom attribute of type `typ` at or after the element index `elem_ind`, and returns the actual element index and length of the name of the custom attribute.

12.2.13 okvCustomAttrGetBigInteger

okvCustomAttrGetBigInteger returns the big integer data found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Category

KMIP custom attributes API

Purpose

okvCustomAttrGetBigInteger returns the big integer data found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Syntax

```

OKVErrNo okvCustomAttrGetBigInteger(OKVEnv *env, OKVTTLV *ttl,
                                   ub4 elem_ind,
                                   oratext *name, ub4 *name1,
                                   ub1 *big_integer,
                                   ub4 *big_integer1,
                                   ub4 *attr_index);

```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttlv	IN	TTLV parent object.
elem_ind	IN	Element Index
name	OUT	Name of the custom attribute.
namel	IN/OUT	Length of the name of custom attribute.
big_integer	OUT	Big Integer value.
big_integerl	IN/OUT	Big Integer value length.
attr_index	OUT	Attribute index of the Big Integer custom attribute.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions:

Oracle Key Vault C SDK version 21.8.0.0.0 and later.

Comments

- Memory for the buffer for the Big Integer Data Type should be pre-allocated and the size of memory passed in as `big_integerl`.
- Either memory for the buffer for the name of the custom attribute should be pre-allocated and the size of memory passed in as `namel`, or both `name` and `namel` should be null. Just one of them cannot be null.

Example

```
OKVTTLV *ttlV = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Big Integer";
ub4 attr_index = 0;
ub4 elem_ind = 0;
ub4 big_intl;
ub4 namel = 100;
ub4 i = 0;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list,
                 &ttlV);
big_intl = okvCustomAttrGetBigIntegerLen(env, ttlV, elem_ind);
ub1 *big_int = (ub1 *) malloc(big_intl * (sizeof(ub1)));
memset((void *) big_int, 0, big_intl);
oratext *name = (oratext *) malloc(namel * (sizeof(oratext)));
```

```
memset((void *) name, 0, namel);
okvCustomAttrGetBigInteger(env, ttlv, elem_ind, name, &namel,
                           big_int, &big_intl, &attr_index);
for (i = 0; i < big_intl; i++)
{
    printf ("%02x", *(big_int + i));
}
...
free(name);
free(big_int);
```

Related Topics

- [okvCustomAttrGetBigIntegerLen](#)
okvCustomAttrGetBigIntegerLen returns the length of the big integer data found at element index elem_ind in the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrAddBigInteger](#)
okvCustomAttrAddBigInteger adds a big integer data to the custom attribute specified by the OKVTTLV parent object.

12.2.14 okvCustomAttrGetBigIntegerLen

okvCustomAttrGetBigIntegerLen returns the length of the big integer data found at element index elem_ind in the custom attribute specified by the OKVTTLV parent object.

Category

KMIP custom attributes API

Purpose

okvCustomAttrGetBigIntegerLen returns the length of the big integer data found at element index elem_ind in the custom attribute specified by the OKVTTLV parent object.

Syntax

```
ub4 okvCustomAttrGetBigIntegerLen(OKVEnv *env, OKVTTLV *ttl,
                                  ub4 elem_ind);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttl	IN	TTLV parent object.
elem_ind	IN	Element index.

Return Values

Return Value	Description
ub4	Length of the attribute value. Success: Length of the big integer data type attribute value. Failure: 0.

Supported Versions:

Oracle Key Vault C SDK version 21.8.0.0.0 and later.

Comments

None.

Example

```
OKVTTLV *attrs = (OKVTTLV *)NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Big Integer";
ub4 len = 0, elem_ind = 0;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &attrs);
len = okvCustomAttrGetBigIntegerLen(env, attrs, elem_ind);
```

Related Topics

- [okvCustomAttrAddBigInteger](#)
okvCustomAttrAddBigInteger adds a big integer data to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrGetBigInteger](#)
okvCustomAttrGetBigInteger returns the big integer data found at element index elem_ind in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

12.2.15 okvCustomAttrGetBoolean

okvCustomAttrGetBoolean fetches a Boolean data type found at the element index elem_ind.

Category

KMIP custom attributes API

Purpose

okvCustomAttrGetBoolean fetches a Boolean data type found at element index elem_ind in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Syntax

```
OKVErrNo okvCustomAttrGetBoolean(OKVEnv *env, OKVTTLV *ttl,
                                ub4 elem_ind, oratext *name, ub4 *name1,
                                ub8 *bool_val, ub4 *attr_index);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttl	IN	TTLV parent object.

Parameter	IN/OUT	Description
elem_ind	IN	Element index.
name	OUT	Name of custom attribute.
namel	IN/OUT	Length of name of custom attribute.
bool_val	OUT	Boolean value in the custom attribute at elem_ind.
attr_index	OUT	Attribute index of the Boolean custom attribute.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

Either memory for the buffer for the name of the custom attribute should be pre-allocated and the size of memory passed in as `namel`, or both `name` and `namel` should be `NULL`. Just one of them cannot be `NULL`.

Example

```
OKVTTLV *ttlV = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Boolean";
ub4 attr_index = 0;
ub4 elem_ind = 0;
ub8 bool_val = 0;
ub4 namel = 20;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &ttlV);
oratext *name = (oratext *) malloc(namel * (sizeof(oratext)));
memset((void *) name, 0, namel);
okvCustomAttrGetBoolean(env, ttlV, elem_ind, name,
                        &namel, &bool_val, &attr_index);
printf ("%d", bool_val);
...
free(name);
```

Related Topics

- [okvCustomAttrAddBoolean](#)
`okvCustomAttrAddBoolean` adds a Boolean data type to the custom attribute specified by the OKVTTLV parent object.

12.2.16 okvCustomAttrGetByName

`okvCustomAttrGetByName` finds custom attribute with name `name` at or after the element index `elem_ind`.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrGetByName` finds custom attribute with name `name` at or after element index `elem_ind`. The actual element index and type of the custom attribute are also returned.

Syntax

```
OKVErrNo okvCustomAttrGetByName(OKVEnv *env, OKVTTLV *ttl,
                                ub4 *elem_ind, oratext *name, ub4 name_len,
                                OKVType *typ);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle
<code>ttl</code>	IN	TTLV parent object
<code>elem_ind</code>	IN/OUT	Element index
<code>name</code>	IN	Name of custom attribute
<code>name_len</code>	IN	Length of name of custom attribute
<code>typ</code>	OUT	Type of the custom attribute

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
OKVTTLV *ttl = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Custom Attribute";
ub4 elem_ind = 0;
ub1 typ = 0;
...
```

```

okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &ttmlv);
okvCustomAttrGetByName(env, ttlv, &elem_ind, attr_name_list[0], strlen((char *)
attr_name_list[0]), &typ);
printf ("%d %d", elem_ind, typ);

```

Related Topics

- [okvCustomAttrGet](#)
okvCustomAttrGet finds any custom attribute at or after element index elem_ind.
- [okvCustomAttrGetByType](#)
okvCustomAttrGetByType finds any custom attribute of type typ at or after the element index elem_ind, and returns the actual element index and length of the name of the custom attribute.

12.2.17 okvCustomAttrGetByteString

okvCustomAttrGetByteString returns the byte string data type found at the element index elem_ind.

Category

KMIP custom attributes API

Purpose

okvCustomAttrGetByteString returns the byte string data type found at element index elem_ind in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Syntax

```

OKVErrNo okvCustomAttrGetByteString(OKVEnv *env, OKVTTLV *ttl,
                                     ub4 elem_ind, oratext *name, ub4 *namel,
                                     ub1 *byte, ub4 *bytlen, ub4 *attr_index);

```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttl	IN	TTLV parent object.
elem_ind	IN	Element index.
name	OUT	Name of custom attribute.
namel	IN/OUT	Length of name of custom attribute.
byte	OUT	Byte string.
bytlen	IN/OUT	Length of byte string.
attr_index	OUT	Attribute index of the byte string custom attribute.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

Memory for the buffer for the byte string data type should be pre-allocated and the size of memory passed in as `bytel`.

Either memory for the buffer for the name of the custom attribute should be pre-allocated and the size of memory passed in as `name1`, or both `name` and `name1` should be NULL. Just one of them cannot be NULL.

Example

```
OKVTTLV *ttlV = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Byte String";
ub4 attr_index = 0;
ub4 elem_ind = 0;
ub4 bytel = 16;
ub4 name1 = 20;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &ttlV);
ub1 *byte = (ub1 *) malloc(bytel * (sizeof(ub1)));
memset((void *) byte, 0, bytel);
oratext *name = (oratext *) malloc(name1 * (sizeof(oratext)));
memset((void *) name, 0, name1);
okvCustomAttrGetByteString(env, ttlV, elem_ind, name,
                           &name1, byte,
                           &bytel, &attr_index);

printf ("%s", byte);
...
free(name);
free(byte);
```

Related Topics

- [okvCustomAttrAddByteString](#)
`okvCustomAttrAddByteString` adds a byte string data type to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrGetByteStringLen](#)
`okvCustomAttrGetByteStringLen` returns the length of the byte string data type found at the element index `elem_ind`.

12.2.18 okvCustomAttrGetByteStringLen

`okvCustomAttrGetByteStringLen` returns the length of the byte string data type found at the element index `elem_ind`.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrGetByteStringLen` returns the length of the byte string data type found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object.

Syntax

```
ub4 okvCustomAttrGetByteStringLen(OKVEnv *env, OKVTTLV *ttl,
                                  ub4 elem_ind);
```

Parameters

Parameters	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>ttl</code>	IN	TTLV parent object.
<code>elem_ind</code>	IN	Element index.

Return Values

Return Value	Description
<code>ub4</code>	Length of the attribute value. Success: Length of the byte string data type. Failure: 0.

Comments

None.

Example

```
OKVTTLV *attrs = (OKVTTLV *)NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Byte String";
ub4 len = 0, elem_ind = 0;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &attrs);
len = okvCustomAttrGetByteStringLen(env, attrs, elem_ind);
```

Related Topics

- [okvCustomAttrAddByteString](#)
`okvCustomAttrAddByteString` adds a byte string data type to the custom attribute specified by the OKVTTLV parent object.

- [okvCustomAttrGetByteString](#)
`okvCustomAttrGetByteString` returns the byte string data type found at the element index `elem_ind`.

12.2.19 okvCustomAttrGetType

`okvCustomAttrGetType` finds any custom attribute of type `typ` at or after the element index `elem_ind`, and returns the actual element index and length of the name of the custom attribute.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrGetType` finds any custom attribute of type `typ` at or after element index `elem_ind`. The actual element index and length of the name of the custom attribute are also returned.

Syntax

```
OKVErrNo okvCustomAttrGetType(OKVEnv *env, OKVTTLV *ttl,
                              ub4 *elem_ind, OKVType typ, ub4 *name_len);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle
<code>ttl</code>	IN	TTLV parent object
<code>elem_ind</code>	IN/OUT	Element index
<code>typ</code>	IN	Type of the custom attribute
<code>name_len</code>	OUT	Length of the name of the custom attribute

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```
OKVTTLV *ttl = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Custom Attribute";
```

```

ub4 elem_ind = 0;
ub1 typ = 0;
ub4 name_len = 0;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &ttlv);

/* We need the type of the custom attribute */
okvCustomAttrGetByName(env, ttlv, &elem_ind, attr_name_list[0],
                      strlen((char *) attr_name_list[0]), &typ);
okvCustomAttrGetType(env, ttlv, &elem_ind, typ, &name_len);
printf ("%d %d", elem_ind, name_len);

```

Related Topics

- [okvCustomAttrGet](#)
okvCustomAttrGet finds any custom attribute at or after element index elem_ind.
- [okvCustomAttrGetByName](#)
okvCustomAttrGetByName finds custom attribute with name name at or after the element index elem_ind.

12.2.20 okvCustomAttrGetDateTime

okvCustomAttrGetDateTime returns a date time data type found at the element index elem_ind.

Category

KMIP custom attributes API

Purpose

okvCustomAttrGetDateTime returns a date time data type found at element index elem_ind in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Syntax

```

OKVErrNo okvCustomAttrGetDateTime(OKVEnv *env, OKVTTLV *ttl,
                                   ub4 elem_ind, oratext *name, ub4 *name1,
                                   ub8 *date_time, ub4 *attr_index);

```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttl	IN	TTLV parent object.
elem_ind	IN	Element index.
name	OUT	Name of custom attribute.
name1	IN/OUT	Length of name of custom attribute.
date_time	OUT	Date-time value in the custom attribute at element index elem_ind.
attr_index	OUT	Attribute index of the date-time custom attribute.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

Either memory for the buffer for the name of the custom attribute should be pre-allocated and the size of memory passed in as `name1`, or both `name` and `name1` should be NULL. Just one of them cannot be NULL.

Example

```
OKVTTLV *ttlV = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Date Time";
ub4 attr_index = 0;
ub4 elem_ind = 0;
ub8 date_time = 0;
ub4 name1 = 20;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &ttlV);
oratext *name = (oratext *) malloc(name1 * (sizeof(oratext)));
memset((void *) name, 0, name1);
okvCustomAttrGetDateTime(env, ttlV, elem_ind, name,
                        &name1, &date_time, &attr_index);
printf ("%d", date_time);
...
free(name);
```

Related Topics

- [okvCustomAttrAddDateTime](#)
`okvCustomAttrAddDateTime` adds a date time data type to the custom attribute specified by the OKVTTLV parent object.

12.2.21 okvCustomAttrGetEnum

`okvCustomAttrGetEnum` returns an enumeration data type found at the element index `elem_ind`.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrGetEnum` returns an enumeration data type found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Syntax

```
OKVErrNo okvCustomAttrGetEnum(OKVEnv *env, OKVTTLV *ttl,
                              ub4 elem_ind, oratext *name, ub4 *namel,
                              ub4 *enumval, ub4 *attr_index);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttl	IN	TTLV parent object.
elem_ind	IN	Element index.
name	OUT	Name of custom attribute.
namel	IN/OUT	Length of name of custom attribute.
enumval	OUT	enum value in the custom attribute at element index elem_ind.
attr_index	OUT	Attribute index of enumeration custom attribute.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

Either memory for the buffer for the name of the custom attribute should be pre-allocated and the size of memory passed in as `namel`, or both `name` and `namel` should be `NULL`. Just one of them cannot be `NULL`.

Example

```
OKVTTLV *ttl = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Enumeration";
ub4 attr_index = 0;
ub4 elem_ind = 0;
ub4 enumval = 0;
ub4 namel = 20;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &ttl);
oratext *name = (oratext *) malloc(namel * (sizeof(oratext)));
memset((void *) name, 0, namel);
okvCustomAttrGetEnum(env, ttl, elem_ind, name,
                    &namel, &enumval, &attr_index);
printf ("%d", enumval);
```

```
...
free(name);
```

Related Topics

- [okvCustomAttrAddEnum](#)
okvCustomAttrAddEnum adds an enumeration data type to the custom attribute specified by the OKVTTLV parent object.

12.2.22 okvCustomAttrGetInteger

Returns an integer data type found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Category

KMIP Custom Attributes API

Purpose

Returns an integer data type found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Syntax

```
OKVErrNo okvCustomAttrGetInteger(OKVEnv *env, OKVTTLV *ttl,
                                ub4 elem_ind, oratext *name, ub4 *name1,
                                ub4 *integer, ub4 *attr_index);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>ttl</code>	IN	TTLV parent object.
<code>elem_ind</code>	IN	Element index.
<code>name</code>	OUT	Name of the custom attribute.
<code>name1</code>	IN/OUT	Length of the name of the custom attribute.
<code>integer</code>	OUT	Integer value in the custom attribute at <code>elem_ind</code> .
<code>attr_index</code>	OUT	Attribute index of the integer custom attribute.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

Either memory for the buffer for the name of the custom attribute should be pre-allocated and the size of memory passed in as `name1`, or both `name` and `name1` should be `NULL`.

Example

```
OKVTTLV *ttl = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Integer";
ub4 attr_index = 0;
ub4 elem_ind = 0;
ub4 integer = 0;
ub4 name1 = 20;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &ttl);
oratext *name = (oratext *) malloc(name1 * (sizeof(oratext)));
memset((void *) name, 0, name1);
okvCustomAttrGetInteger(env, ttl, elem_ind, name,
                        &name1, &integer, &attr_index);
printf ("%d", integer);
...
free(name);
```

Related Topics

- [okvCustomAttrAddInteger](#)
`okvCustomAttrAddInteger` adds an integer data type to the custom attribute specified by the OKVTTLV parent object.

12.2.23 okvCustomAttrGetInterval

`okvCustomAttrGetInterval` returns an interval data type found at the element index `elem_ind`.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrGetInterval` returns an interval data type found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Syntax

```
OKVErrNo okvCustomAttrGetInterval(OKVEnv *env, OKVTTLV *ttl,
                                  ub4 elem_ind, oratext *name, ub4 *name1,
                                  ...
                                  ub4 *interval, ub4 *attr_index);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>ttl</code>	IN	TTLV parent object.

Parameter	IN/OUT	Description
elem_ind	IN	Element index.
name	OUT	Name of custom attribute.
namel	IN/OUT	Length of name of custom attribute.
interval	OUT	Interval value in the custom attribute at element index elem_ind.
attr_index	OUT	Attribute index of the Interval custom attribute.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

Either memory for the buffer for the name of the custom attribute should be pre-allocated and the size of memory passed in as `namel`, or both `name` and `namel` should be NULL. Just one of them cannot be NULL.

Example

```
OKVTTLV *ttlv = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Interval";
ub4 attr_index = 0;
ub4 elem_ind = 0;
ub4 interval = 0;
ub4 namel = 20;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &ttlv);
oratext *name = (oratext *) malloc(namel * (sizeof(oratext)));
memset((void *) name, 0, namel);
okvCustomAttrGetInterval(env, ttlv, elem_ind, name,
                        &namel, &interval, &attr_index);
printf ("%d", interval);
...
free(name);
```

Related Topics

- [okvCustomAttrAddInterval](#)
okvCustomAttrAddInterval adds an interval data type to the custom attribute specified by the OKVTTLV parent object.

12.2.24 okvCustomAttrGetLongInteger

`okvCustomAttrGetLongInteger` returns a long integer data type found at the element index `elem_ind`.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrGetLongInteger` returns a long integer data type found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Syntax

```
OKVErrNo okvCustomAttrGetLongInteger(OKVEnv *env, OKVTTLV *ttl,
                                     ub4 elem_ind, oratext *name, ub4 *name1,
                                     ub8 *long_integer, ub4 *attr_index);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>ttl</code>	IN	TTLV parent object.
<code>elem_ind</code>	IN	Element index.
<code>name</code>	OUT	Name of custom attribute.
<code>name1</code>	IN/OUT	Length of name of custom attribute.
<code>long_integer</code>	OUT	Long integer value in the custom attribute at element index <code>elem_ind</code> .
<code>attr_index</code>	OUT	Attribute index of the long integer custom attribute.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

Either memory for the buffer for the name of the custom attribute should be pre-allocated and the size of memory passed in as `name1`, or both `name` and `name1` should be `NULL`. Just one of them cannot be `NULL`.

Example

```
OKVTTLV *ttl = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Long Integer";
ub4 attr_index = 0;
ub4 elem_ind = 0;
ub8 long_integer = 0;
ub4 namel = 20;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &ttl);
oratext *name = (oratext *) malloc(namel * (sizeof(oratext)));
memset((void *) name, 0, namel);
okvCustomAttrGetLongInteger(env, ttl, elem_ind, name,
                           &namel, &long_integer, &attr_index);
printf ("%ld", long_integer);
...
free(name);
```

Related Topics

- [okvCustomAttrAddLongInteger](#)
okvCustomAttrAddLongInteger adds a long integer data type to the custom attribute specified by the OKVTTLV parent object.

12.2.25 okvCustomAttrGetStructure

okvCustomAttrGetStructure returns a TTLV structure data type found at element index elem_ind.

Category

KMIP custom attributes API

Purpose

okvCustomAttrGetStructure returns a TTLV structure data type found at element index elem_ind in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Syntax

```
OKVErrNo okvCustomAttrGetStructure(OKVEnv *env, OKVTTLV *ttl,
                                   ub4 elem_ind, oratext *name,
                                   ub4 *namel, OKVTTLV **structure,
                                   ub4 *attr_index);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle
ttl	IN	TTLV parent object
elem_ind	IN	Element index
name	OUT	Name of custom attribute

Parameter	IN/OUT	Description
name1	IN/OUT	Length of name of custom attribute
structure	OUT	TTLV structure of the custom attribute
attr_index	OUT	Attribute index of the structure custom attribute

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

Either memory for the buffer for the name of the custom attribute should be pre-allocated and the size of memory passed in as `name1`, or both `name` and `name1` should be `NULL`. Just one of them cannot be `NULL`.

Example

```
OKVTTLV *ttl = (OKVTTLV *) NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Structure";
ub4 attr_index = 0;
ub4 elem_ind = 0;
OKVTTLV *structure = (OKVTTLV *) NULL;
ub4 name1 = 20;
...

/* Retrieve the structure */
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &ttl);
oratext *name = (oratext *) malloc(name1 * (sizeof(oratext)));
memset((void *) name, 0, name1);
okvCustomAttrGetStructure(env, ttl, elem_ind, name,
                          &name1, &structure, &attr_index);

/* Parse the retrieved structure */
ub4 len = 0;
OKVTTLV *cttl = okvTTLVGetChild(env, structure, 0, (OKVTag *) 0,
                                (OKVType *) 0, &len);
oratext *cttl_val = (oratext *) okvTTLVGetValue(cttl);
printf ("%s", cttl_val);
...
free(name);
```

Related Topics

- [okvCustomAttrAddStructure](#)
`okvCustomAttrAddStructure` adds a TTLV structure to the custom attribute specified by the OKVTTLV parent object.

12.2.26 okvCustomAttrGetTextString

`okvCustomAttrGetTextString` returns the text string data type found at the element index `elem_ind`.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrGetTextString` returns the text string data type found at element index `elem_ind` in the custom attribute specified by the OKVTTLV parent object along with the attribute index.

Syntax

```
OKVErrNo okvCustomAttrGetTextString(OKVEnv *env, OKVTTLV *ttl,
                                     ub4 elem_ind, oratext *name,
                                     ub4 *namel, oratext *text,
                                     ub4 *textl, ub4 *attr_index);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle
<code>ttl</code>	IN	TTLV parent object
<code>elem_ind</code>	IN	Element index.
<code>name</code>	OUT	Name of the custom attribute.
<code>namel</code>	IN/OUT	Length of the name of the custom attribute.
<code>text</code>	OUT	Text string.
<code>textl</code>	IN/OUT	Length of the text string.
<code>attr_index</code>	OUT	Attribute index of text string custom attribute.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS</code> (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

Memory for the buffer for the text string data type should be pre-allocated and the size of memory passed in as `textl`.

Either memory for the buffer for the name of the custom attribute should be pre-allocated and the size of memory passed in as `name1`, or both `name` and `name1` should be `NULL`.

Example

```
OKVTTLV *ttl = (OKVTTLV *) NULL;
oracore_text *attr_name_list[1];
attr_name_list[0] = "x-My Text String";
ub4 attr_index = 0;
ub4 elem_ind = 0;
ub4 textl = 16;
ub4 name1 = 20;
...
okvGetAttributes(env, uid, 1, (oracore_text **) attr_name_list, &ttl);
oracore_text *text = (oracore_text *) malloc(textl * (sizeof(oracore_text)));
memset((void *) text, 0, textl);
oracore_text *name = (oracore_text *) malloc(name1 * (sizeof(oracore_text)));
memset((void *) name, 0, name1);
okvCustomAttrGetTextString(env, ttl, elem_ind, name,
    &name1, text,
    &textl, &attr_index);
printf ("%s", text);
...
free(name);
free(text);
```

Related Topics

- [okvCustomAttrAddTextString](#)
`okvCustomAttrAddTextString` adds a text string data type to the custom attribute specified by the `OKVTTLV` parent object.
- [okvCustomAttrGetTextStringLen](#)
`okvCustomAttrGetTextStringLen` returns the length of the text string data type found at the element index `elem_ind`.

12.2.27 okvCustomAttrGetTextStringLen

`okvCustomAttrGetTextStringLen` returns the length of the text string data type found at the element index `elem_ind`.

Category

KMIP custom attributes API

Purpose

`okvCustomAttrGetTextStringLen` returns the length of the text string data type found at element index `elem_ind` in the custom attribute specified by the `OKVTTLV` parent object.

Syntax

```
ub4 okvCustomAttrGetTextStringLen(OKVEnv *env, OKVTTLV *ttl,
    ub4 elem_ind);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle
ttlv	IN	TTLV parent object
elem_ind	IN	Element index

Return Values

Return Value	Description
ub4	Length of the attribute value. Success: Length of the text string data type attribute value. Failure: 0.

Comments

None.

Example

```
OKVTTLV *attrs = (OKVTTLV *)NULL;
oratext *attr_name_list[1];
attr_name_list[0] = "x-My Text String";
ub4 len = 0, elem_ind = 0;
...
okvGetAttributes(env, uid, 1, (oratext **) attr_name_list, &attrs);
len = okvCustomAttrGetTextStringLen(env, attrs, elem_ind);
```

Related Topics

- [okvCustomAttrAddTextString](#)
`okvCustomAttrAddTextString` adds a text string data type to the custom attribute specified by the OKVTTLV parent object.
- [okvCustomAttrGetTextString](#)
`okvCustomAttrGetTextString` returns the text string data type found at the element index `elem_ind`.

13

Oracle Key Vault Client SDK Extension Operation Management APIs

Oracle Key Vault client SDK provides operations used to execute custom KMIP requests.

- [About the Oracle Key Vault Client SDK Extension Operation Management APIs](#)
This section describes the interfaces for Oracle Key Vault operations used to execute custom KMIP requests.
- [okvOpsCreate](#)
`okvOpsCreate` creates the Oracle Key Vault operation handle that will be used to execute custom KMIP operations.
- [okvOpsExecuteOp](#)
`okvOpsExecuteOp` executes one or more custom KMIP operations.
- [okvOpsFree](#)
`okvOpsFree` frees the Oracle Key Vault operation handle.

13.1 About the Oracle Key Vault Client SDK Extension Operation Management APIs

This section describes the interfaces for Oracle Key Vault operations used to execute custom KMIP requests.

13.2 `okvOpsCreate`

`okvOpsCreate` creates the Oracle Key Vault operation handle that will be used to execute custom KMIP operations.

Category

KMIP extension operation management API

Purpose

`okvOpsCreate` is used to create the Oracle Key Vault operation handle which will be used to execute custom KMIP operations.

Syntax

```
OKVOps *okvOpsCreate(OKVEnv *env, OKVopsNo ops);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle

Parameter	IN/OUT	Description
ops	IN	KMIP operation

Return Values

Return Value	Description
OKVops*	Oracle Key Vault operation handle. Success: A valid pointer to the Oracle Key Vault operation handle is returned. Failure: A <code>NULL</code> pointer is returned.

Comments

Oracle Key Vault KMIP extension APIs can be used to create custom OKVTTLV request packets that can be sent to the Oracle Key Vault server to get a KMIP response packet. An operation with custom OKVTTLV request packet is a custom KMIP operation.

Oracle Key Vault KMIP extension APIs can also parse the KMIP response. Once the operation is executed, Oracle Key Vault operation handle will also hold the OKVTTLV response packet from the Oracle Key Vault server.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *) NULL;
...
OKVops *op = okvOpsCreate(env, OKVOpAddAttribute);
req = okvTTLVGetRequest(env, op);
attr_in = okvAddAttributeObject(env, req, OKVAttrName, 0);
okvAttrAddName(env, attr_in, "XYZ", strlen("XYZ"), 1);
okvAddAttribute(env, uid, &attr_in);
```

Related Topics

- [okvOpsExecuteOp](#)
okvOpsExecuteOp executes one or more custom KMIP operations.
- [okvOpsFree](#)
okvOpsFree frees the Oracle Key Vault operation handle.

13.3 okvOpsExecuteOp

okvOpsExecuteOp executes one or more custom KMIP operations.

Category

KMIP extension operation management API

Purpose

okvOpsExecuteOp is used to execute one or more custom KMIP operations. The operations are batched and executed.

Syntax

```
OKVErrNo okvOpsExecuteOp(OKVEnv *env, OKVOps **opsr, ub4 ops_cnt);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
opsr	IN	Oracle Key Vault operation handle.
ops_cnt	IN	Count of Oracle Key Vault operation handle.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

opsr is an array of operations to be batched and executed. ops_cnt is the count of the operations batched.

The error handle will hold the error returned by the Oracle Key Vault server. But this error need not be for all the operations in the operation array. Even if there is an error, the Oracle Key Vault operation handle should be checked for valid response packets.

There is no order to interpret the operation array. The result of the third operation can be processed before that of the first one.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *) NULL;
OKVTTLV *template;
OKVOps *ops[2];
...
/* First Batch Operation */
ops[0] = okvOpsCreate(env, OKVOpCreate);
req = okvTTLVGetRequest(env, ops[0]);
okvAttrAddObjectType(env, req, OKVObjSymmetric);
template = okvTTLVAddToObject(env, req, OKVDEF_TAG_TEMPLATE_ATTR_ST,
                              OKVDEF_ITEM_TYPE_STRUCT, (void *) NULL,
                              (ub4) 0);
attr_in = okvAddAttributeObject(env, template, OKVAttrCryptoAlg, 0);
okvAttrAddCryptoAlgo(env, attr_in, (ub4) CRYPTO_ALG_AES);
attr_in = okvAddAttributeObject(env, template, OKVAttrCryptoLen, 0);
okvAttrAddCryptoLen(env, attr_in, (ub4) 128);
attr_in = okvAddAttributeObject(env, template, OKVAttrCryptoUsageMask, 0);
okvAttrAddCryptoUsageMask(env, attr_in, (ub4) 12);
```

```

/* Second Batch Operation */
ops[1] = okvOpsCreate(env, OKVOpActivate);
req = okvTTLVGetRequest(env, ops[1]);

/* Execute Batch Operation */
okvOpsExecuteOp(env, ops, 2);

```

Related Topics

- [okvOpsCreate](#)
okvOpsCreate creates the Oracle Key Vault operation handle that will be used to execute custom KMIP operations.
- [okvOpsFree](#)
okvOpsFree frees the Oracle Key Vault operation handle.

13.4 okvOpsFree

okvOpsFree frees the Oracle Key Vault operation handle.

Category

KMIP extension operation management API

Purpose

okvOpsFree is used to free the Oracle Key Vault operation handle.

Syntax

```
void okvOpsFree(OKVEnv *env, OKVOps **ops);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle
ops	IN	Oracle Key Vault operation handle

Return Values

None.

Comments

None.

Example

```

OKVOps ops = okvOpsCreate(env, OKVOpCreate);
...
okvOpsFree(env, &ops);

```

Related Topics

- [okvOpsCreate](#)
`okvOpsCreate` creates the Oracle Key Vault operation handle that will be used to execute custom KMIP operations.
- [okvOpsExecuteOp](#)
`okvOpsExecuteOp` executes one or more custom KMIP operations.

Oracle Key Vault Client SDK TTLV Object APIs

The SDK `TTLV` object APIs enable you to perform activities such as getting the child of an `OKVTTLV` object.

- [About the Oracle Key Vault Client SDK TTLV Object APIs](#)
Oracle Key Vault provides interfaces for the Oracle Key Vault KMIP parser and builder, which help build the `OKVTTLV` objects and help parse them.
- [okvTTLVAddToObject](#)
`okvTTLVAddToObject` creates an `OKVTTLV` object and makes this object a child object of the `OKVTTLV` parent object.
- [okvTTLVAddToObjectByTag](#)
`okvTTLVAddToObjectByTag` creates an `OKVTTLV` object and makes this object a child object of the `OKVTTLV` parent object.
- [okvTTLVGetChild](#)
`okvTTLVGetChild` retrieves a child `OKVTTLV` object from the `OKVTTLV` object at the given element index.
- [okvTTLVGetChildByTag](#)
`okvTTLVGetChildByTag` retrieves a child `OKVTTLV` object from the `OKVTTLV` object with the specified tag.
- [okvTTLVGetChildCount](#)
`okvTTLVGetChildCount` returns the number of child `OKVTTLV` objects of the specified `OKVTTLV` parent object.
- [okvTTLVGetChildCountByTag](#)
`okvTTLVGetChildCountByTag` will return the number of child `OKVTTLV` objects of the specified `OKVTTLV` parent object that have the given tag.
- [okvTTLVGetFirstChildByTag](#)
`okvTTLVGetFirstChildByTag` retrieves the first child of the `OKVTTLV` object that has the specified tag.
- [okvTTLVGetLen](#)
`okvTTLVGetLen` returns the length of the value of the `OKVTTLV` object.
- [okvTTLVGetRequest](#)
`okvTTLVGetRequest` returns the `OKVTTLV` request object of the operation.
- [okvTTLVGetResponse](#)
`okvTTLVGetResponse` returns the `OKVTTLV` response object of the custom KMIP operation.
- [okvTTLVGetTag](#)
`okvTTLVGetTag` returns the tag value of the `OKVTTLV` object.
- [okvTTLVGetType](#)
`okvTTLVGetType` returns the type value of the `OKVTTLV` object.

- [okvTTLVGetValue](#)
`okvTTLVGetValue` returns the pointer to the value of the OKVTTLV object.
- [okvTTLVGetValueCopy](#)
`okvTTLVGetValueCopy` copies the value of the OKVTTLV object into the supplied buffer.

14.1 About the Oracle Key Vault Client SDK TTLV Object APIs

Oracle Key Vault provides interfaces for the Oracle Key Vault KMIP parser and builder, which help build the OKVTTLV objects and help parse them.

TTLV stands for tag type length value. The element and attribute indexes used in the Oracle Key Vault SDK TTLV object APIs have same meaning as the Oracle Key Vault KMIP attribute APIs.

Related Topics

- [About the Oracle Key Vault KMIP Attribute APIs](#)
This section describes the interfaces that help create and interpret Oracle Key Vault KMIP attributes.

14.2 okvTTLVAddToObject

`okvTTLVAddToObject` creates an OKVTTLV object and makes this object a child object of the OKVTTLV parent object.

Category

KMIP extension TTLV object API

Purpose

`okvTTLVAddToObject` will create an OKVTTLV object and make the newly created OKVTTLV object a child object of the OKVTTLV parent object.

Syntax

```
OKVTTLV *okvTTLVAddToObject(OKVEnv *env, OKVTTLV *ttlV,
                             OKVTag tag, OKVType typ, void *val, ub4 len);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>ttlV</code>	IN	OKVTTLV parent object.
<code>tag</code>	IN	Tag of the OKVTTLV object.
<code>typ</code>	IN	Type of the OKVTTLV object.
<code>val</code>	IN	Value of the OKVTTLV object.
<code>len</code>	IN	Length of value of the OKVTTLV object.

Return Values

Return Value	Description
OKVTTLV*	OKVTTLV object. Success: A valid pointer to the created OKVTTLV object is returned. Failure: A NULL pointer is returned.

Comments

None.

Example

```

OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *template;
...
OKVOps *ops = okvOpsCreate(env, OKVOpCreate);
req = okvTTLVGetRequest(env, ops);
...
template = okvTTLVAddToObject(env, req, OKVDEF_TAG_TEMPLATE_ATTR_ST,
                              OKVDEF_ITEM_TYPE_STRUCT, (void *) NULL,
                              (ub4) 0);

```

Related Topics

- [okvTTLVAddToObjectByTag](#)
okvTTLVAddToObjectByTag creates an OKVTTLV object and makes this object a child object of the OKVTTLV parent object.

14.3 okvTTLVAddToObjectByTag

okvTTLVAddToObjectByTag creates an OKVTTLV object and makes this object a child object of the OKVTTLV parent object.

Category

KMIP extension TTLV object API

Purpose

okvTTLVAddToObjectByTag will create an OKVTTLV object and make the newly created OKVTTLV object a child object of the OKVTTLV parent object.

Syntax

```

OKVTTLV *okvTTLVAddToObjectByTag(OKVEnv *env, OKVTTLV *ttl,
                                  OKVTag tag, void *val, ub4 len);

```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle

Parameter	IN/OUT	Description
ttlV	IN	OKVTTLV parent object
tag	IN	Tag of the OKVTTLV object
val	IN	Value of the OKVTTLV object
len	IN	Length of the value of the OKVTTLV object

Return Values

Return Value	Description
OKVTTLV*	OKVTTLV object Success: A valid pointer to the created OKVTTLV object is returned. Failure: A NULL pointer is returned.

Comments

The difference between `okvTTLVAddToObjectByTag` and `okvTTLVAddToObject` is that `okvTTLVAddToObjectByTag` will try to interpret the type from the tag. This can be done most of the times but not always.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *template;
...
OKVops *ops = okvOpsCreate(env, OKVopCreate);
req = okvTTLVGetRequest(env, ops);
...
template = okvTTLVAddToObjectByTag(env, req,
                                   OKVDEF_TAG_TEMPLATE_ATTR_ST,
                                   (void *) NULL, (ub4) 0);
```

Related Topics

- [okvTTLVAddToObject](#)
`okvTTLVAddToObject` creates an OKVTTLV object and makes this object a child object of the OKVTTLV parent object.

14.4 okvTTLVGetChild

`okvTTLVGetChild` retrieves a child OKVTTLV object from the OKVTTLV object at the given element index.

Category

KMIP extension TTLV object API

Purpose

`okvTTLVGetChild` retrieves a child OKVTTLV object from the OKVTTLV object at the given element index. The tag and type of the OKVTTLV object and length of the value of the OKVTTLV object are also returned.

Syntax

```
OKVTTLV *okvTTLVGetChild(OKVEnv *env, OKVTTLV *ttl,
                        ub4 elem_index,
                        OKVTag *tag, OKVType *typ, ub4 *len);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle
ttl	IN	OKVTTLV parent object
elem_index	IN	Element index of the child OKVTTLV object
tag	OUT	Tag of the child OKVTTLV object being retrieved
typ	OUT	Type of the OKVTTLV object being retrieved
len	OUT	Length of the value of the OKVTTLV object

Return Values

Return Value	Description
OKVTTLV*	Child OKVTTLV object at element index <code>elem_index</code> . Success: A valid pointer to the child OKVTTLV object at element index <code>elem_index</code> is returned. Failure: A NULL pointer is returned..

Comments

- If `elem_index` exceeds the number of children, then NULL is returned.
- The tag of the value of OKVTTLV object is also returned if `tag` is not NULL.
- The type of the value of OKVTTLV object is also returned if `typ` is not NULL.
- The length of the value of OKVTTLV object is also returned if `len` is not NULL.

Example

```
OKVTTLV *resp = (OKVTTLV *) NULL;
OKVTTLV *tagid = (OKVTTLV *) NULL;
OKVTag ctag;
OKVType ctyp;
ub4 clen;
...
OKVOps *ops = okvOpsCreate(env, OKVOpCreate);
resp = okvTTLVGetResponse(env, ops);
tagid = okvTTLVGetChild(env, resp, 1, &ctag, &ctyp, &clen);
```

Related Topics

- [okvTTLVGetChildByTag](#)
okvTTLVGetChildByTag retrieves a child OKVTTLV object from the OKVTTLV object with the specified tag.
- [okvTTLVGetFirstChildByTag](#)
okvTTLVGetFirstChildByTag retrieves the first child of the OKVTTLV object that has the specified tag.

14.5 okvTTLVGetChildByTag

okvTTLVGetChildByTag retrieves a child OKVTTLV object from the OKVTTLV object with the specified tag.

Category

KMIP extension TTLV object API

Purpose

okvTTLVGetChildByTag is used to retrieve a child OKVTTLV object from the OKVTTLV object with the specified tag at or after element index `elem_index`. The actual element index is also returned.

Syntax

```
OKVTTLV *okvTTLVGetChildByTag(OKVEnv *env, OKVTTLV *ttl,
                               OKVTag tag, ub4 *elem_index);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttl	IN	OKVTTLV parent object.
tag	IN	Tag of the OKVTTLV object being retrieved.
elem_index	IN/OUT	Element index of the child OKVTTLV object.

Return Values

Return Value	Description
OKVTTLV*	OKVTTLV object with the given tag. Success: A valid pointer to the child OKVTTLV object with the given tag at or after element index <code>elem_index</code> is returned. Failure: A NULL pointer is returned.

Comments

If `elem_index` exceeds the number of children, then NULL is returned.

Example

```

OKVTTLV *resp = (OKVTTLV *) NULL;
OKVTTLV *tagid = (OKVTTLV *) NULL;
OKVTag ctag;
OKVType ctyp;
ub4 clen;
ub4 elem_index = 0;
...
OKVOps *ops = okvOpsCreate(env, OKVOpCreate);
resp = okvTTLVGetResponse(env, ops);
tagid = okvTTLVGetChildByTag(env, resp, OKVDEF_TAG_ID, &elem_index);
ctag = okvTTLVGetTag(tagid);
ctyp = okvTTLVGetType(tagid);
clen = okvTTLVGetLen(tagid);

```

Related Topics

- [okvTTLVGetChild](#)
okvTTLVGetChild retrieves a child OKVTTLV object from the OKVTTLV object at the given element index.
- [okvTTLVGetFirstChildByTag](#)
okvTTLVGetFirstChildByTag retrieves the first child of the OKVTTLV object that has the specified tag.

14.6 okvTTLVGetChildCount

okvTTLVGetChildCount returns the number of child OKVTTLV objects of the specified OKVTTLV parent object.

Category

KMIP extension TTLV object API

Purpose

okvTTLVGetChildCount will return the number of child OKVTTLV objects of the specified OKVTTLV parent object.

Syntax

```
ub4 okvTTLVGetChildCount(OKVTTLV *ttlV);
```

Parameters

Parameter	IN/OUT	Description
ttlV	IN	OKVTTLV object

Return Values

Return Value	Description
ub4	<p>Number of child OKVTTLV objects of the specified OKVTTLV object.</p> <p>Success: Count of child OKVTTLV objects of the specified OKVTTLV parent object.</p> <p>Failure: A zero is returned on error or if the OKVTTLV parent object is not a <code>STRUCTURE</code>.</p>

Comments

If the specified OKVTTLV object is not a `STRUCTURE`, then zero is returned. If the specified OKVTTLV object is a `STRUCTURE` and there was an error, zero is returned.

Example

```
OKVTTLV *resp = (OKVTTLV *) NULL;
ub4 child_count;
...
OKVOps *ops = okvOpsCreate(env, OKVOpCreate);
resp = okvTTLVGetResponse(env, ops);
child_count = okvTTLVGetChildCount(resp);
```

Related Topics

- [okvTTLVGetChildCountByTag](#)
okvTTLVGetChildCountByTag will return the number of child OKVTTLV objects of the specified OKVTTLV parent object that have the given tag.

14.7 okvTTLVGetChildCountByTag

okvTTLVGetChildCountByTag will return the number of child OKVTTLV objects of the specified OKVTTLV parent object that have the given tag.

Category

KMIP extension TTLV object API

Purpose

okvTTLVGetChildCountByTag will return the number of child OKVTTLV objects of the specified OKVTTLV parent object that have the given tag.

Syntax

```
ub4 okvTTLVGetChildCountByTag(OKVTTLV *ttl, OKVTag tag);
```

Parameters

Parameter	IN/OUT	Description
ttl	IN	OKVTTLV object
tag	IN	Tag of the child OKVTTLV objects being counted

Return Values

Return Value	Description
ub4	<p>Number of child OKVTTLV Objects of the specified OKVTTLV parent object with the given tag.</p> <p>Success: Count of the child OKVTTLV objects of the specified OKVTTLV parent object with the given tag.</p> <p>Failure: A zero is returned on error or if the OKVTTLV parent object is not a STRUCTURE.</p>

Comments

If the specified OKVTTLV object is not a STRUCTURE, then zero is returned. If the specified OKVTTLV object is a STRUCTURE and there was an error, zero is returned.

Example

```
OKVTTLV *resp = (OKVTTLV *) NULL;
ub4 unique_id_count;
...
OKVOps *ops = okvOpsCreate(env, OKVOpCreate);
resp = okvTTLVGetResponse(env, ops);
unique_id_count = okvTTLVGetChildCountByTag(resp, OKVDEF_TAG_ID);
```

Related Topics

- [okvTTLVGetChildCount](#)
okvTTLVGetChildCount returns the number of child OKVTTLV objects of the specified OKVTTLV parent object.

14.8 okvTTLVGetFirstChildByTag

okvTTLVGetFirstChildByTag retrieves the first child of the OKVTTLV object that has the specified tag.

Category

KMIP extension TTLV object API

Purpose

okvTTLVGetFirstChildByTag is used to retrieve the first child of the OKVTTLV object that has the specified tag.

Syntax

```
OKVTTLV *okvTTLVGetFirstChildByTag(OKVEnv *env,
                                   OKVTTLV *ttl, OKVTag tag);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle
ttlv	IN	OKVTTLV parent object
tag	IN	Tag of the OKVTTLV object being retrieved

Return Values

Return Value	Description
OKVTTLV*	OKVTTLV object with the given tag. Success: A valid pointer to the child OKVTTLV object with the given tag is returned. Failure: A NULL pointer is returned.

Comments

None.

Example

```

OKVTTLV *resp = (OKVTTLV *) NULL;
OKVTTLV *tagid = (OKVTTLV *) NULL;
OKVTag ctag;
OKVType ctyp;
ub4 clen;
...
OKVOps *ops = okvOpsCreate(env, OKVOpCreate);
resp = okvTTLVGetResponse(env, ops);
tagid = okvTTLVGetFirstChildByTag(env, resp, OKVDEF_TAG_ID);
ctag = okvTTLVGetTag(tagid);
ctyp = okvTTLVGetType(tagid);
clen = okvTTLVGetLen(tagid);

```

Related Topics

- [okvTTLVGetChild](#)
okvTTLVGetChild retrieves a child OKVTTLV object from the OKVTTLV object at the given element index.
- [okvTTLVGetChildByTag](#)
okvTTLVGetChildByTag retrieves a child OKVTTLV object from the OKVTTLV object with the specified tag.

14.9 okvTTLVGetLen

okvTTLVGetLen returns the length of the value of the OKVTTLV object.

Category

KMIP extension TTLV object API

Purpose

okvTTLVGetLen will return the length of the value of the OKVTTLV object.

Syntax

```
ub4 okvTTLVGetLen(OKVTTLV *ttl);
```

Parameters

Parameter	IN/OUT	Description
ttl	IN	OKVTTLV object

Return Values

Return Value	Description
ub4	Length of the OKVTTLV object value Success: Length of the value of the OKVTTLV object is returned. Failure: A zero is returned if the OKVTTLV object is a STRUCTURE or if there was an error.

Comments

If length returned is zero, then it implies an error except when the OKVTTLV type is a STRUCTURE.

Example

```
OKVTTLV *resp = (OKVTTLV *) NULL;
OKVTTLV *tagid = (OKVTTLV *) NULL;
ub4 clen;
...
OKVOps *ops = okvOpsCreate(env, OKVOpCreate);
resp = okvTTLVGetResponse(env, ops);
tagid = okvTTLVGetFirstChildByTag(env, resp, OKVDEF_TAG_ID);
clen = okvTTLVGetLen(tagid);
```

Related Topics

- [okvTTLVGetTag](#)
okvTTLVGetTag returns the tag value of the OKVTTLV object.
- [okvTTLVGetType](#)
okvTTLVGetType returns the type value of the OKVTTLV object.
- [okvTTLVGetValue](#)
okvTTLVGetValue returns the pointer to the value of the OKVTTLV object.
- [okvTTLVGetValueCopy](#)
okvTTLVGetValueCopy copies the value of the OKVTTLV object into the supplied buffer.

14.10 okvTTLVGetRequest

okvTTLVGetRequest returns the OKVTTLV request object of the operation.

Category

KMIP extension TTLV object API

Purpose

okvTTLVGetRequest will return the OKVTTLV request object of the operation. This object will be the root OKVTTLV object used to build the KMIP Request. All OKVTTLV objects used in the KMIP request will fall under the OKVTTLV request object.

Syntax

```
OKVTTLV *okvTTLVGetRequest(OKVEnv *env, OKVOps *ops);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle
ops	IN	Oracle Key Vault operation handle

Return Values

Return Value	Description
OKVTTLV*	OKVTTLV request object for the operation. Success: A valid pointer to the OKVTTLV request object is returned. Failure: A NULL pointer is returned.

Comments

None.

Example

```
OKVTTLV *req = (OKVTTLV *) NULL;
OKVTTLV *attr_in = (OKVTTLV *)NULL;
...
OKVOps *op = okvOpsCreate(env, OKVOpAddAttribute);
req = okvTTLVGetRequest(env, op);
attr_in = okvAddAttributeObject(env, req, OKVAttrName, 0);
okvAttrAddName(env, attr_in, "XYZ", strlen("XYZ"), 1);
okvAddAttribute(env, uid, &attr_in);
```

Related Topics

- [okvTTLVGetResponse](#)
okvTTLVGetResponse returns the OKVTTLV response object of the custom KMIP operation.

14.11 okvTTLVGetResponse

okvTTLVGetResponse returns the OKVTTLV response object of the custom KMIP operation.

Category

KMIP extension TTLV object API

Purpose

okvTTLVGetResponse will return the OKVTTLV response object of the custom KMIP operation. This object will be used to parse the KMIP response from the Oracle Key Vault server. All OKVTTLV objects of the KMIP response have to be extracted and processed from the OKVTTLV response object.

Syntax

```
OKVTTLV *okvTTLVGetResponse (OKVEnv *env, OKVOps *ops);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ops	IN	Oracle Key Vault operation handle.

Return Values

Return Value	Description
OKVTTLV*	OKVTTLV response object of the operation. Success: A valid pointer to the OKVTTLV Response object is returned. Failure: A NULL pointer is returned.

Comments

None.

Example

```
OKVTTLV *resp = (OKVTTLV *) NULL;
OKVTTLV *tagid = (OKVTTLV *) NULL;
OKVTag ctag, rtag;
OKVType ctyp, rtyp;
oratext cval[OKV_UNIQUE_ID_MAXLEN + 1], rval[OKV_UNIQUE_ID_MAXLEN + 1];
ub4 clen, rlen;
OKVOps *ops[2];
...
/* Get the result of the First Batch Operation */
ops[0] = okvOpsCreate(env, OKVOpCreate);
resp = okvTTLVGetResponse(env, ops[0]);

/* Retrieve the Unique Identifier */
```

```

tagid = okvTTLVGetChild(env, resp, 1, &ctag, &ctyp, &cclen);
printf("\n%d %d %d ", ctag, ctyp, clen);
okvTTLVGetValueCopy(tagid, (void *)cval, clen);
cval[clen] = 0;
printf("%s\n", cval); /* Print the Unique Identifier */

/* Get the result of the Second Batch Operation */
ops[1] = okvOpsCreate(env, OKVOpActivate);
resp = okvTTLVGetResponse(env, ops[1]);

/* Retrieve the Unique Identifier */
tagid = okvTTLVGetChild(env, resp, 0, &rtag, &rtyp, &rclen);
printf("\n%d %d %d ", rtag, rtyp, rlen);
okvTTLVGetValueCopy(tagid, (void *)rval, rlen);
rval[rlen] = 0;
printf("%s\n", rval); /* Print the Unique Identifier */

```

Related Topics

- [okvTTLVGetRequest](#)
okvTTLVGetRequest returns the OKVTTLV request object of the operation.

14.12 okvTTLVGetTag

okvTTLVGetTag returns the tag value of the OKVTTLV object.

Category

KMIP extension TTLV object API

Purpose

okvTTLVGetTag will return the tag value of the OKVTTLV object.

Syntax

```
OKVTag okvTTLVGetTag(OKVTTLV *ttlV);
```

Parameters

Parameter	IN/OUT	Description
ttlV	IN	OKVTTLV object

Return Values

Return Value	Description
OKVTag	Tag of the OKVTTLV object. Success: A valid tag value of the OKVTTLV object is returned. Failure: A zero is returned.

Comments

None.

Example

```

OKVTTLV *resp = (OKVTTLV *) NULL;
OKVTTLV *tagid = (OKVTTLV *) NULL;
OKVTag ctag;
...
OKVOps *ops = okvOpsCreate(env, OKVOpCreate);
resp = okvTTLVGetResponse(env, ops);
tagid = okvTTLVGetFirstChildByTag(env, resp, OKVDEF_TAG_ID);
ctag = okvTTLVGetTag(tagid);

```

Related Topics

- [okvTTLVGetType](#)
okvTTLVGetType returns the type value of the OKVTTLV object.
- [okvTTLVGetLen](#)
okvTTLVGetLen returns the length of the value of the OKVTTLV object.
- [okvTTLVGetValue](#)
okvTTLVGetValue returns the pointer to the value of the OKVTTLV object.
- [okvTTLVGetValueCopy](#)
okvTTLVGetValueCopy copies the value of the OKVTTLV object into the supplied buffer.

14.13 okvTTLVGetType

okvTTLVGetType returns the type value of the OKVTTLV object.

Category

KMIP extension TTLV object API

Purpose

okvTTLVGetType will return the type value of the OKVTTLV object.

Syntax

```
OKVType okvTTLVGetType(OKVTTLV *ttlV);
```

Parameters

Parameter	IN/OUT	Description
ttlV	IN	OKVTTLV object

Return Values

Return Value	Description
OKVType	Type of the OKVTTLV object. Success: A valid Type value of the OKVTTLV object is returned. Failure: A zero is returned if there was an error.

Comments

None.

Example

```
OKVTTLV *resp = (OKVTTLV *) NULL;
OKVTTLV *tagid = (OKVTTLV *) NULL;
OKVType ctyp;
...
OKVOps *ops = okvOpsCreate(env, OKVOpCreate);
resp = okvTTLVGetResponse(env, ops);
tagid = okvTTLVGetFirstChildByTag(env, resp, OKVDEF_TAG_ID);
ctyp = okvTTLVGetType(tagid);
```

Related Topics

- [okvTTLVGetTag](#)
okvTTLVGetTag returns the tag value of the OKVTTLV object.
- [okvTTLVGetLen](#)
okvTTLVGetLen returns the length of the value of the OKVTTLV object.
- [okvTTLVGetValue](#)
okvTTLVGetValue returns the pointer to the value of the OKVTTLV object.
- [okvTTLVGetValueCopy](#)
okvTTLVGetValueCopy copies the value of the OKVTTLV object into the supplied buffer.

14.14 okvTTLVGetValue

okvTTLVGetValue returns the pointer to the value of the OKVTTLV object.

Category

KMIP extension TTLV object API

Purpose

okvTTLVGetValue returns the pointer to the value of the OKVTTLV object.

Syntax

```
void *okvTTLVGetValue(OKVTTLV *ttlV);
```

Parameters

Parameter	IN/OUT	Description
ttlV	IN	OKVTTLV object

Return Values

Return Value	Description
void*	OKVTTLV object value. Success: Pointer to the value of the OKVTTLV object is returned. Failure: A NULL pointer is returned if there is an error.

Comments

None.

Example

```

OKVTTLV *resp = (OKVTTLV *) NULL;
OKVTTLV *tagid = (OKVTTLV *) NULL;
ub4 clen;
oratext *cval;
...
OKVOps *ops = okvOpsCreate(env, OKVOpCreate);
resp = okvTTLVGetResponse(env, ops);
tagid = okvTTLVGetFirstChildByTag(env, resp, OKVDEF_TAG_ID);
clen = okvTTLVGetLen(tagid);
cval = (oratext *) okvTTLVGetValue(tagid);
cval[clen] = 0;
printf("%s", cval);

```

Related Topics

- [okvTTLVGetTag](#)
okvTTLVGetTag returns the tag value of the OKVTTLV object.
- [okvTTLVGetType](#)
okvTTLVGetType returns the type value of the OKVTTLV object.
- [okvTTLVGetLen](#)
okvTTLVGetLen returns the length of the value of the OKVTTLV object.
- [okvTTLVGetValueCopy](#)
okvTTLVGetValueCopy copies the value of the OKVTTLV object into the supplied buffer.

14.15 okvTTLVGetValueCopy

okvTTLVGetValueCopy copies the value of the OKVTTLV object into the supplied buffer.

Category

KMIP extension TTLV object API

Purpose

okvTTLVGetValueCopy will copy the value of the OKVTTLV object into the supplied buffer.

Syntax

```
ub4 okvTTLVGetValueCopy(OKVTTLV *ttl, void *val, ub4 len);
```

Parameters

Parameter	IN/OUT	Description
ttlv	IN	OKVTTLV object
val	OUT	Buffer for the OKVTTLV object value
len	IN	Length of the OKVTTLV object value

Return Values

Return Value	Description
ub4	Length of the OKVTTLV object value. Success: Length of the value of the OKVTTLV object is returned. Failure: Zero is returned.

Comments

The memory for the value has to be pre-allocated before making a call to this function.

Depending on the type of the OKVTTLV object, the value can be interpreted differently. For example, if the type of the OKVTTLV object is `INTEGER`, then the value can be stored in a `ub4` variable. However, if the OKVTTLV object is a `BYTE STRING`, the value is a `ub1` array of length `len`.

This function should not be used for OKVTTLV objects that are of type `STRUCTURE`.

Example

```
OKVTTLV *resp = (OKVTTLV *) NULL;
OKVTTLV *tagid = (OKVTTLV *) NULL;
ub4 clen;
oratext cval[OKV_UNIQUE_ID_MAXLEN + 1];
...
OKVOps *ops = okvOpsCreate(env, OKVOpCreate);
resp = okvTTLVGetResponse(env, ops);
tagid = okvTTLVGetFirstChildByTag(env, resp, OKVDEF_TAG_ID);
clen = okvTTLVGetLen(tagid);
okvTTLVGetValueCopy(tagid, (void *)cval, clen);
cval[clen] = 0;
printf("%s", cval);
```

Related Topics

- [okvTTLVGetTag](#)
`okvTTLVGetTag` returns the tag value of the OKVTTLV object.
- [okvTTLVGetType](#)
`okvTTLVGetType` returns the type value of the OKVTTLV object.
- [okvTTLVGetLen](#)
`okvTTLVGetLen` returns the length of the value of the OKVTTLV object.

- [okvTTLVGetValue](#)
okvTTLVGetValue returns the pointer to the value of the OKVTTLV object.

Oracle Key Vault Client SDK Utility APIs

You can use the Oracle Key Vault client SDK utility APIs with other Oracle Key Vault functions to simplify common operations.

The element and attribute index used in the Oracle Key Vault utility functions have the same meaning as described in section [Attribute Index and Element Index](#).

- [About the Oracle Key Vault Client SDK Utility APIs](#)
You can use the Oracle Key Vault SDK utility APIs with other Oracle Key Vault APIs to simplify commonly used operations.
- [okvAttrExtractTTLV](#)
`okvAttrExtractTTLV` converts the attributes that are child OKVTTLV objects of the specified OKVTTLV parent object into `OKVAttr`.
- [okvAttrMakeTTLV](#)
`okvAttrMakeTTLV` converts the `OKVAttr` into an OKVTTLV structure.
- [okvCryptoContextCreate](#)
`okvCryptoContextCreate` creates the cryptographic context required for cryptographic operations.
- [okvCryptoContextFree](#)
`okvCryptoContextFree` frees the memory allocated to cryptographic context structure.
- [okvCryptoContextGetAuthEncryptionAdditionalData](#)
`okvCryptoContextGetAuthEncryptionAdditionalData` gets the authenticated encryption additional data parameter value from cryptographic context structure.
- [okvCryptoContextGetAuthEncryptionTag](#)
`okvCryptoContextGetAuthEncryptionTag` gets the authenticated encryption tag parameter value from cryptographic context structure.
- [okvCryptoContextGetBlockCipherMode](#)
`okvCryptoContextGetBlockCipherMode` gets the block cipher mode parameter value from cryptographic context structure.
- [okvCryptoContextGetIV](#)
`okvCryptoContextGetIV` gets the IV parameter value from cryptographic context structure.
- [okvCryptoContextGetPadding](#)
`okvCryptoContextGetPadding` gets the padding parameter value from cryptographic context structure.
- [okvCryptoContextGetRandomIV](#)
`okvCryptoContextGetRandomIV` gets the random IV parameter value from cryptographic context structure.
- [okvCryptoContextSetAuthEncryptionAdditionalData](#)
`okvCryptoContextSetAuthEncryptionAdditionalData` sets the authenticated encryption additional data parameter value in the cryptographic context structure.

- [okvCryptoContextSetAuthEncryptionTag](#)
`okvCryptoContextSetAuthEncryptionTag` sets the authenticated encryption tag parameter value in the cryptographic context structure.
- [okvCryptoContextSetBlockCipherMode](#)
`okvCryptoContextSetBlockCipherMode` sets the block cipher mode parameter value in the cryptographic context structure.
- [okvCryptoContextSetIV](#)
`okvCryptoContextSetIV` sets the IV parameter value in the cryptographic context structure.
- [okvCryptoContextSetPadding](#)
`okvCryptoContextSetPadding` sets the padding parameter value in the cryptographic context structure.
- [okvCryptoContextSetRandomIV](#)
`okvCryptoContextSetRandomIV` sets the random IV parameter value in the cryptographic context structure.
- [okvCryptoResponseGetAuthEncryptionTag](#)
`okvCryptoResponseGetAuthEncryptionTag` gets the authenticated encryption tag value from encrypt response structure.
- [okvCryptoResponseGetDecryptedData](#)
`okvCryptoResponseGetDecryptedData` gets the decrypted data value from decrypt response structure.
- [okvCryptoResponseGetEncryptedData](#)
`okvCryptoResponseGetEncryptedData` gets the encrypted data value from encrypt response structure.
- [okvCryptoResponseGetIV](#)
`okvCryptoResponseGetIV` gets the IV value from encrypt response structure used by server for encryption, if the random IV was set and IV was not provided in the request.
- [okvDecryptResponseCreate](#)
`okvDecryptResponseCreate` creates the decrypt response structure to hold the decrypt operation response details.
- [okvDecryptResponseFree](#)
`okvDecryptResponseFree` frees the memory allocated to decrypt response structure.
- [okvEncryptResponseCreate](#)
`okvEncryptResponseCreate` creates the encrypt response structure to hold the encrypt operation response details.
- [okvEncryptResponseFree](#)
`okvEncryptResponseFree` frees the memory allocated to encrypt response structure.
- [okvGetTextForAttributeNum](#)
`okvGetTextForAttributeNum` returns the attribute name for a given Oracle Key Vault attribute number.
- [okvGetTextForTag](#)
`okvGetTextForTag` returns the name of the valid KMIP tag.

- [okvGetTextForTagEnum](#)
`okvGetTextForTagEnum` returns the name of the enumerated value for a valid KMIP tag of `ENUMERATION` type.
- [okvGetTextForTagType](#)
`okvGetTextForTagType` returns the name of the valid KMIP type.
- [okvGetTextLenForAttributeNum](#)
`okvGetTextLenForAttributeNum` returns the length of the name of the attribute for a given Oracle Key Vault attribute number.
- [okvObjGetAttrNo](#)
`okvObjGetAttrNo` will return the Oracle Key Vault attribute number for a given TTLV object.
- [okvCryptoContextSetCryptoAlgo](#)
`okvCryptoContextSetCryptoAlgo` sets the cryptographic algorithm parameter value in the cryptographic context structure.
- [okvCryptoContextSetHashingAlgo](#)
`okvCryptoContextSetHashingAlgo` sets the hashing algorithm parameter value in the cryptographic context structure.
- [okvCryptoContextSetDigitalSignAlgo](#)
`okvCryptoContextSetDigitalSignAlgo` sets the digital signature algorithm parameter value in the cryptographic context structure.
- [okvCryptoContextGetCryptoAlgo](#)
`okvCryptoContextGetCryptoAlgo` gets the cryptographic algorithm parameter value from cryptographic context structure.
- [okvCryptoContextGetHashingAlgo](#)
`okvCryptoContextGetHashingAlgo` gets the hashing algorithm parameter value in the cryptographic context structure.
- [okvCryptoContextGetDigitalSignAlgo](#)
`okvCryptoContextGetDigitalSignAlgo` gets the digital signature algorithm parameter value from cryptographic context structure.
- [okvCryptoResponseGetSignatureData](#)
`okvCryptoResponseGetSignatureData` gets the signature data value from the sign response structure.
- [okvCryptoResponseGetRecoveredData](#)
`okvCryptoResponseGetRecoveredData` gets the recovered data value from the signature verify response structure.
- [okvCryptoResponseGetValidity](#)
`okvCryptoResponseGetValidity` gets the validity value from the signature verify response structure.
- [okvSignResponseCreate](#)
`okvSignResponseCreate` creates the sign response structure to hold the sign operation response details.
- [okvSignResponseFree](#)
`okvSignResponseFree` frees the memory allocated to the sign response structure.
- [okvSignVerifyResponseCreate](#)
`okvSignVerifyResponseCreate` creates the signature verify response structure to hold the signature verify operation response details.

- [okvSignVerifyResponseFree](#)
`okvSignVerifyResponseFree` frees the memory allocated to the signature verify response structure.

15.1 About the Oracle Key Vault Client SDK Utility APIs

You can use the Oracle Key Vault SDK utility APIs with other Oracle Key Vault APIs to simplify commonly used operations.

The client SDK utility API element and attribute indexes have the same structure as the Oracle Key Vault KMIP attribute APIs.

Related Topics

- [About the Oracle Key Vault KMIP Attribute APIs](#)
This section describes the interfaces that help create and interpret Oracle Key Vault KMIP attributes.

15.2 `okvAttrExtractTTLV`

`okvAttrExtractTTLV` converts the attributes that are child OKVTTLV objects of the specified OKVTTLV parent object into OKVAttr.

Category

KMIP utility API

Purpose

`okvAttrExtractTTLV` will convert the attributes that are child OKVTTLV objects of the specified OKVTTLV parent object into OKVAttr.

Syntax

```
OKVErrNo okvAttrExtractTTLV(OKVEnv *env, OKVTTLV *attr_ttlv,
                             OKVAttr *attr_col);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>attr_ttlv</code>	IN	TTLV parent object containing attributes.
<code>attr_col</code>	OUT	Collection of attributes.

Return Values

Return Value	Description
<code>OKVErrNo</code>	Oracle Key Vault error number. Success: <code>OKV_SUCCESS (0)</code> is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

None.

Example

```

OKVAttr attr_struct;
ub4 index = 0;
memset((void *)&attr_struct, 0, sizeof(attr_struct));
...
okvAttrExtractTTLV(env, ttlv, &attr_struct);
printf("\nAttributes Extracted:");
printf("\nName: %s ", attr_struct.name[index].name);
printf("\nName Length: %d ", attr_struct.name[index].name1);

/* Null terminate the unique identifier */
attr_struct.unique_identifier.id[attr_struct.unique_identifier.idl] = 0;
printf("\nUnique ID: %s ", attr_struct.unique_identifier.id);
printf("\nUnique ID Length: %d ", attr_struct.unique_identifier.idl);
printf("\nCryptographic Algorithm: %d ", attr_struct.crypto_algorithm);

```

Related Topics

- [okvAttrMakeTTLV](#)
okvAttrMakeTTLV converts the OKVAttr into an OKVTTLV structure.

15.3 okvAttrMakeTTLV

okvAttrMakeTTLV converts the OKVAttr into an OKVTTLV structure.

Category

KMIP utility API

Purpose

okvAttrMakeTTLV will convert the OKVAttr into an OKVTTLV structure and all the new attributes in the OKVTTLV will be collected under the specified OKVTTLV parent object.

Syntax

```

OKVErrNo okvAttrMakeTTLV(OKVEnv *env, OKVAttr *attr_col
                        OKVTTLV *attr_ttlv);

```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
attr_col	IN	Collection of attributes.
attr_ttlv	OUT	TTLV parent object containing attributes.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Comments

For multi-instance attributes, the count of the attribute must be set. For example, `name` is a multi-instance attribute. Hence, if `name` is being added, `name_count` must also be specified.

Example

```
OKVTTLV *ttlV = (OKVTTLV *)NULL;
OKVOps *ops;
OKVAttr attrs;
memset((void *)&attrs, 0, sizeof(attrs));
...

/* Adding name attribute to the structure */
ub4 index = 0;
attrs.name_count = 1;
attrs.name[index].name = "attr_name";
attrs.name[index].name1 = strlen(attrs.name[index].name);
attrs.name[index].type = 1;

/* Adding cryptographic algo attribute to the structure */
attrs.crypto_algorithm = CRYPTO_ALG_AES;

/* Adding unique identifier attribute to the structure */
attrs.unique_identifier.id = uid;
attrs.unique_identifier.id1 = strlen(attrs.unique_identifier.id);
ops = okvOpsCreate(env, OKVOpAddAttribute);
ttlV = okvTTLVGetRequest(env, ops);

/* Convert OKVAttr structure to TTLV Attributes Object */
okvAttrMakeTTLV(env, &attrs, ttlV);
```

Related Topics

- [okvAttrExtractTTLV](#)
`okvAttrExtractTTLV` converts the attributes that are child OKVTTLV objects of the specified OKVTTLV parent object into OKVAttr.

15.4 okvCryptoContextCreate

`okvCryptoContextCreate` creates the cryptographic context required for cryptographic operations.

Category

KMIP utility API

Purpose

okvCryptoContextCreate creates the cryptographic context required for cryptographic operations OR encrypt, decrypt, sign, and signature verify operations.

Syntax

```
OKVCryptoContext *okvCryptoContextCreate(OKVEnv *env, OKVOpNo operation);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
operation	IN	KMIP operation.

Return Values

Return Value	Description
OKVCryptoContext *	Pointer to OKVCryptoContext object. Success: Pointer to OKVCryptoContext object. Failure: NULL pointer.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVCryptoContext *crypto_context = okvCryptoContextCreate(env, OKVOpEncrypt);
```

Related Topics

- [okvCryptoContextFree](#)
okvCryptoContextFree frees the memory allocated to cryptographic context structure.

15.5 okvCryptoContextFree

okvCryptoContextFree frees the memory allocated to cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextFree frees the memory allocated to cryptographic context structure.

Syntax

```
void okvCryptoContextFree(OKVEnv *env, OKVCryptoContext** crypto_context);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for cryptographic operations.

Return Values

No values returned.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVCryptoContext *crypto_context = okvCryptoContextCreate(env, OKVOpEncrypt);
...
okvCryptoContextFree(env, &crypto_context);
```

Related Topics

- [okvCryptoContextCreate](#)
okvCryptoContextCreate creates the cryptographic context required for cryptographic operations.

15.6 okvCryptoContextGetAuthEncryptionAdditionalData

okvCryptoContextGetAuthEncryptionAdditionalData gets the authenticated encryption additional data parameter value from cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextGetAuthEncryptionAdditionalData gets the Authenticated encryption additional data parameter value from cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextGetAuthEncryptionAdditionalData(OKVEnv *env,
                                                         OKVCryptoContext
                                                         *crypto_context,
                                                         ub1
                                                         *auth_encryption_additional_data,
                                                         ub4
                                                         *auth_encryption_additional_data);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for encryption/decryption like cryptographic parameters and IV.
auth_encryption_additional_data	OUT	Authenticated encryption additional data value.
auth_encryption_additional_data1	OUT	Authenticated encryption additional data value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub1 *auth_enc_addl_data = (ub1 *)NULL;
ub4 auth_enc_addl_data1 = 0;
okvCryptoContextGetAuthEncryptionAdditionalData (env, crypto_context,
                                                auth_enc_addl_data,
                                                &auth_enc_addl_data1);
```

Related Topics

- [okvCryptoContextSetAuthEncryptionAdditionalData](#)
okvCryptoContextSetAuthEncryptionAdditionalData sets the authenticated encryption additional data parameter value in the cryptographic context structure.

15.7 okvCryptoContextGetAuthEncryptionTag

okvCryptoContextGetAuthEncryptionTag gets the authenticated encryption tag parameter value from cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextGetAuthEncryptionTag gets the Authenticated encryption tag parameter value from cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextGetAuthEncryptionTag (OKVEnv *env,
                                               OKVCryptoContext *crypto_context,
                                               ub1 *auth_encryption_tag,
                                               ub4 *auth_encryption_tagl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for encryption/decryption like cryptographic parameters and IV.
auth_encryption_tag	OUT	Authenticated encryption tag value.
auth_encryption_tagl	OUT	Authenticated encryption tag value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub1 *auth_enc_tag = (ub1 *)NULL;
ub4 auth_enc_tagl = 0;
okvCryptoContextGetAuthEncryptionTag(env, crypto_context,
                                     auth_enc_tag, &auth_enc_tagl);
```

Related Topics

- [okvCryptoContextSetAuthEncryptionTag](#)
okvCryptoContextSetAuthEncryptionTag sets the authenticated encryption tag parameter value in the cryptographic context structure.

15.8 okvCryptoContextGetBlockCipherMode

okvCryptoContextGetBlockCipherMode gets the block cipher mode parameter value from cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextGetBlockCipherMode gets the block cipher mode parameter value from cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextGetBlockCipherMode(OKVEnv *env,  
                                             OKVCryptoContext *crypto_context,  
                                             ub4 *block_cipher_mode);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for encryption/decryption like cryptographic parameters and IV.
block_cipher_mode	OUT	Block Cipher Mode value.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub4 block_cipher_mode;  
okvCryptoContextGetBlockCipherMode(env, crypto_context, &block_cipher_mode);
```

Related Topics

- [okvCryptoContextSetBlockCipherMode](#)
okvCryptoContextSetBlockCipherMode sets the block cipher mode parameter value in the cryptographic context structure.

15.9 okvCryptoContextGetIV

okvCryptoContextGetIV gets the IV parameter value from cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextGetIV gets the IV parameter value from cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextGetIV(OKVEnv *env,
                               OKVCryptoContext *crypto_context,
                               ub1 *iv, ub4 *ivl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for encryption/decryption like cryptographic parameters and IV.
iv	OUT	IV value.
ivl	OUT	IV value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub1 *iv = (ub1 *)NULL;
ub4 ivl = 0;
okvCryptoContextGetIV(env, crypto_context, iv, &ivl);
```

Related Topics

- [okvCryptoContextSetIV](#)
okvCryptoContextSetIV sets the IV parameter value in the cryptographic context structure.

15.10 okvCryptoContextGetPadding

okvCryptoContextGetPadding gets the padding parameter value from cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextGetPadding gets the padding parameter value from cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextGetPadding(OKVEnv *env,
                                     OKVCryptoContext *crypto_context,
                                     ub4 *padding);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for cryptographic operations.
padding	OUT	Padding value.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub4 padding;
okvCryptoContextGetPadding(env, crypto_context, &padding);
```

Related Topics

- [okvCryptoContextSetPadding](#)
okvCryptoContextSetPadding sets the padding parameter value in the cryptographic context structure.

15.11 okvCryptoContextGetRandomIV

okvCryptoContextGetRandomIV gets the random IV parameter value from cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextGetRandomIV gets the random IV parameter value from cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextGetRandomIV(OKVEnv *env,
                                       OKVCryptoContext *crypto_context,
                                       ub8 *random_iv);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for encryption/decryption like cryptographic parameters and IV.
random_iv	OUT	Random IV value.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub8 random_iv;
okvCryptoContextGetRandomIV(env, crypto_context, &random_iv);
```

Related Topics

- [okvCryptoContextSetRandomIV](#)
okvCryptoContextSetRandomIV sets the random IV parameter value in the cryptographic context structure.

15.12 okvCryptoContextSetAuthEncryptionAdditionalData

okvCryptoContextSetAuthEncryptionAdditionalData sets the authenticated encryption additional data parameter value in the cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextSetAuthEncryptionAdditionalData sets the Authenticated encryption additional data parameter value in the cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextSetAuthEncryptionAdditionalData(OKVEnv *env,
                                                         OKVCryptoContext
                                                         *crypto_context,
                                                         ub1
                                                         *auth_encryption_additional_data,
                                                         ub4
                                                         auth_encryption_additional_data);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for encryption/decryption like cryptographic parameters and IV.
auth_encryption_additional_data	IN	Authenticated encryption additional data value.
auth_encryption_additional_data_length	IN	Authenticated encryption additional data value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVCryptoContext *crypto_context = okvCryptoContextCreate(env, OKVOpEncrypt);
ub1 auth_enc_addl_data[] = "Additional Data";
ub4 auth_enc_addl_data1 = strlen((const char *) auth_enc_addl_data);
okvCryptoContextSetAuthEncryptionAdditionalData(env, crypto_context,
auth_enc_addl_data,
                                auth_enc_addl_data1);
```

Related Topics

- [okvCryptoContextGetAuthEncryptionAdditionalData](#)
okvCryptoContextGetAuthEncryptionAdditionalData gets the authenticated encryption additional data parameter value from cryptographic context structure.

15.13 okvCryptoContextSetAuthEncryptionTag

okvCryptoContextSetAuthEncryptionTag sets the authenticated encryption tag parameter value in the cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextSetAuthEncryptionTag sets the Authenticated encryption tag parameter value in the cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextSetAuthEncryptionTag(OKVEnv *env,
                                OKVCryptoContext *crypto_context,
                                ub1 *auth_encryption_tag,
                                ub4 auth_encryption_tag1);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for encryption/decryption like cryptographic parameters and IV.
auth_encryption_tag	IN	Authenticated encryption tag value.
auth_encryption_tagl	IN	Authenticated encryption tag value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVCryptoContext *crypto_context = okvCryptoContextCreate(env, OKVOpEncrypt);
ub1 auth_enc_tag[] = "Auth Tag";
ub4 auth_enc_tagl = strlen((const char *) auth_enc_tag);
okvCryptoContextSetAuthEncryptionTag(env, crypto_context, auth_enc_tag, auth_enc_tagl);
```

Related Topics

- [okvCryptoContextGetAuthEncryptionTag](#)
`okvCryptoContextGetAuthEncryptionTag` gets the authenticated encryption tag parameter value from cryptographic context structure.

15.14 okvCryptoContextSetBlockCipherMode

`okvCryptoContextSetBlockCipherMode` sets the block cipher mode parameter value in the cryptographic context structure.

Category

KMIP utility API

Purpose

`okvCryptoContextSetBlockCipherMode` sets the block cipher mode parameter value in the cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextSetBlockCipherMode (OKVEnv *env,
                                             OKVCryptoContext *crypto_context,
                                             ub4 block_cipher_mode);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for encryption/decryption like cryptographic parameters and IV.
block_cipher_mode	IN	Block Cipher Mode value.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVCryptoContext *crypto_context = okvCryptoContextCreate(env, OKVOpEncrypt);
okvCryptoContextSetBlockCipherMode(env, crypto_context, BLK_CIPHER_CBC);
```

Related Topics

- [okvCryptoContextGetBlockCipherMode](#)
`okvCryptoContextGetBlockCipherMode` gets the block cipher mode parameter value from cryptographic context structure.

15.15 okvCryptoContextSetIV

`okvCryptoContextSetIV` sets the IV parameter value in the cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextSetIV sets the IV parameter value in the cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextSetIV(OKVEnv *env,
                                OKVCryptoContext *crypto_context,
                                ub1 *iv, ub4 ivl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for encryption/decryption like cryptographic parameters and IV.
iv	IN	IV value.
ivl	IN	IV value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVCryptoContext *crypto_context = okvCryptoContextCreate(env, OKVOpEncrypt);
ub1 iv[] = "5432109876543210";
ub4 ivl = strlen((const char *) iv);
okvCryptoContextSetIV(env, crypto_context, iv, ivl);
```

Related Topics

- [okvCryptoResponseGetIV](#)
okvCryptoResponseGetIV gets the IV value from encrypt response structure used by server for encryption, if the random IV was set and IV was not provided in the request.

15.16 okvCryptoContextSetPadding

okvCryptoContextSetPadding sets the padding parameter value in the cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextSetPadding sets the padding parameter value in the cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextSetPadding(OKVEnv *env,  
                                     OKVCryptoContext *crypto_context,  
                                     ub4 padding);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for cryptographic operations like cryptographic parameters and IV.
padding	IN	Padding value.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVCryptoContext *crypto_context = okvCryptoContextCreate(env, OKVOpEncrypt);  
okvCryptoContextSetPadding(env, crypto_context, PADDING_PKCS5);
```

Related Topics

- [okvCryptoContextGetPadding](#)
okvCryptoContextGetPadding gets the padding parameter value from cryptographic context structure.

15.17 okvCryptoContextSetRandomIV

okvCryptoContextSetRandomIV sets the random IV parameter value in the cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextSetRandomIV sets the random IV parameter value in the cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextSetRandomIV(OKVEnv *env,
                                       OKVCryptoContext *crypto_context,
                                       ub8 random_iv);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for encryption/decryption like cryptographic parameters and IV.
random_iv	IN	Random IV value.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVCryptoContext *crypto_context = okvCryptoContextCreate(env, OKVOpEncrypt);
okvCryptoContextSetRandomIV(env, crypto_context, (ub8)1);
```

Related Topics

- [okvCryptoContextGetRandomIV](#)
okvCryptoContextGetRandomIV gets the random IV parameter value from cryptographic context structure.

15.18 okvCryptoResponseGetAuthEncryptionTag

okvCryptoResponseGetAuthEncryptionTag gets the authenticated encryption tag value from encrypt response structure.

Category

KMIP utility API

Purpose

okvCryptoResponseGetAuthEncryptionTag gets the Authenticated encryption tag value from encrypt response structure.

Syntax

```
OKVErrNo okvCryptoResponseGetAuthEncryptionTag(OKVEnv *env,
                                               OKVEncryptResponse
*encrypt_response,
                                               ub1 *auth_encryption_tag,
                                               ub4 *auth_encryption_tagl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
encrypt_response	IN	Encrypt operation response.
auth_encryption_tag	OUT	Authenticated encryption tag value.
auth_encryption_tagl	OUT	Authenticated encryption tag value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub1 auth_enc_tag[100];
ub4 auth_enc_tag1 = sizeof(auth_enc_tag);
...
/* Perform Encrypt operation and get encrypt operation response in 'encrypt_response'
*/
...
memset(auth_enc_tag, 0, auth_enc_tag1);
okvCryptoResponseGetAuthEncryptionTag(env, encrypt_response, auth_enc_tag,
&auth_enc_tag1);
```

Related Topics

- [okvCryptoResponseGetEncryptedData](#)
okvCryptoResponseGetEncryptedData gets the encrypted data value from encrypt response structure.
- [okvCryptoResponseGetIV](#)
okvCryptoResponseGetIV gets the IV value from encrypt response structure used by server for encryption, if the random IV was set and IV was not provided in the request.
- [okvEncryptResponseCreate](#)
okvEncryptResponseCreate creates the encrypt response structure to hold the encrypt operation response details.
- [okvEncryptResponseFree](#)
okvEncryptResponseFree frees the memory allocated to encrypt response structure.

15.19 okvCryptoResponseGetDecryptedData

okvCryptoResponseGetDecryptedData gets the decrypted data value from decrypt response structure.

Category

KMIP utility API

Purpose

okvCryptoResponseGetDecryptedData gets the decrypted data value from decrypt response structure.

Syntax

```
OKVErrNo okvCryptoResponseGetDecryptedData (OKVEnv *env,
                                             OKVDecryptResponse *decrypt_response,
                                             ub1 *decrypted_data,
                                             ub4 *decrypted_data1);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
decrypt_response	IN	Decrypt operation response.
decrypted_data	OUT	Decrypted data value.
decrypted_data1	OUT	Decrypted data value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub1 decrypted_data[100];
ub4 decrypted_data1 = sizeof(decrypted_data);
...
/* Perform Decrypt operation and get decrypt operation response in
'decrypt_response' */
...
memset(decrypted_data, 0, decrypted_data1);
okvCryptoResponseGetDecryptedData(env, decrypt_response, decrypted_data,
&decrypted_data1);
```

Related Topics

- [okvDecryptResponseCreate](#)
okvDecryptResponseCreate creates the decrypt response structure to hold the decrypt operation response details.
- [okvDecryptResponseFree](#)
okvDecryptResponseFree frees the memory allocated to decrypt response structure.

15.20 okvCryptoResponseGetEncryptedData

okvCryptoResponseGetEncryptedData gets the encrypted data value from encrypt response structure.

Category

KMIP utility API

Purpose

okvCryptoResponseGetEncryptedData gets the encrypted data value from encrypt response structure.

Syntax

```
OKVErrNo okvCryptoResponseGetEncryptedData (OKVEnv *env,
                                             OKVEncryptResponse *encrypt_response,
                                             ub1 *encrypted_data, ub4 *encrypted_data1);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
encrypt_response	IN	Encrypt operation response.
encrypted_data	OUT	Encrypted data value.
encrypted_data1	OUT	Encrypted data value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub1 encrypted_data[100];
ub4 encrypted_data1 = sizeof(encrypted_data);
...
/* Perform Encrypt operation and get encrypt operation response in 'encrypt_response'
*/
...
```



```
memset(encrypted_data, 0, encrypted_data1);
okvCryptoResponseGetEncryptedData(env, encrypt_response, encrypted_data,
&encrypted_data1);
```

Related Topics

- [okvCryptoResponseGetAuthEncryptionTag](#)
okvCryptoResponseGetAuthEncryptionTag gets the authenticated encryption tag value from encrypt response structure.
- [okvCryptoResponseGetIV](#)
okvCryptoResponseGetIV gets the IV value from encrypt response structure used by server for encryption, if the random IV was set and IV was not provided in the request.
- [okvEncryptResponseCreate](#)
okvEncryptResponseCreate creates the encrypt response structure to hold the encrypt operation response details.
- [okvEncryptResponseFree](#)
okvEncryptResponseFree frees the memory allocated to encrypt response structure.

15.21 okvCryptoResponseGetIV

okvCryptoResponseGetIV gets the IV value from encrypt response structure used by server for encryption, if the random IV was set and IV was not provided in the request.

Category

KMIP utility API

Purpose

okvCryptoResponseGetIV gets the IV value from encrypt response structure used by server for encryption, if the random IV was set and IV was not provided in the request.

Syntax

```
OKVErrNo okvCryptoResponseGetIV(OKVEnv *env,
                                OKVEncryptResponse *encrypt_response,
                                ub1 *iv, ub4 *ivl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
encrypt_response	IN	Encrypt operation response.
iv	OUT	IV value.
ivl	OUT	IV value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) is returned. Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
ub1 iv[100];
ub4 ivl = sizeof(iv);
...
/* Perform Encrypt operation and get encrypt operation response in 'encrypt_response'
*/
...
memset(iv, 0, ivl);
okvCryptoResponseGetIV(env, encrypt_response, iv, &ivl);
```

Related Topics

- [okvCryptoContextGetAuthEncryptionTag](#)
`okvCryptoContextGetAuthEncryptionTag` gets the authenticated encryption tag parameter value from cryptographic context structure.
- [okvCryptoResponseGetEncryptedData](#)
`okvCryptoResponseGetEncryptedData` gets the encrypted data value from encrypt response structure.
- [okvEncryptResponseCreate](#)
`okvEncryptResponseCreate` creates the encrypt response structure to hold the encrypt operation response details.
- [okvEncryptResponseFree](#)
`okvEncryptResponseFree` frees the memory allocated to encrypt response structure.

15.22 okvDecryptResponseCreate

`okvDecryptResponseCreate` creates the decrypt response structure to hold the decrypt operation response details.

Category

KMIP utility API

Purpose

`okvDecryptResponseCreate` creates the decrypt response structure to hold the decrypt operation response details.

Syntax

```
OKVDecryptResponse *okvDecryptResponseCreate(OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
<code>OKVDecryptResponse *</code>	Pointer to <code>OKVDecryptResponse</code> object. Success: Pointer to <code>OKVDecryptResponse</code> object. Failure: NULL pointer.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVDecryptResponse *decrypt_response = okvDecryptResponseCreate(env);
```

Related Topics

- [okvCryptoResponseGetDecryptedData](#)
`okvCryptoResponseGetDecryptedData` gets the decrypted data value from decrypt response structure.
- [okvDecryptResponseFree](#)
`okvDecryptResponseFree` frees the memory allocated to decrypt response structure.

15.23 okvDecryptResponseFree

`okvDecryptResponseFree` frees the memory allocated to decrypt response structure.

Category

KMIP utility API

Purpose

okvDecryptResponseFree frees the memory allocated to decrypt response structure.

Syntax

```
void okvDecryptResponseFree (OKVEnv *env, OKVDecryptResponse** decrypt_response);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
decrypt_response	IN	Decrypt operation response.

Return Values

No values returned.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVDecryptResponse *decrypt_response = okvDecryptResponseCreate (env);  
...  
okvDecryptResponseFree (env, &decrypt_response);
```

Related Topics

- [okvCryptoResponseGetDecryptedData](#)
okvCryptoResponseGetDecryptedData gets the decrypted data value from decrypt response structure.
- [okvDecryptResponseCreate](#)
okvDecryptResponseCreate creates the decrypt response structure to hold the decrypt operation response details.

15.24 okvEncryptResponseCreate

okvEncryptResponseCreate creates the encrypt response structure to hold the encrypt operation response details.

Category

KMIP utility API

Purpose

okvEncryptResponseCreate creates the encrypt response structure to hold the encrypt operation response details.

Syntax

```
OKVEncryptResponse *okvEncryptResponseCreate(OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
OKVEncryptResponse *	Pointer to OKVEncryptResponse object. Success: Pointer to OKVEncryptResponse object. Failure: NULL pointer.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVEncryptResponse *encrypt_response = okvEncryptResponseCreate(env);
```

Related Topics

- [okvCryptoResponseGetAuthEncryptionTag](#)
`okvCryptoResponseGetAuthEncryptionTag` gets the authenticated encryption tag value from encrypt response structure.
- [okvCryptoResponseGetEncryptedData](#)
`okvCryptoResponseGetEncryptedData` gets the encrypted data value from encrypt response structure.
- [okvCryptoResponseGetIV](#)
`okvCryptoResponseGetIV` gets the IV value from encrypt response structure used by server for encryption, if the random IV was set and IV was not provided in the request.
- [okvEncryptResponseFree](#)
`okvEncryptResponseFree` frees the memory allocated to encrypt response structure.

15.25 okvEncryptResponseFree

okvEncryptResponseFree frees the memory allocated to encrypt response structure.

Category

KMIP utility API

Purpose

okvEncryptResponseFree frees the memory allocated to encrypt response structure.

Syntax

```
void okvEncryptResponseFree (OKVEnv *env, OKVEncryptResponse** encrypt_response);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
encrypt_response	IN	Encrypt operation response.

Return Values

No values returned.

Supported Versions

Oracle Key Vault C SDK release 21.4.0.0.0 and later.

Comments

None.

Example

```
OKVEncryptResponse *encrypt_response = okvEncryptResponseCreate(env);  
...  
okvEncryptResponseFree(env, &encrypt_response);
```

Related Topics

- [okvCryptoResponseGetAuthEncryptionTag](#)
okvCryptoResponseGetAuthEncryptionTag gets the authenticated encryption tag value from encrypt response structure.
- [okvCryptoResponseGetEncryptedData](#)
okvCryptoResponseGetEncryptedData gets the encrypted data value from encrypt response structure.
- [okvCryptoResponseGetIV](#)
okvCryptoResponseGetIV gets the IV value from encrypt response structure used by server for encryption, if the random IV was set and IV was not provided in the request.

- [okvEncryptResponseCreate](#)
okvEncryptResponseCreate creates the encrypt response structure to hold the encrypt operation response details.

15.26 okvGetTextForAttributeNum

okvGetTextForAttributeNum returns the attribute name for a given Oracle Key Vault attribute number.

Category

KMIP Utility API

Purpose

okvGetTextForAttributeNum returns the attribute name for a given Oracle Key Vault attribute number.

Syntax

```
oratext *okvGetTextForAttributeNum(OKVAttrNo attrno);
```

Parameters

Parameter	IN/OUT	Description
attrno	IN	Oracle Key Vault attribute number of the KMIP attribute.

Return Values

Return Value	Description
oratext*	Name of KMIP attribute. Success: A valid pointer to the name of the KMIP attribute. Failure: A NULL pointer is returned.

Comments

None.

Example

```
printf("%s", okvGetTextForAttributeNum(OKVAttrActivationDate));
```

Related Topics

- [okvGetTextForTag](#)
okvGetTextForTag returns the name of the valid KMIP tag.
- [okvGetTextForTagEnum](#)
okvGetTextForTagEnum returns the name of the enumerated value for a valid KMIP tag of ENUMERATION type.
- [okvGetTextForTagType](#)
okvGetTextForTagType returns the name of the valid KMIP type.

- [okvGetTextLenForAttributeNum](#)
okvGetTextLenForAttributeNum returns the length of the name of the attribute for a given Oracle Key Vault attribute number.

15.27 okvGetTextForTag

okvGetTextForTag returns the name of the valid KMIP tag.

Category

KMIP utility API

Purpose

okvGetTextForTag returns the name of the valid KMIP tag. A NULL value is returned for invalid KMIP tag.

Syntax

```
oratest *okvGetTextForTag(OKVTag tag);
```

Parameters

Parameter	IN/OUT	Description
tag	IN	KMIP tag

Return Values

Return Value	Description
oratest*	KMIP tag name. Success: A valid pointer to the KMIP tag name is returned. Failure: A NULL pointer is returned.

Comments

None.

Example

```
printf("%s", okvGetTextForTag(OKVDEF_TAG_ID));
```

Related Topics

- [okvGetTextForAttributeNum](#)
okvGetTextForAttributeNum returns the attribute name for a given Oracle Key Vault attribute number.
- [okvGetTextForTagEnum](#)
okvGetTextForTagEnum returns the name of the enumerated value for a valid KMIP tag of ENUMERATION type.
- [okvGetTextForTagType](#)
okvGetTextForTagType returns the name of the valid KMIP type.

- [okvGetTextLenForAttributeNum](#)
okvGetTextLenForAttributeNum returns the length of the name of the attribute for a given Oracle Key Vault attribute number.

15.28 okvGetTextForTagEnum

okvGetTextForTagEnum returns the name of the enumerated value for a valid KMIP tag of ENUMERATION type.

Category

KMIP utility API

Purpose

okvGetTextForTagEnum will return the name of the enumerated value for a valid KMIP tag of EMUMERATION type.

Syntax

```
orertext *okvGetTextForTagEnum(OKVTag tag, ub4 val);
```

Parameters

Parameter	IN/OUT	Description
tag	IN	KMIP enum tag
val	IN	KMIP enum tag value

Return Values

Return Value	Description
orertext*	Name of KMIP enum tag value. Success: A valid pointer to the name of the KMIP enum tag value is returned. Failure: A NULL pointer is returned.

Comments

A NULL value is returned for invalid KMIP tag or invalid value of the KMIP tag or if the KMIP tag is not of ENUMERATION type.

Example

```
printf("%s", okvGetTextForTagEnum(OKVDEF_TAG_STATE, OKVDEF_STATE_ACTIVE));
```

Related Topics

- [okvGetTextForAttributeNum](#)
okvGetTextForAttributeNum returns the attribute name for a given Oracle Key Vault attribute number.
- [okvGetTextForTag](#)
okvGetTextForTag returns the name of the valid KMIP tag.

- [okvGetTextForTagType](#)
okvGetTextForTagType returns the name of the valid KMIP type.
- [okvGetTextLenForAttributeNum](#)
okvGetTextLenForAttributeNum returns the length of the name of the attribute for a given Oracle Key Vault attribute number.

15.29 okvGetTextForTagType

okvGetTextForTagType returns the name of the valid KMIP type.

Category

KMIP utility API

Purpose

okvGetTextForTagType returns the name of the valid KMIP type. A NULL value is returned for invalid KMIP type.

Syntax

```
oratest *okvGetTextForTagType (OKVType typ);
```

Parameters

Parameter	IN/OUT	Description
typ	IN	KMIP type

Return Values

Return Value	Description
oratest*	KMIP type name. Success: A valid pointer to the KMIP type name is returned. Failure: A NULL pointer is returned.

Comments

None.

Example

```
printf("%s", okvGetTextForTagType (OKVDEF_ITEM_TYPE_INT));
```

Related Topics

- [okvGetTextForTag](#)
okvGetTextForTag returns the name of the valid KMIP tag.
- [okvGetTextForTagEnum](#)
okvGetTextForTagEnum returns the name of the enumerated value for a valid KMIP tag of ENUMERATION type.

- [okvGetTextForAttributeNum](#)
`okvGetTextForAttributeNum` returns the attribute name for a given Oracle Key Vault attribute number.
- [okvGetTextLenForAttributeNum](#)
`okvGetTextLenForAttributeNum` returns the length of the name of the attribute for a given Oracle Key Vault attribute number.

15.30 okvGetTextLenForAttributeNum

`okvGetTextLenForAttributeNum` returns the length of the name of the attribute for a given Oracle Key Vault attribute number.

Category

KMIP Utility API

Purpose

`okvGetTextLenForAttributeNum` returns the length of the name of the attribute for a given Oracle Key Vault attribute number.

Syntax

```
ub4 okvGetTextLenForAttributeNum(OKVAttrNo attrno);
```

Parameters

Parameter	IN/OUT	Description
attrno	IN	Oracle Key Vault attribute number of the KMIP attribute.

Return Values

Return Value	Description
ub4	Length of the attribute name. Success: Length of the buffer is returned. Failure: 0.

Comments

None.

Example

```
printf("%d", okvGetTextLenForAttributeNum(OKVAttrActivationDate));
```

Related Topics

- [okvGetTextForAttributeNum](#)
`okvGetTextForAttributeNum` returns the attribute name for a given Oracle Key Vault attribute number.
- [okvGetTextForTag](#)
`okvGetTextForTag` returns the name of the valid KMIP tag.

- [okvGetTextForTagEnum](#)
okvGetTextForTagEnum returns the name of the enumerated value for a valid KMIP tag of ENUMERATION type.
- [okvGetTextForTagType](#)
okvGetTextForTagType returns the name of the valid KMIP type.

15.31 okvObjGetAttrNo

okvObjGetAttrNo will return the Oracle Key Vault attribute number for a given TTLV object.

Category

KMIP Utility API

Purpose

okvObjGetAttrNo will return the Oracle Key Vault attribute number for a given TTLV object.

Syntax

```
OKVAttrNo okvObjGetAttrNo(OKVEnv *env, OKVTTLV *ttl);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
ttl	IN	OKVTTLV object.

Return Values

Return Value	Description
OKVAttrNo	Oracle Key Vault attribute number for the TTLV object. Success: Oracle Key Vault attribute number for the given TTLV object is returned. Failure: OKVAttrInvalid is returned.

Comments

None.

Example

```
OKVTTLV *ttl = (OKVTTLV *) NULL;
...
switch (okvObjGetAttrNo(env, ttl))
{
    ...
    case OKVAttrObjType:
        ...
    case OKVAttrCryptoAlg:
        ...
    case OKVAttrCryptoLen:
        ...
}
```

```

    case OKVAttrCryptoUsageMask:
        ...
}

```

15.32 okvCryptoContextSetCryptoAlgo

okvCryptoContextSetCryptoAlgo sets the cryptographic algorithm parameter value in the cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextSetCryptoAlgo sets the cryptographic algorithm parameter value in the cryptographic context structure.

Syntax

```

OKVErrNo okvCryptoContextSetCryptoAlgo(OKVEnv *env,
                                       OKVCryptoContext
                                       *crypto_context,
                                       ub4 crypto_algo);

```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for cryptographic operations.
crypto_algo	IN	Cryptographic algorithm.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
OKVCryptoContext *crypto_context = okvCryptoContextCreate(env, OKVOpSign);
okvCryptoContextSetCryptoAlgo(env, crypto_context, CRYPTO_ALG_RSA);
```

Related Topics

- [okvCryptoContextGetCryptoAlgo](#)
okvCryptoContextGetCryptoAlgo gets the cryptographic algorithm parameter value from cryptographic context structure.

15.33 okvCryptoContextSetHashingAlgo

okvCryptoContextSetHashingAlgo sets the hashing algorithm parameter value in the cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextSetHashingAlgo sets the hashing algorithm parameter value in the cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextSetHashingAlgo(OKVEnv *env,
                                         OKVCryptoContext *crypto_context,
                                         ub4 hashing_algo);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for cryptographic operations.
hashing_algo	IN	Hashing algorithm.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
OKVCryptoContext *crypto_context =
okvCryptoContextCreate (env, OKVOpSign);
okvCryptoContextSetHashingAlgo (env, crypto_context, HASH_ALG_SHA_256);
```

Related Topics

- [okvCryptoContextGetHashingAlgo](#)
okvCryptoContextGetHashingAlgo gets the hashing algorithm parameter value in the cryptographic context structure.

15.34 okvCryptoContextSetDigitalSignAlgo

okvCryptoContextSetDigitalSignAlgo sets the digital signature algorithm parameter value in the cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextSetDigitalSignAlgo sets the digital signature algorithm parameter value in the cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextSetDigitalSignAlgo (OKVEnv *env,
                                             OKVCryptoContext *crypto_context,
                                             ub4 digital_sign_algo);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for cryptographic operations.
digital_sign_algo	IN	Digital signature algorithm.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
OKVCryptoContext *crypto_context = okvCryptoContextCreate(env, OKVOpSign);
okvCryptoContextSetDigitalSignAlgo(env, crypto_context,
SIGN_ALG_SHA256_W_RSA);
```

Related Topics

- [okvCryptoContextGetDigitalSignAlgo](#)
`okvCryptoContextGetDigitalSignAlgo` gets the digital signature algorithm parameter value from cryptographic context structure.

15.35 okvCryptoContextGetCryptoAlgo

`okvCryptoContextGetCryptoAlgo` gets the cryptographic algorithm parameter value from cryptographic context structure.

Category

KMIP utility API

Purpose

`okvCryptoContextGetCryptoAlgo` gets the cryptographic algorithm parameter value from cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextGetCryptoAlgo(OKVEnv *env,
                                        OKVCryptoContext *crypto_context,
                                        ub4 *crypto_algo);
```


Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for cryptographic operations.
crypto_algo	OUT	Cryptographic algorithm.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
ub4 crypto_algo;
okvCryptoContextGetCryptoAlgo(env, crypto_context, &crypto_algo);
```

Related Topics

- [okvCryptoContextSetCryptoAlgo](#)
okvCryptoContextSetCryptoAlgo sets the cryptographic algorithm parameter value in the cryptographic context structure.

15.36 okvCryptoContextGetHashingAlgo

okvCryptoContextGetHashingAlgo gets the hashing algorithm parameter value in the cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextGetHashingAlgo gets the hashing algorithm parameter value in the cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextGetHashingAlgo(OKVEnv *env,
                                         OKVCryptoContext *crypto_context,
                                         ub4 *hashing_algo);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for cryptographic operations.
hashing_algo	OUT	Hashing algorithm.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
ub4 hashing_algo;
okvCryptoContextGetHashingAlgo(env, crypto_context, &hashing_algo);
```

Related Topics

- [okvCryptoContextSetHashingAlgo](#)
okvCryptoContextSetHashingAlgo sets the hashing algorithm parameter value in the cryptographic context structure.

15.37 okvCryptoContextGetDigitalSignAlgo

okvCryptoContextGetDigitalSignAlgo gets the digital signature algorithm parameter value from cryptographic context structure.

Category

KMIP utility API

Purpose

okvCryptoContextGetDigitalSignAlgo gets the digital signature algorithm parameter value from cryptographic context structure.

Syntax

```
OKVErrNo okvCryptoContextGetDigitalSignAlgo (OKVEnv *env,  
                                             OKVCryptoContext *crypto_context,  
                                             ub4 *digital_sign_algo);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
crypto_context	IN	Cryptographic context contains required parameters for cryptographic operations.
digital_sign_algo	OUT	Digital signature algorithm

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
ub4 digital_sign_algo;  
okvCryptoContextGetDigitalSignAlgo(env, crypto_context,  
&digital_sign_algo);
```

Related Topics

- [okvCryptoContextSetDigitalSignAlgo](#)
okvCryptoContextSetDigitalSignAlgo sets the digital signature algorithm parameter value in the cryptographic context structure.

15.38 okvCryptoResponseGetSignatureData

okvCryptoResponseGetSignatureData gets the signature data value from the sign response structure.

Category

KMIP utility API

Purpose

okvCryptoResponseGetSignatureData gets the signature data value from the sign response structure.

Syntax

```
OKVErrNo okvCryptoResponseGetSignatureData (OKVEnv *env,
                                             OKVSignResponse *sign_response,
                                             ub1 *signature_data,
                                             ub4 *signature_datal);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle
sign_response	IN	Sign operation response.
signature_data	OUT	Signature data value.
signature_datal	OUT	Signature data value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
ub1 signature_data[OKV_OBJECT_MAXLEN];
ub4 signature_datal = sizeof(signature_data);
...
/* Perform Sign operation and get sign operation response in 'sign_response'
```

```

*/
...
memset(signature_data, 0, signature_datal);
okvCryptoResponseGetSignatureData(env, sign_response, signature_data,
&signature_datal);

```

Related Topics

- [okvSign](#)
okvSign implements the KMIP Sign operation.
- [okvSignResponseCreate](#)
okvSignResponseCreate creates the sign response structure to hold the sign operation response details.
- [okvSignResponseFree](#)
okvSignResponseFree frees the memory allocated to the sign response structure.

15.39 okvCryptoResponseGetRecoveredData

okvCryptoResponseGetRecoveredData gets the recovered data value from the signature verify response structure.

Category

KMIP utility API

Purpose

okvCryptoResponseGetRecoveredData gets the recovered data value from the signature verify response structure.

Syntax

```

OKVErrNo okvCryptoResponseGetRecoveredData (OKVEnv *env,
                                             OKVSignVerifyResponse
*sign_verify_response,
                                             ub1 *recovered_data,
                                             ub4 *recovered_datal);

```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle
sign_verify_response	IN	Signature verify operation response.
recovered_data	OUT	Recovered data value.
recovered_datal	OUT	Recovered data value length.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) Failure: A valid error number is returned for the error on top of the error stack.

Comments

Returning recovered data is not currently supported by Oracle Key Vault.

15.40 okvCryptoResponseGetValidity

`okvCryptoResponseGetValidity` gets the validity value from the signature verify response structure.

Category

KMIP utility API

Purpose

`okvCryptoResponseGetValidity` gets the validity value from the signature verify response structure.

Syntax

```
OKVErrNo okvCryptoResponseGetValidity(OKVEnv *env,
                                       OKVSignVerifyResponse *sign_verify_response,
                                       ub4 *validity);
```

Parameters

Parameter	IN/OUT	Description
<code>env</code>	IN	Oracle Key Vault environment handle.
<code>sign_verify_response</code>	IN	Signature verify operation response.
<code>validity</code>	OUT	Validity value.

Return Values

Return Value	Description
OKVErrNo	Oracle Key Vault error number. Success: OKV_SUCCESS (0) Failure: A valid error number is returned for the error on top of the error stack.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
ub4 validity;
...
/* Perform Signature Verify operation and get signature verify
operation response in 'sign_verify_response' */
...
okvCryptoResponseGetValidity(env, sign_verify_response, &validity);
```

Related Topics

- [okvSignVerify](#)
okvSignVerify implements the KMIP Signature Verify operation.
- [okvSignVerifyResponseCreate](#)
okvSignVerifyResponseCreate creates the signature verify response structure to hold the signature verify operation response details.
- [okvSignVerifyResponseFree](#)
okvSignVerifyResponseFree frees the memory allocated to the signature verify response structure.

15.41 okvSignResponseCreate

okvSignResponseCreate creates the sign response structure to hold the sign operation response details.

Category

KMIP utility API

Purpose

okvSignResponseCreate creates the sign response structure to hold the sign operation response details.

Syntax

```
OKVSignResponse *okvSignResponseCreate(OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
OKVSignResponse*	Pointer to OKVSignResponse object. Success: Pointer to OKVSignResponse object. Failure: NULL pointer.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
OKVSignResponse *sign_response = okvSignResponseCreate(env);
```

Related Topics

- [okvSignResponseFree](#)
okvSignResponseFree frees the memory allocated to the sign response structure.

15.42 okvSignResponseFree

okvSignResponseFree frees the memory allocated to the sign response structure.

Category

KMIP utility API

Purpose

okvSignResponseFree frees the memory allocated to the sign response structure.

Syntax

```
void okvSignResponseFree(OKVEnv *env, OKVSignResponse **sign_response);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
sign_response	IN	Signature operation response.

Return Values

No value returned.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
OKVSignResponse *sign_response = okvSignResponseCreate(env);
...
okvSignResponseFree(env, &sign_response);
```

Related Topics

- [okvSignResponseCreate](#)
okvSignResponseCreate creates the sign response structure to hold the sign operation response details.

15.43 okvSignVerifyResponseCreate

okvSignVerifyResponseCreate creates the signature verify response structure to hold the signature verify operation response details.

Category

KMIP utility API

Purpose

okvSignVerifyResponseCreate creates the signature verify response structure to hold the signature verify operation response details.

Syntax

```
OKVSignVerifyResponse *okvSignVerifyResponseCreate(OKVEnv *env);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.

Return Values

Return Value	Description
OKVSignVerifyResponse *	Pointer to OKVSignVerifyResponse object. Success: Pointer to OKVSignVerifyResponse object. Failure: NULL pointer.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
OKVSignVerifyResponse *sign_verify_response =
okvSignVerifyResponseCreate(env);
```

Related Topics

- [okvSignVerifyResponseFree](#)
okvSignVerifyResponseFree frees the memory allocated to the signature verify response structure.

15.44 okvSignVerifyResponseFree

okvSignVerifyResponseFree frees the memory allocated to the signature verify response structure.

Category

KMIP utility API

Purpose

okvSignVerifyResponseFree frees the memory allocated to the signature verify response structure.

Syntax

```
void okvSignVerifyResponseFree(OKVEnv *env,
                              OKVSignVerifyResponse **sign_verify_response);
```

Parameters

Parameter	IN/OUT	Description
env	IN	Oracle Key Vault environment handle.
sign_verify_response	IN	Signature verify operation response.

Return Values

No value returned.

Supported Versions

Oracle Key Vault C SDK release 21.6.0.0.0 and later.

Comments

None.

Example

```
OKVSignVerifyResponse *sign_verify_response =  
okvSignVerifyResponseCreate(env);  
...  
okvSignVerifyResponseFree(env, &sign_verify_response);
```

Related Topics

- [okvSignVerifyResponseCreate](#)
okvSignVerifyResponseCreate creates the signature verify response structure to hold the signature verify operation response details.

Part III

Oracle Key Vault Client Java SDK API Reference

Part III provides information about the Oracle Key Vault Java SDK packages and its APIs.

- [Oracle Key Vault Java SDK Packages](#)
The Oracle Key Vault Java SDK provides five packages.
- [Oracle Key Vault Java SDK APIs](#)
The Oracle Key Vault Java SDK provides APIs similar to C SDK APIs.

16

Oracle Key Vault Java SDK Packages

The Oracle Key Vault Java SDK provides five packages.

Table 16-1 Oracle Key Vault Java SDK Packages

Package	Description
<code>oracle.okv.exception</code>	This package contains all the exceptions thrown by the Java SDK Oracle Key Vault interface.
<code>oracle.okv.kmip</code>	This package contains <code>enum</code> class for KMIP tags, tag enumerations, and types.
<code>oracle.okv.operation</code>	This package contains the <code>OKVBatchOperation</code> class through which KMIP operations can be batched.
<code>oracle.okv.response</code>	This package contains all the response classes whose objects are the return values of various high-level Oracle Key Vault Java SDK APIs.
<code>oracle.okv.service</code>	This package contains the <code>OKVService</code> class through which all the high level Java SDK APIs are exposed.

- [oracle.okv.exception Java Package](#)
The `oracle.okv.exception` package contains all the exceptions thrown by the Java SDK Oracle Key Vault interface.
- [oracle.okv.kmip Java Package](#)
The `oracle.okv.kmip` package contains `enum` class for KMIP tags, tag enumerations, and types.
- [oracle.okv.operation Java Package](#)
The `oracle.okv.operation` package contains the `OKVBatchOperation` class.
- [oracle.okv.response Java Package](#)
The `oracle.okv.response` package contains all the response classes whose objects are the return values of various high-level Oracle Key Vault Java SDK APIs.
- [oracle.okv.service Java Package](#)
The `oracle.okv.service` package contains the `OKVService` class through which all the high level Java SDK APIs are exposed.

16.1 oracle.okv.exception Java Package

The `oracle.okv.exception` package contains all the exceptions thrown by the Java SDK Oracle Key Vault interface.

Exceptions

- [OKVAppNamespaceNotSuppException](#)
- [OKVAuthNotSuccessfulException](#)

- OKVBatchResponseException
- OKVConfigurationException
- OKVConnectionException
- OKVCryptographicFailureException
- OKVEncodingOptionException
- OKVEndpointUpdatesNotSuccessfulException
- OKVException
- OKVFeatureNotSuppException
- OKVGeneralFailureException
- OKVIllegalOperationException
- OKVIndexOutOfBoundsException
- OKVInsufficientGrpPrivException
- OKVInvalidArgumentException
- OKVInvalidAttrValueException
- OKVInvalidFieldException
- OKVInvalidGroupException
- OKVInvalidMessageException
- OKVInvalidTTLVException
- OKVItemNotFoundException
- OKVKeyCompressionTypeNotSuppException
- OKVKeyFormatTypeNotSuppException
- OKVMissingDataException
- OKVNoReasonException
- OKVNotExtractableException
- OKVObjectArchivedException
- OKVOperationCancelledException
- OKVOperationNotSuppException
- OKVPermissionDeniedException
- OKVResponseException
- OKVResponseTooLargeException
- OKVRestrictedModeException
- OKVWrongObjectTypeException

16.2 oracle.okv.kmip Java Package

The `oracle.okv.kmip` package contains `enum` class for KMIP tags, tag enumerations, and types.

Interfaces

- [OKVPrimitiveConnection](#)

Classes

- [OKVConnection](#)
- [OKVCryptoContext](#)
- [OKVSSLConnection](#)
- [OKVTTLV](#)

Enums

- [DataType](#)
- [OKVTag](#)
- [OKVTagEnum](#)
- [OKVType](#)

16.3 oracle.okv.operation Java Package

The `oracle.okv.operation` package contains the `OKVBatchOperation` class.

Classes

- [OKVBatchOperation](#)

16.4 oracle.okv.response Java Package

The `oracle.okv.response` package contains all the response classes whose objects are the return values of various high-level Oracle Key Vault Java SDK APIs.

Interfaces

- [OKVAppSpecificInfo](#)
- [OKVAttribute](#)
- [OKVAttrListResponse](#)
- [OKVAttrsResponse](#)
- [OKVBatchResponse](#)
- [OKVCertificateRequestResponse](#)
- [OKVCertificateResponse](#)
- [OKVCryptoDomainParams](#)
- [OKVCryptoParams](#)
- [OKVCryptoResponse](#)
- [OKVDecryptResponse](#)
- [OKVDigest](#)
- [OKVEncryptResponse](#)
- [OKVKeyPairUidResponse](#)
- [OKVKeyResponse](#)

- [OKVLink](#)
- [OKVName](#)
- [OKVOpaqueDataResponse](#)
- [OKVPrivateKeyResponse](#)
- [OKVPublicKeyResponse](#)
- [OKVQueryResponse](#)
- [OKVResponse](#)
- [OKVRevocationReason](#)
- [OKVSecretDataResponse](#)
- [OKVSignResponse](#)
- [OKVSignVerifyResponse](#)
- [OKVTemplateResponse](#)
- [OKVUidListResponse](#)
- [OKVUidResponse](#)
- [OKVUsageLimits](#)
- [OKVX509CertId](#)

Classes

- [OKVServerInformation](#)

16.5 oracle.okv.service Java Package

The `oracle.okv.service` package contains the `OKVService` class through which all the high level Java SDK APIs are exposed.

Interfaces

- [OKVTransporter](#)

Classes

- [OKVService](#)
- [OKVTransporterImpl](#)

Oracle Key Vault Java SDK APIs

The Oracle Key Vault Java SDK provides APIs similar to C SDK APIs.

- [Java SDK Management APIs](#)
This section describes the interfaces for Oracle Key Vault program environment.
- [Java SDK Connection Management APIs](#)
This section describes the interfaces for Oracle Key Vault connection management.
- [Java SDK KMIP APIs](#)
The Java SDK KMIP APIs provide functions for creating keys, activating keys, adding attributes to keys, destroying keys, and other operations.
- [Java SDK KMIP Batch APIs](#)
This section describes the interfaces for the Oracle Key Vault KMIP Batch functions.
- [Java SDK KMIP Attribute APIs](#)
This section describes the interfaces that help create and interpret Oracle Key Vault KMIP attributes.
- [Java SDK KMIP Custom Attribute APIs](#)
This section describes the interfaces that help create and interpret Oracle Key Vault KMIP custom attributes.
- [Java SDK Extension Operation Management APIs](#)
This section describes the interfaces for Oracle Key Vault operations used to execute custom KMIP requests.
- [Java SDK TTLV Object APIs](#)
This section describes the interfaces for Oracle Key Vault KMIP parser/builder.
- [Java SDK Utility APIs](#)
The Java SDK Utility API provides a function for creating the cryptographic context.

17.1 Java SDK Management APIs

This section describes the interfaces for Oracle Key Vault program environment.

Management APIs

- [okvEnvGetOpRequestObj](#)
- [okvEnvSetConfig](#)

17.2 Java SDK Connection Management APIs

This section describes the interfaces for Oracle Key Vault connection management.

Connection Management APIs

- [okvConnect](#)
- [okvConnSendRecvBytes](#)

- [okvDisconnect](#)

17.3 Java SDK KMIP APIs

The Java SDK KMIP APIs provide functions for creating keys, activating keys, adding attributes to keys, destroying keys, and other operations.

KMIP APIs

- [okvActivate](#)
- [okvAddAttribute](#)
- [okvCreateKey](#)
- [okvCreateKeyPair](#)
- [okvDecrypt](#)
- [okvDeleteAttribute](#)
- [okvDestroy](#)
- [okvEncrypt](#)
- [okvGetAttributeList](#)
- [okvGetAttributes](#)
- [okvGetCertificate](#)
- [okvGetCertificateRequest](#)
- [okvGetKey](#)
- [okvGetOpaqueData](#)
- [okvGetPrivateKey](#)
- [okvGetPublicKey](#)
- [okvGetSecretData](#)
- [okvGetTemplate](#)
- [okvLocate](#)
- [okvModifyAttribute](#)
- [okvQueryCapability](#)
- [okvRegCertificate](#)
- [okvRegCertificateRequest](#)
- [okvRegKey](#)
- [okvRekey](#)
- [okvRegOpaqueData](#)
- [okvRegPrivateKey](#)
- [okvRegPublicKey](#)
- [okvRevoke](#)
- [okvRegSecretData](#)
- [okvRegTemplate](#)

- [okvSign](#)
- [okvSignVerify](#)

17.4 Java SDK KMIP Batch APIs

This section describes the interfaces for the Oracle Key Vault KMIP Batch functions.

KMIP Batch APIs

- [okvActivate](#)
- [okvAddAttribute](#)
- [okvBatchExecute](#)
- [okvCreateKey](#)
- [okvCreateKeyPair](#)
- [okvDecrypt](#)
- [okvDeleteAttribute](#)
- [okvDestroy](#)
- [okvEncrypt](#)
- [okvGetAttributeList](#)
- [okvGetAttributes](#)
- [okvGetCertificate](#)
- [okvGetCertificateRequest](#)
- [okvGetKey](#)
- [okvGetOpaqueData](#)
- [okvGetPrivateKey](#)
- [okvGetPublicKey](#)
- [okvGetSecretData](#)
- [okvGetTemplate](#)
- [okvLocate](#)
- [okvModifyAttribute](#)
- [okvQueryCapability](#)
- [okvRegCertificate](#)
- [okvRegCertificateRequest](#)
- [okvRegKey](#)
- [okvRegOpaqueData](#)
- [okvRegPrivateKey](#)
- [okvRegPublicKey](#)
- [okvRegSecretData](#)
- [okvRegTemplate](#)

- [okvRekey](#)
- [okvRevoke](#)
- [okvSign](#)
- [okvSignVerify](#)

17.5 Java SDK KMIP Attribute APIs

This section describes the interfaces that help create and interpret Oracle Key Vault KMIP attributes.

KMIP Attribute APIs

- [okvAddAttributeObject](#)
- [okvAttrAddActivationDate](#)
- [okvAttrAddArchiveDate](#)
- [okvAttrAddCertLen](#)
- [okvAttrAddCertType](#)
- [okvAttrAddCompromiseDate](#)
- [okvAttrAddCompromiseOccurrenceDate](#)
- [okvAttrAddContactInfo](#)
- [okvAttrAddCryptoAlgo](#)
- [okvAttrAddCryptoLen](#)
- [okvAttrAddCryptoParams](#)
- [okvAttrAddCryptoUsageMask](#)
- [okvAttrAddDeactivationDate](#)
- [okvAttrAddDestroyDate](#)
- [okvAttrAddDigest](#)
- [okvAttrAddDigitalSignAlgo](#)
- [okvAttrAddExtractable](#)
- [okvAttrAddFresh](#)
- [okvAttrAddInitialDate](#)
- [okvAttrAddLastChangeDate](#)
- [okvAttrAddLeaseTime](#)
- [okvAttrAddName](#)
- [okvAttrAddNeverExtractable](#)
- [okvAttrAddObjectGroup](#)
- [okvAttrAddObjectType](#)
- [okvAttrAddProcessStartDate](#)
- [okvAttrAddProtectStopDate](#)
- [okvAttrAddRevocationReason](#)

- `okvAttrAddState`
- `okvAttrAddUniqueID`
- `okvAttrAddUsageLimits`
- `okvAttrAddX509CertId`
- `okvAttrAddX509CertIss`
- `okvAttrAddX509CertIssAltName`
- `okvAttrAddX509CertSubj`
- `okvAttrAddX509CertSubjAltName`
- `okvAttrGetActivationDate`
- `okvAttrGetArchiveDate`
- `okvAttrGetCertLen`
- `okvAttrGetCertType`
- `okvAttrGetCompromiseDate`
- `okvAttrGetCompromiseOccurrenceDate`
- `okvAttrGetContactInfo`
- `okvAttrGetCryptoAlgo`
- `okvAttrGetCryptoLen`
- `okvAttrGetCryptoParams`
- `okvAttrGetCryptoUsageMask`
- `okvAttrGetDeactivationDate`
- `okvAttrGetDestroyDate`
- `okvAttrGetDigest`
- `okvAttrGetDigitalSignAlgo`
- `okvAttrGetExtractable`
- `okvAttrGetFresh`
- `okvAttrGetInitialDate`
- `okvAttrGetLastChangeDate`
- `okvAttrGetLeaseTime`
- `okvAttrGetName`
- `okvAttrGetNeverExtractable`
- `okvAttrGetObjectGroup`
- `okvAttrGetObjectType`
- `okvAttrGetProcessStartDate`
- `okvAttrGetProtectStopDate`
- `okvAttrGetRevocationReason`
- `okvAttrGetState`
- `okvAttrGetUniqueID`

- [okvAttrGetUsageLimits](#)
- [okvAttrGetX509CertId](#)
- [okvAttrGetX509CertIss](#)
- [okvAttrGetX509CertIssAltName](#)
- [okvAttrGetX509CertSubj](#)
- [okvAttrGetX509CertSubjAltName](#)
- [okvGetAttributeObject](#)

17.6 Java SDK KMIP Custom Attribute APIs

This section describes the interfaces that help create and interpret Oracle Key Vault KMIP custom attributes.



Note:

Do not use the prefix of `x-OKV` with custom attribute names. The custom attributes that start with the `x-OKV` prefix are reserved for use by Oracle Key Vault only.

KMIP Custom Attribute APIs

- [okvCustomAttrAddBoolean](#)
- [okvCustomAttrAddByteString](#)
- [okvCustomAttrAddBigInteger](#)
- [okvCustomAttrAddDateTime](#)
- [okvCustomAttrAddEnum](#)
- [okvCustomAttrAddInteger](#)
- [okvCustomAttrAddInterval](#)
- [okvCustomAttrAddLongInteger](#)
- [okvCustomAttrAddStructure](#)
- [okvCustomAttrAddTextString](#)
- [okvCustomAttrGetBigInteger](#)
- [okvCustomAttrGetBoolean](#)
- [okvCustomAttrGetByName](#)
- [okvCustomAttrGetByteString](#)
- [okvCustomAttrGetByType](#)
- [okvCustomAttrGetDateTime](#)
- [okvCustomAttrGetEnum](#)
- [okvCustomAttrGetInteger](#)
- [okvCustomAttrGetInterval](#)

- [okvCustomAttrGetLongInteger](#)
- [okvCustomAttrGetStructure](#)
- [okvCustomAttrGetTextString](#)

17.7 Java SDK Extension Operation Management APIs

This section describes the interfaces for Oracle Key Vault operations used to execute custom KMIP requests.

Extension Operation Management APIs

- [okvOpsExecuteOp](#)

17.8 Java SDK TTLV Object APIs

This section describes the interfaces for Oracle Key Vault KMIP parser/builder.

KMIP Extension TTLV Object APIs

- [okvTTLVGetChild](#)
- [okvTTLVGetChildByTag](#)
- [okvTTLVGetFirstChildByTag](#)
- [okvTTLVGetLen](#)
- [okvTTLVGetTag](#)
- [okvTTLVGetType](#)
- [okvTTLVGetValue](#)

17.9 Java SDK Utility APIs

The Java SDK Utility API provides a function for creating the cryptographic context.

Utility APIs

- [okvCryptoContextCreate](#)

Part IV

Oracle Key Vault Client SDK Troubleshooting

Part VII describes troubleshooting issues with using the Oracle Key Vault Client SDK.

- [Troubleshooting](#)
Oracle Key Vault SDK programs can be debugged using the tracing infrastructure which is included as a part of Oracle Key Vault SDK deliverable.

Troubleshooting

Oracle Key Vault SDK programs can be debugged using the tracing infrastructure which is included as a part of Oracle Key Vault SDK deliverable.

Refer the content below for using the tracing infrastructure for C SDK and Java SDK programs.

- **C SDK Tracing:** Before turning on the tracing, identify the version of C SDK software being used on your system as shown below. If you have deployed C SDK under \$OKV_HOME, then execute the following commands:

```
cd $OKV_HOME/csdk/lib
strings libokvcsdk.so | grep "Oracle Key Vault C SDK Version"
```

The Oracle Key Vault C SDK supports an extensive tracing infrastructure in order to debug errors encountered during execution of a C SDK endpoint program. The tracing can be enabled for a C SDK program using the `okvEnvSetTrace` API. The Oracle Key Vault C SDK supports different trace levels to filter trace messages generated for a C SDK endpoint program. Refer to section [okvEnvSetTrace](#) to find information on various trace levels and refer the example in same section to enable tracing for a C SDK endpoint program. The trace files can be found in the location provided as input to `okvEnvSetTrace` API call. The trace files have the format

```
okv_csdk_<Process_ID_of_CSDK_Program>.trc.
```

- **Java SDK Tracing:** Before turning on the tracing, identify the version of Java SDK software being used on your system as shown below. If you have deployed Java SDK under \$OKV_HOME, then execute the following commands:

```
cd $OKV_HOME/jsdk/lib
unzip -p okvjsdk.jar | strings | grep "Oracle Key Vault Java SDK Version"
```

Tracing for the Oracle Key Vault Java SDK is supported at the standard `java.util.logging` trace levels: OFF, SEVERE, WARNING, INFO, FINE, FINER, and ALL. Tracing can be turned on by setting the trace level in configuration file `logging.properties`. This configuration file is provided as part of the Oracle Key Vault Java SDK deliverable. Please make sure to turn on the global trace level `.level` and `java.util.logging.FileHandler.level` in the configuration file so that the Java SDK traces are generated in a file. Also you may change the directory in which you want the trace file to be generated by editing the property `java.util.logging.FileHandler.pattern` in the configuration file.

For more information on trace levels, refer to <https://docs.oracle.com/javase/7/docs/api/java/util/logging/Level.html>. For more information on `java.util.logging` FileHandler, refer to <https://docs.oracle.com/javase/7/docs/api/java/util/logging/FileHandler.html>.

Provide the SDK version information and the trace logs when raising SDK issues to support team. Note that no sensitive information is written to a trace file during program execution.

Related Topics

- [okvEnvSetTrace](#)
`okvEnvSetTrace` sets up the Oracle Key Vault trace configuration context.

Index

A

algorithm

- digital signature algorithm, getting with
okvAttrGetDigitalSignAlgo, [12-65](#)

attribute index

- about, [12-7](#)

attribute objects

- about, [12-6](#)
- adding archive date with
okvAttrAddArchiveDate, [12-8](#)
- adding certificate length with
okvAttrAddCertLen, [12-11](#)
- adding certificate type with
okvAttrAddCertType, [12-13](#)
- adding digital signature algorithm with
okvAttrAddDigitalSignAlgo, [12-24](#)
- adding extractable attribute with
okvAttrAddExtractable, [12-25](#)
- adding initial date with okvAttrAddInitialDate,
[12-27](#)
- adding last change date with
okvAttrAddLastChangeDate, [12-28](#)
- adding state with okvAttrAddState, [12-38](#)
- adding with okvAddAttributeObject, [12-9](#)
- adding X509 certificate ID with
okvAttrAddX509CertId, [12-41](#)
- adding X509 certificate issuer alternate name
with
okvAttrAddX509CertIssAltName,
[12-44](#)
- adding X509 certificate issuer with
okvAttrAddX509CertIss, [12-42](#)
- adding X509 certificate subject alternate
name with
okvAttrAddX509CertSubjAltName,
[12-47](#)
- adding X509 certificate subject with
okvAttrAddX509CertSubj, [12-45](#)
- decrypt operation response details with
OKVDecryptResponse, [6-7](#)
- defining KMIP attributes with OKVATTRMAX
using OKVAttrNo, [6-5](#)
- defining KMIP attributes with OKVOBJMAX
using OKVObjNo, [6-11](#)

attribute objects (*continued*)

- defining KMIP attributes with OKVOPSMAX
using OKVOpsNo, [6-12](#)
 - encrypt operation response details with
OKVEncryptResponse, [6-7](#)
 - parameters with OKVCryptoContext, [6-6](#)
 - text string data type, getting with
okvCustomAttrGetTextString, [12-138](#)
 - TTLV structure data type, getting with
okvCustomAttrGetStructure, [12-136](#)
- ### attribute objects, custom
- about, [12-104](#)
 - Boolean data type, adding with
okvCustomAttrAddBoolean, [12-107](#)
 - Boolean data type, getting with
okvCustomAttrGetBoolean, [12-122](#)
 - byte string data type length, getting with
okvCustomAttrGetByteStringLen,
[12-127](#)
 - byte string data type, adding with
okvCustomAttrAddByteString,
[12-108](#)
 - byte string data type, getting with
okvCustomAttrGetByteString, [12-125](#)
 - custom attribute with name, getting with
okvCustomAttrGetByName, [12-124](#)
 - custom attribute, getting with
okvCustomAttrGetType, [12-128](#)
 - custom attributes, getting with
okvCustomAttrGet, [12-118](#)
 - date time data type, adding with
okvCustomAttrAddDateTime, [12-109](#)
 - date time data type, getting with
okvCustomAttrGetDateTime, [12-129](#)
 - enumeration data type, adding with
okvCustomAttrAddEnum, [12-111](#)
 - enumeration data type, getting with
okvCustomAttrGetEnum, [12-130](#)
 - integer data type, adding with
okvCustomAttrAddInteger, [12-112](#)
 - interval data type, adding with
okvCustomAttrAddInterval, [12-113](#)
 - interval data type, getting with
okvCustomAttrGetInterval, [12-133](#)

attribute objects, custom (*continued*)

- long integer data type, adding with `okvCustomAttrAddLongInteger`, [12-114](#)
- long integer data type, getting with `okvCustomAttrGetLongInteger`, [12-135](#)
- text string data type length, getting with `okvCustomAttrGetTextStringLen`, [12-139](#)
- text string data type, adding with `okvCustomAttrAddTextString`, [12-117](#)
- TTLV structure, adding with `okvCustomAttrAddStructure`, [12-115](#)

B

batch operations

- ending with `okvBatchFree`, [11-98](#)
- executing with `okvBatchExecute`, [11-97](#)
- getting counts of batch operations with `okvGetBatchOperationCount`, [11-100](#)
- getting name of batch job number with `okvGetBatchOperationName`, [11-101](#)
- start of with `okvBatchCreate`, [11-96](#)

C

certificate

- request object, [11-59](#)

client SDK KMIP APIs

- about, [11-3](#)

connections

- creating with `OKIConnConnec`, [8-1](#)
- KMIP response messaging with `okvConnSendRecvBytes`, [8-3](#)
- KMIP response messaging with `okvConnSet`, [8-4](#)
- KMIP response messaging with `okvConnUnSet`, [8-6](#)
- OKI types, [5-9](#)
- removing with `okvDisconnect`, [8-7](#)
- SSL connection wallet, password, [7-7](#)

contact information

- adding with `okvAttrAddContactInfo`, [12-16](#)
- getting with `okvAttrGetContactInfo`, [12-54](#)
- length, getting with `okvAttrGetContactInfoLen`, [12-55](#)

cryptographic

- algorithm, adding with `okvAttrAddCryptoAlgo`, [12-17](#)
- algorithm, getting with `okvAttrGetCryptoAlgo`, [12-56](#)
- length, adding with `okvAttrAddCryptoLen`, [12-18](#)

cryptographic (*continued*)

- length, getting with `okvAttrGetCryptoLen`, [12-58](#)
- parameters, adding with `okvAttrAddCryptoParams`, [12-19](#)
- parameters, getting with `okvAttrGetCryptoParams`, [12-59](#)
- usage mask, adding with `okvAttrAddCryptoUsageMask`, [12-20](#)
- usage mask, getting with `okvAttrGetCryptoUsageMask`, [12-60](#)

D

data, opaque

- getting with `okvGetOpaqueData`, [11-34](#)
- registering with `okvRegOpaqueData`, [11-63](#)

data, secret

- getting with `okvGetSecretData`, [11-43](#)
- registering with `okvRegSecretData`, [11-76](#)

dates

- activation date, getting with `okvAttrGetActivationDate`, [12-48](#)
- adding activation date attribute with `okvAttrAddActivationDate`, [12-10](#)
- adding initial with `okvCreateKeyPair`, [11-92](#)
- adding initial with `okvSign`, [11-86](#)
- adding initial with `okvSignatureVerify`, [11-89](#)
- adding initial with `OKVSignResponse`, [6-14](#)
- adding initial with `OKVSignVerifyResponse`, [6-14](#)
- archive date, getting with `okvAttrGetArchiveDate`, [12-49](#)
- compromise date, adding with `okvAttrAddCompromiseDate`, [12-14](#)
- compromise date, getting with `okvAttrGetCompromiseDate`, [12-52](#)
- compromise occurrence date, adding with `okvAttrAddCompromiseOccurrenceDate`, [12-15](#)
- compromise occurrence date, getting with `okvAttrGetCompromiseOccurrenceDate`, [12-53](#)
- deactivation date, adding with `okvAttrAddDeactivationDate`, [12-21](#)
- deactivation date, getting with `okvAttrGetDeactivationDate`, [12-61](#)
- destroy date, adding with `okvAttrAddDestroyDate`, [12-22](#)
- destroy date, getting with `okvAttrGetDestroyDate`, [12-62](#)
- initial, getting with `okvAttrGetInitialDate`, [12-68](#)
- last change, with with `okvAttrGetLastChangeDate`, [12-69](#)
- `okvCustomAttrAddDateTime`, [12-109](#)
- `okvCustomAttrGetDateTime`, [12-129](#)

dates (*continued*)

- process start date, adding with
 - okvAttrAddProcessStartDate, [12-35](#)
- process start date, getting with
 - okvAttrGetProcessStartDate, [12-78](#)
- process stop date, getting with
 - okvAttrGetProtectStopDate, [12-79](#)
- protect stop date, adding with
 - okvAttrAddProtectStopDate, [12-36](#)

digest

- adding with okvAttrAddDigest, [12-23](#)
- digest attribute, getting with
 - okvAttrGetDigest, [12-63](#)
- length, getting with okvAttrGetDigestLen, [12-64](#)

downloading SDK software, [4-1](#)

E

element index

- about, [12-7](#)

ending Oracle Key Vault Interface environment,

- okvEnvFree, [7-3](#)

endpoints

- SDK program behavior, OKVEnv, [6-8](#)
- SDK program behavior, okvEnvCreate, [7-1](#)

error handling

- capturing errors with OKVErr, [6-9](#)
- depth of error stack for batch job with
 - okvErrGetDepthForBatch, [10-3](#)
- depth of error stack with okvErrGetDepth, [10-1](#)
- error at depth with okvErrGetNumAtDepth, [10-6](#)
- error number at specified depth of error stack with
 - okvErrGetNumAtDepthForBatch, [10-7](#)
- error number for batch with
 - okvErrGetNumForBatch, [10-9](#)
- get error number with okvErrGetNum, [10-4](#)
- reset error stack with okvErrReset, [10-11](#)
- text of error with okvGetTextForErrNum, [10-12](#)

extractable

- extractable attribute, getting with
 - okvAttrGetExtractable, [12-66](#)

F

freeing Oracle Key Vault Interface TTLV

- descriptor, okvEnvFreeResultObj, [7-4](#)

fresh attributes

- adding with okvAttrAddFresh, [12-26](#)
- getting with okvAttrGetFresh, [12-67](#)

J

Java packages

- enum class, in oracle.okv.kmip, [16-2](#)
- exceptions, in oracle.okv.exception, [16-1](#)
- OKVBatchOperation class, in
 - oracle.okv.operation, [16-3](#)
- OKVService class, in oracle.okv.service, [16-4](#)
- response classes, in oracle.okv.response, [16-3](#)

K

keys

- creating KMIP key object with okvCreateKey, [11-8](#)
- getting symmetric keys with okvGetKey, [11-32](#)
- registering symmetric, [11-65](#)
- rekeying with okvRekey, [11-81](#)

KMIP features

- supported managed objects, [3-1](#)
- supported operations, [3-2](#)
- supported profiles, [3-1](#)
- supported version, [3-1](#)
- used with Oracle Key Vault client SDK, [3-1](#)

KMIP objects

- activating with okvActivate, [11-3](#)
- adding attributes with okvAddAttribute, [11-5](#)
- certificate request operations with
 - okvRegCertificateRequest, [11-59](#)
- creating key with okvCreateKey, [11-8](#)
- decrypting with okvDecrypt, [11-10](#)
- deleting attributes with okvDeleteAttribute, [11-14](#)
- destroying with okvDestroy, [11-16](#)
- encrypting with okvEncrypt, [11-18](#)
- getting attribute list with okvGetAttributeList, [11-21](#)
- getting attributes with okvGetAttributes, [11-24](#)
- getting certificate request with
 - okvGetCertificateRequest, [11-29](#)
- getting certificate with okvGetCertificate, [11-26](#)
- getting opaque data with
 - okvGetOpaqueData, [11-34](#)
- getting private key with okvGetPrivateKey, [11-37](#)
- getting public key with okvGetPublicKey, [11-40](#)
- getting secret data with okvGetSecretData, [11-43](#)
- getting symmetric key objects with
 - okvGetKey, [11-32](#)

KMIP objects (*continued*)

- getting template objects with
 - okvGetTemplate, [11-45](#)
- implementing locate operations with
 - okvLocate, [11-47](#)
- modifying attributes with okvModifyAttribute, [11-50](#)
- opaque data object register operations with
 - okvRegOpaqueData, [11-63](#)
- querying with okvQueryCapability, [11-52](#)
- register certificate with okvRegCertificate, [11-55](#)
- register private key with okvRegPrivateKey, [11-69](#)
- register public key with okvRegPublicKey, [11-72](#)
- rekey operations with okvRekey, [11-81](#)
- revoke operations with okvRevoke, [11-84](#)
- secret data object register operations with
 - okvRegSecretData, [11-76](#)
- symmetric key object register operations with
 - okvRegKey, [11-65](#)
- template object register operations with
 - okvRegTemplate, [11-79](#)

L

length

- certificate length, getting with
 - okvAttrGetCertLen, [12-50](#)

M

memory management

- memory management context with
 - OKVMemoryCtx, [6-10](#)
- memory re-allocation with okvRealloc, [9-3](#)
- pointer to memory allocation program with
 - okvMalloc, [9-2](#)
- pointer to memory freeing program with
 - okvFree, [9-1](#)

N

names

- adding with okvAttrAddName, [12-30](#)
- attribute, name, and index, getting with
 - okvGetAttributeObject, [12-101](#)
- getting name, index attribute with
 - okvAttrGetName, [12-71](#)
- getting name, index length attribute with
 - okvAttrGetNameValueLen, [12-72](#)

never extractable

- adding with okvAttrAddNeverExtractable, [12-32](#)
- getting never extractable attribute with
 - okvAttrGetNeverExtractable, [12-73](#)

O

objects

- group, adding with okvAttrAddObjectGroup, [12-33](#)
- group, getting with okvAttrGetObjectGroup, [12-74](#)
- length, getting with
 - okvAttrGetObjectGroupLen, [12-76](#)
- type, adding with okvAttrAddObjectType, [12-34](#)
- type, getting with okvAttrGetObjectType, [12-77](#)
- OKITTLVGetChild, [14-6](#)
- okvActivate C API, [11-3](#)
- okvAddAttribute C API, [11-5](#)
- okvAddAttributeObject C API, [12-9](#)
- OKVAttr C API, [6-2](#)
- okvAttrAddActivationDate C API, [12-10](#)
- okvAttrAddArchiveDate C API, [12-8](#)
- okvAttrAddCertLen C API, [12-11](#)
- okvAttrAddCertType C API, [12-13](#)
- okvAttrAddCompromiseDate C API, [12-14](#)
- okvAttrAddCompromiseOccurrenceDate C API, [12-15](#)
- okvAttrAddContactInfo C API, [12-16](#)
- okvAttrAddCryptoAlgo C API, [12-17](#)
- okvAttrAddCryptoLen C API, [12-18](#)
- okvAttrAddCryptoParams C API, [12-19](#)
- okvAttrAddCryptoUsageMask C API, [12-20](#)
- okvAttrAddDeactivationDate C API, [12-21](#)
- okvAttrAddDestroyDate C API, [12-22](#)
- okvAttrAddDigest C API, [12-23](#)
- okvAttrAddDigitalSignAlgo C API, [12-24](#)
- okvAttrAddExtractable C API, [12-25](#)
- okvAttrAddFresh C API, [12-26](#)
- okvAttrAddInitialDate C API, [12-27](#)
- okvAttrAddLastChangeDate C API, [12-28](#)
- okvAttrAddLeaseTime C API, [12-29](#)
- okvAttrAddName C API, [12-30](#)
- okvAttrAddNeverExtractable C API, [12-32](#)
- okvAttrAddObjectGroup C API, [12-33](#)
- okvAttrAddObjectType C API, [12-34](#)
- okvAttrAddProcessStartDate C API, [12-35](#)
- okvAttrAddProtectStopDate C API, [12-36](#)
- okvAttrAddRevocationReason C API, [12-37](#)
- okvAttrAddState C API, [12-38](#)
- okvAttrAddUniqueID C API, [12-39](#)
- okvAttrAddUsageLimits C API, [12-40](#)

- okvAttrAddX509CertId C API, [12-41](#)
- okvAttrAddX509CertIss C API, [12-42](#)
- okvAttrAddX509CertIssAltName C API, [12-44](#)
- okvAttrAddX509CertSubj C API, [12-45](#)
- okvAttrAddX509CertSubjAltName C API, [12-47](#)
- okvAttrExtractTTLV C API, [15-4](#)
- okvAttrGetActivationDate C API, [12-48](#)
- okvAttrGetArchiveDate C API, [12-49](#)
- okvAttrGetCertLen C API, [12-50](#)
- okvAttrGetCertType C API, [12-51](#)
- okvAttrGetCompromiseDate C API, [12-52](#)
- okvAttrGetCompromiseOccurrenceDate C API, [12-53](#)
- okvAttrGetContactInfo C API, [12-54](#)
- okvAttrGetContactInfoLen C API, [12-55](#)
- okvAttrGetCryptoAlgo C API, [12-56](#)
- okvAttrGetCryptoLen C API, [12-58](#)
- okvAttrGetCryptoParams C API, [12-59](#)
- okvAttrGetCryptoUsageMask C API, [12-60](#)
- okvAttrGetDeactivationDate C API, [12-61](#)
- okvAttrGetDestroyDate C API, [12-62](#)
- okvAttrGetDigest C API, [12-63](#)
- okvAttrGetDigestLen C API, [12-64](#)
- okvAttrGetDigitalSignAlgo C API, [12-65](#)
- okvAttrGetExtractable C API, [12-66](#)
- okvAttrGetFresh C API, [12-67](#)
- okvAttrGetInitialDate C API, [12-68](#)
- okvAttrGetLastChangeDate C API, [12-69](#)
- okvAttrGetLeaseTime C API, [12-70](#)
- okvAttrGetName C API, [12-71](#)
- okvAttrGetNameValueLen C API, [12-72](#)
- okvAttrGetNeverExtractable C API, [12-73](#)
- okvAttrGetObjectGroup C API, [12-74](#)
- okvAttrGetObjectGroupLen C API, [12-76](#)
- okvAttrGetObjectType C API, [12-77](#)
- okvAttrGetProcessStartDate C API, [12-78](#)
- okvAttrGetProtectStopDate C API, [12-79](#)
- okvAttrGetRevocationReason C API, [12-80](#)
- okvAttrGetRevocationReasonMessageLen C API, [12-81](#)
- okvAttrGetState C API, [12-82](#)
- okvAttrGetUniqueID C API, [12-83](#)
- okvAttrGetUniqueIDLen C API, [12-84](#)
- okvAttrGetUsageLimits C API, [12-85](#)
- okvAttrGetX509CertId C API, [12-86](#)
- okvAttrGetX509CertIdIssuerLen C API, [12-87](#)
- okvAttrGetX509CertIdSerialNoLen C API, [12-88](#)
- okvAttrGetX509CertIss C API, [12-90](#)
- okvAttrGetX509CertIssAltName C API, [12-91](#)
- okvAttrGetX509CertIssAltNameLen C API, [12-93](#)
- okvAttrGetX509CertIssDNLen C API, [12-94](#)
- okvAttrGetX509CertSubj C API, [12-95](#)
- okvAttrGetX509CertSubjAltName C API, [12-97](#)
- okvAttrGetX509CertSubjAltNameLen C API, [12-98](#)
- okvAttrGetX509CertSubjDNLen C API, [12-100](#)
- okvAttrMakeTTLV C API, [15-5](#)
- OKVAttrNo C API, [6-5](#)
- okvBatchCreate C API, [11-96](#)
- okvBatchExecute C API, [11-97](#)
- okvBatchFree C API, [11-98](#)
- okvConnect C API, [8-1](#)
- okvConnSendRecvBytes C API, [8-3](#)
- okvConnSet C API, [8-4](#)
- okvConnUnSet C API, [8-6](#)
- okvCreateKey C API, [11-8](#)
- okvCreateKeyPair C API, [11-92](#)
- OKVCryptoContext C API, [6-6](#)
- okvCryptoContextCreate C API, [15-6](#)
- okvCryptoContextFree C API, [15-7](#)
- okvCryptoContextGetAuthEncryptionAdditionalData C API, [15-8](#)
- okvCryptoContextGetAuthEncryptionTag C API, [15-9](#)
- okvCryptoContextGetBlockCipherMode C API, [15-11](#)
- okvCryptoContextGetIV C API, [15-12](#)
- okvCryptoContextGetPadding C API, [15-13](#)
- okvCryptoContextGetRandomIV C API, [15-14](#)
- okvCryptoContextSetAuthEncryptionAdditionalData C API, [15-15](#)
- okvCryptoContextSetAuthEncryptionTag C API, [15-16](#)
- okvCryptoContextSetBlockCipherMode C API, [15-17](#)
- okvCryptoContextSetIV C API, [15-18](#)
- okvCryptoContextSetPadding C API, [15-20](#)
- okvCryptoContextSetRandomIV C API, [15-21](#)
- okvCryptoResponseGetAuthEncryptionTag C API, [15-22](#)
- okvCryptoResponseGetDecryptedData C API, [15-23](#)
- okvCryptoResponseGetEncryptedData C API, [15-25](#)
- okvCryptoResponseGetIV C API, [15-26](#)
- okvCustomAttrAddBoolean C API, [12-107](#)
- okvCustomAttrAddByteString C API, [12-108](#)
- okvCustomAttrAddDateTime C API, [12-109](#)
- okvCustomAttrAddEnum C API, [12-111](#)
- okvCustomAttrAddInteger C API, [12-112](#)
- okvCustomAttrAddInterval C API, [12-113](#)
- okvCustomAttrAddLongInteger C API, [12-114](#)
- okvCustomAttrAddStructure C API, [12-115](#)
- okvCustomAttrAddTextString C API, [12-117](#)
- okvCustomAttrGet C API, [12-118](#)
- okvCustomAttrGetBoolean C API, [12-122](#)
- okvCustomAttrGetByName C API, [12-124](#)
- okvCustomAttrGetByteString C API, [12-125](#)
- okvCustomAttrGetByteStringLen C API, [12-127](#)
- okvCustomAttrGetType C API, [12-128](#)

- okvCustomAttrGetDateTime C API, [12-129](#)
- okvCustomAttrGetEnum C API, [12-130](#)
- okvCustomAttrGetInterval C API, [12-133](#)
- okvCustomAttrGetLongInteger C API, [12-135](#)
- okvCustomAttrGetStructure C API, [12-136](#)
- okvCustomAttrGetTextString C API, [12-138](#)
- okvCustomAttrGetTextStringLen C API, [12-139](#)
- okvDecrypt C API, [11-10](#)
- OKVDecryptResponse C API, [6-7](#)
- okvDecryptResponseCreate C API, [15-27](#)
- okvDecryptResponseFree C API, [15-28](#)
- okvDeleteAttribute C API, [11-14](#)
- okvDestroy C API, [11-16](#)
- okvDisconnect C API, [8-7](#)
- okvEncrypt C API, [11-18](#)
- OKVEncryptResponse C API, [6-7](#)
- okvEncryptResponseCreate C API, [15-29](#)
- okvEncryptResponseFree C API, [15-31](#)
- OKVEnv C API, [6-8](#)
- okvEnvCreate C API, [7-1](#)
- okvEnvFree C API, [7-3](#)
- okvEnvFreeResultObj C API, [7-4](#)
- okvEnvGetOpRequestObj C API, [7-5](#)
- okvEnvSetConfig C API, [7-7](#)
- okvEnvSetTrace C API, [7-8](#)
- OKVErr C API, [6-9](#)
- okvErrGetDepth C API, [10-1](#)
- okvErrGetDepthForBatch C API, [10-3](#)
- okvErrGetNum C API, [10-4](#)
- okvErrGetNumAtDepth C API, [10-6](#)
- okvErrGetNumAtDepthForBatch C API, [10-7](#)
- okvErrGetNumForBatch C API, [10-9](#)
- okvErrReset C API, [10-11](#)
- okvFree C API, [9-1](#)
- okvGetAttributeList C API, [11-21](#)
- okvGetAttributeObject C API, [12-101](#)
- okvGetAttributes C API, [11-24](#)
- okvGetBatchOperationCount C API, [11-100](#)
- okvGetBatchOperationName C API, [11-101](#)
- okvGetCertificate C API, [11-26](#)
- okvGetCertificateRequest C API, [11-29](#)
- okvGetKey C API, [11-32](#)
- okvGetOpaqueData C API, [11-34](#)
- okvGetPrivateKey C API, [11-37](#)
- okvGetPublicKey C API, [11-40](#)
- okvGetSecretData C API, [11-43](#)
- okvGetTemplate C API, [11-45](#)
- okvGetTextForErrNum C API, [10-12](#)
- okvGetTextForTag C API, [15-33](#)
- okvGetTextForTagEnum C API, [15-34](#)
- okvGetTextForTagType C API, [15-35](#)
- okvLocate C API, [11-47](#)
- okvMalloc C API, [9-2](#)
- OKVMemoryCtx C API, [6-10](#)
- okvModifyAttribute C API, [11-50](#)
- OKVObjNo C API, [6-11](#)
- OKVOps C API, [6-11](#)
- okvOpsCreate C API, [13-1](#)
- okvOpsExecuteOp C API, [13-2](#)
- okvOpsFree C API, [13-4](#)
- OKVOpsNo C API, [6-12](#)
- okvQueryCapability C API, [11-52](#)
- okvRealloc C API, [9-3](#)
- okvRegCertificate C API, [11-55](#)
- okvRegCertificateRequest C API, [11-59](#)
- okvRegKey C API, [11-65](#)
- okvRegOpaqueData C API, [11-63](#)
- okvRegPrivateKey C API, [11-69](#)
- okvRegPublicKey C API, [11-72](#)
- okvRegSecretData C API, [11-76](#)
- okvRegTemplate C API, [11-79](#)
- okvRekey C API, [11-81](#)
- okvRevoke C API, [11-84](#)
- OKVServerInformation C API, [6-13](#)
- okvSign C API, [11-86](#)
- OKVSignResponse C API, [6-14](#)
- okvSignVerify C API, [11-89](#)
- OKVSignVerifyResponse C API, [6-14](#)
- OKVTTLV C API, [6-13](#)
- okvTTLVAddToObject C API, [14-2](#)
- okvTTLVAddToObjectByTag C API, [14-3](#)
- okvTTLVGetChild C API, [14-4](#)
- okvTTLVGetChildCount C API, [14-7](#)
- okvTTLVGetChildCountByTag C API, [14-8](#)
- okvTTLVGetFirstChildByTag C API, [14-9](#)
- okvTTLVGetLen C API, [14-10](#)
- okvTTLVGetRequest C API, [14-12](#)
- okvTTLVGetResponse C API, [14-13](#)
- okvTTLVGetTag C API, [14-14](#)
- okvTTLVGetType C API, [14-15](#)
- okvTTLVGetValue C API, [14-16](#)
- okvTTLVGetValueCopy C API, [14-17](#)
- operation management
 - about, [13-1](#)
 - creating OKI operation handle with
 - okvOpsCreate, [13-1](#)
 - executing custom KMIP operations with
 - okvOpsExecuteOp, [13-2](#)
 - freeing OKI operation handle with
 - okvOpsFree, [13-4](#)
 - getting query information TTLV structure with
 - OKVServerInformation, [6-13](#)
 - getting request and response OKVTTLV structure with OKVOps, [6-11](#)
- Oracle Key Vault, [5-1](#)
 - advanced program, about, [5-4](#)
 - basic program, about, [5-2](#)
 - program connection, [5-9](#)
 - program environment, [5-8](#)
 - program session, [5-9](#)

Oracle Key Vault (*continued*)

- program with batching, about, [5-4](#), [5-6](#)
 - See also Oracle Key Vault Interface (Oracle Key Vault)

Oracle Key Vault client SDK

- about, [2-1](#)
- advantages, [2-2](#)
- C SDK file contents, [4-5](#)
- downloading, [4-1](#)
- Java SDK file contents, [4-7](#)
- platforms supported, [2-2](#)
- program structure, [5-1](#)
- who should use, [2-2](#)

Oracle Key Vault Interface (Oracle Key Vault), [5-1](#)

- program structure, [5-1](#)

oracle.okv.exception Java package, [16-1](#)

oracle.okv.kmip Java package, [16-2](#)

oracle.okv.operation Java package, [16-3](#)

oracle.okv.response Java package, [16-3](#)

oracle.okv.service Java package, [16-4](#)

P

passwords

- SSL connection wallet, `okvEnvSetConfig`, [7-7](#)

Q

queries

- `okvQueryCapability`, [11-52](#)

R

revokes

- `okvRevoke`, [11-84](#)
- reason message length, getting with `okvAttrGetRevocationReasonMessageLen`, [12-81](#)
- reason, getting with `okvAttrGetRevocationReason`, [12-80](#)
- revocation reason, adding with `okvAttrAddRevocationReason`, [12-37](#)

S

sessions

- Oracle Key Vault program, [5-9](#)

state

- attribute, getting with `okvAttrGetState`, [12-82](#)

T

templates

- getting with `okvGetTemplate`, [11-45](#)
- registering with `okvRegTemplate`, [11-79](#)

time

- lease time, adding with `okvAttrAddLeaseTime`, [12-29](#)
- lease time, getting with `okvAttrGetLeaseTime`, [12-70](#)
- `okvCustomAttrAddDateTime`, [12-109](#)
- `okvCustomAttrGetDateTime`, [12-129](#)

trace files

- location of, using `okvEnvSetTrace`, [7-8](#)

TTLV (tag type length value)

- freeing TTLV descriptor, `okvEnvFreeResultObj`, [7-4](#)
- root of Oracle Key Vault Interface TTLV descriptor, `okvEnvGetOpRequestObj`, [7-5](#)

TTLV objects

- about, [14-2](#)
- child TTLV object, creating with `okvTTLVAddToObject`, [14-2](#)
- child TTLV object, creating with `okvTTLVAddToObjectByTag`, [14-3](#)
- child TTLV object, getting with `okvTTLVGetChild`, [14-4](#)
- child TTLV object, getting with tag using `OKITTLVGetChild`, [14-6](#)
- first child TTLV object, getting with `okvTTLVGetFirstChildByTag`, [14-9](#)
- length value of TTLV object, getting with `okvTTLVGetLen`, [14-10](#)
- number of child TTLV objects, getting of parent with `okvTTLVGetChildCountByTag`, [14-8](#)
- number of child TTLV objects, getting with `okvTTLVGetChildCount`, [14-7](#)
- Oracle Key Vault structure, defining with `OKVTTLV`, [6-13](#)
- tag value of TTLV object, getting with `okvTTLVGetTag`, [14-14](#)
- TTLV child attributes, converting with `OKIAttrExtractTTLV`, [15-5](#)
- TTLV child attributes, converting with `okvAttrExtractTTLV`, [15-4](#)
- TTLV object pointer, getting with `okvTTLVGetValue`, [14-16](#)
- TTLV object type value, getting with `okvTTLVGetType`, [14-15](#)
- TTLV object value, getting with `okvTTLVGetValueCopy`, [14-17](#)
- TTLV request object, getting with `okvTTLVGetRequest`, [14-12](#)

TTLV objects (*continued*)

TTLV response object, getting with
 okvTTLVGetResponse, [14-13](#)

type

certificate type, getting with
 okvAttrGetCertType, [12-51](#)

 U

unique IDs

adding with okvAttrAddUniqueID, [12-39](#)
 attribute, getting with okvAttrGetUniqueID,
[12-83](#)
 length, getting with okvAttrGetUniqueIDLen,
[12-84](#)

usage

limits, adding with okvAttrAddUsageLimits,
[12-40](#)
 limits, getting with okvAttrGetUsageLimits,
[12-85](#)

utility APIs

about, [15-4](#)
 collection of KMIP attributes with OKVAttr, [6-2](#)
 creating crypto context, creating with okvGetTextForTag,
[15-6](#)
 creating decrypt response structure, creating with
 okvDecryptResponseCreate, [15-27](#)
 creating encrypt response structure, creating with
 okvEncryptResponseCreate, [15-29](#)
 freeing crypto context, freeing with okvCryptoContextFree,
[15-7](#)
 freeing decrypt response structure, freeing with
 okvDecryptResponseFree, [15-28](#)
 freeing memory for encrypt response structure, freeing with
 okvEncryptResponseFree, [15-31](#)
 getting authenticated encryption additional data, getting with
 okvCryptoContextGetAuthEncryptionAdditionalData,
[15-8](#)
 getting authenticated encryption tag, getting with
 okvCryptoContextGetAuthEncryptionTag, [15-9](#)
 getting authenticated encryption value, getting with
 okvCryptoResponseGetAuthEncryptionTag, [15-22](#)
 getting block cipher mode, getting with
 okvCryptoContextGetBlockCipherMode, [15-11](#)
 getting decrypted data from response structure, getting with
 okvCryptoResponseGetDecryptedData, [15-23](#)
 getting encrypted data from response structure, getting with
 okvCryptoResponseGetEncryptedData, [15-25](#)
 getting IV parameter, getting with okvCryptoContextGetIV,
[15-12](#)
 getting IV value from encrypt response structure, getting
 with okvCryptoResponseGetIV, [15-26](#)
 getting padding IV parameter, getting with
 okvCryptoContextGetRandomIV, [15-14](#)

utility APIs (*continued*)

getting padding parameter, getting with
 okvCryptoContextGetPadding, [15-13](#)
 name of KMIP tag enumerated value, getting with
 okvGetTextForTagEnum, [15-34](#)
 name of KMIP tag, getting with okvGetTextForTag, [15-33](#)
 name of KMIP type, okvGetTextForTagType, [15-35](#)
 OKIAttr to TTLV structure, converting with
 okvAttrMakeTTLV, [15-5](#)
 setting authenticated encryption additional data, setting with
 okvCryptoContextSetAuthEncryptionAdditionalData,
[15-15](#)
 setting authenticated encryption tag, setting with
 okvCryptoContextSetAuthEncryptionTag, [15-16](#)
 setting block cipher mode, setting with
 okvCryptoContextSetBlockCipherMode, [15-17](#)
 setting IV parameter, setting with okvCryptoContextSetIV,
[15-18](#)
 setting padding parameter, setting with
 okvCryptoContextSetPadding, [15-20](#)
 setting random IV parameter, setting with
 okvCryptoContextSetRandomIV, [15-21](#)
 TTLV child attributes, converting with okvAttrExtractTTLV,
[15-4](#)

 X

X.509 certificate

add certificate ID, adding with
 okvAttrAddX509CertId, [12-41](#)
 add certificate issuer alternate name, adding
 with okvAttrAddX509CertIssAltName,
[12-44](#)
 add certificate issuer, adding with
 okvAttrAddX509CertIss, [12-42](#)
 add certificate subject alternate name, adding
 with
 okvAttrAddX509CertSubjAltName,
[12-47](#)
 add certificate subject, adding with
 okvAttrAddX509CertSubj, [12-45](#)
 get certificate ID issuer length, getting with
 okvAttrGetX509CertIdIssuerLen,
[12-87](#)
 get certificate ID serial number length, getting
 with
 okvAttrGetX509CertIdSerialNoLen,
[12-88](#)
 get certificate ID, getting with
 okvAttrGetX509CertId, [12-86](#)
 get certificate issuer alternate name length,
 getting with
 okvAttrGetX509CertIssAltNameLen,
[12-93](#)

X.509 certificate (*continued*)

- get certificate issuer alternate name, getting with `okvAttrGetX509CertIssAltName`, [12-91](#)
- get certificate issuer distinguished name length, getting with `okvAttrGetX509CertIssDNLen`, [12-94](#)
- get certificate issuer, getting with `okvAttrGetX509CertIss`, [12-90](#)
- get certificate subject alternate name length, getting with `okvAttrGetX509CertSubjAltNameLen`, [12-98](#)

X.509 certificate (*continued*)

- get certificate subject alternate name, getting with `okvAttrGetX509CertSubjAltName`, [12-97](#)
- get certificate subject distinguished name length, getting with `okvAttrGetX509CertSubjDNLen`, [12-100](#)
- get certificate subject, getting with `okvAttrGetX509CertSubj`, [12-95](#)