Java Card Development Kit

Simulator Release Notes

Release 24.0

F92101-02

February 2024

ORACLE

Java Card Development Kit Simulator Release Notes, Release 24.0

F92101-02

Contents

Topic

Release Notes for Java Card Development Kit Simulator 24.0.

Table of Contents

Introduction

Java Card technology enables secure elements, such as smart cards and other tamper-resistant security chips to host applications called applets, which employ Java technology.

Java Card technology offers a secure and interoperable execution platform that can store and update multiple applications on a single resource constrained device, while retaining the highest certification levels and compatibility with standards. Java Card developers can build, test, and deploy applications and services rapidly and securely. This accelerated process reduces development costs, increases product differentiation, and enhances value to the customers.

The Java Card Development Kit is a suite of components and tools for designing implementations of Java Card technology and developing applets based on the Java Card Specifications. It is available as three independent downloads:

- The Java Card Development Kit Simulator offers a runtime reference for Java Card applications.
- The Java Card Development Kit Tools are used to convert and verify Java Card applications.
- The Java Card Development Kit Eclipse plug-in offers an easy path for developing, testing and debugging Java Card applications.

Together, these three downloads provide a complete, stand-alone development environment in which applications written for the Java Card platform can be developed and tested.

These release notes describe the Java Card Development Kit Simulator, Version 24.0, which is based on version 3.2 of the Java Card Platform Specifications.

What's New

The complete set of Java Card SDK features are described in the Java Card Development Kit User Guide in the Java Card Documentation web site.

Java Card 3.2

The Java Card Development Kit Simulator now supports version 3.2 of the Java Card Platform specifications.

Additional Optional Features

The document Java Card Platform Options List describes the list of options available to implement a Java Card platform, based on the Java Card Specifications.

The following Java Card optional features and packages are supported by the Java Card Development Kit Simulator:

- Integer support
- Extended length APDU
- Encodings for 4 or 20 Logical Channels
- Object Deletion
- Extended CAP files
- Sensitive arrays
- Key Derivation Function (package `javacardx.security.derivation`)
- Sensitive Result (package `javacardx.security`)
- ByteBuffer (`javacardx.framework.nio`)
- StringUtil (`javacardx.framework.string`)
- Monotonic Counter (package `javacardx.security.util`)
- Certificate parsing (package `javacard.security.cert`)
- BCDUtil, BigNumber and ParityBit classes (package `javacardx.framework.math`)
- SysTime, TimeDuration classes (package `javacardx.framework.time`)
- TLV (package `javacardx.framework.tlv`)

List of Supported Cryptographic Algorithms

A list of algorithms supported in the Java Card Development Kit Simulator.

Table List of Supported Cryptographic Algorithms

Algorithms	Operations	Keys
NIST SP 800-90A DRBG	Pseudo Random Generation	-
CRC16, CRC32	Checksum	-

Table (Cont.) List of Supported Cryptographic Algorithms

Algorithms	Operations	Keys
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, MD5, RIPEMD-160	Message Digest	-
Symmetric Cryptography		
HMAC (SHA-1, SHA-256)	Signature	up to 512 bits
HKDF (SHA-1, SHA-256)	Key Derivation	up to 512 bits
DES, 3DES (2 keys, 3 keys)	Cipher, MAC Modes: ECB, CBC Paddings: ISO 9797 (M1, M2), PKCS5	64, 128, 192 bits
AES	Cipher, AEAD, MAC Modes: ECB, CBC, CFB, XTS, CCM, GCM Paddings: ISO 9797 (M1, M2), PKCS5	128, 192, 256 bits
Korean Seed	Cipher, MAC Modes: ECB, CBC	128 bits
Asymmetric Cryptography		
DSA	DSA Signature	1024, 2048 bits
RSA	Cipher, Signature schemes: PKCS1, PSS, OAEP	up to 4096 bits
DH	DH Key Agreement	1024, 2048 bits
ECC	ECDSA Signature, ECDH & PACE Key Agreement	NIST & Brainpool (112 to 521 bits)

GlobalPlatform

The Java Card SDK supports GlobalPlatform specification version 2.3.1 for application management.

It includes the following features:

- Issuer Security Domain
- SCP-03, i='70', AES 128-bit, 192-bit, 256-bit keys
- Card content management:
  - Load
  - Install
  - Make Selectable
  - Delete
- Store Data
- Card Recognition Data
- GlobalPlatform API (`org.globalplatform` version 1.6)

Please refer to the *Java Card Development Kit Simulator User Guide* for the complete set of supported features.

System Requirements

This product is targeted for use on a PC running on the following operating systems:

- Microsoft Windows for versions 10 or 11
- Linux for Ubuntu 20.04 LTS

The following software must be installed for the Java Card Development Kit Simulator to work:

- **Java Development Kit** (JDK): This release has been verified and tested with Oracle JDK 17 (64 bit version) and OpenJDK 17 (64 bit version). Download the JDK software from:

  https://www.oracle.com/technetwork/java/javase/downloads

  Install it according to the instructions on the website.
- **Eclipse IDE**: Eclipse IDE is optional and is required only for using Eclipse plug-in. Download the Windows Eclipse IDE from the following URL, and install it according to instructions on the website:

  https://www.eclipse.org/
- **OpenSSL 3.0.12**: The 32-bit version of the OpenSSL library is required for the Java Card Development Kit Simulator to work. See https://openssl.org.

Installation

The Java Card Specifications, the Java Card Development Kit Simulator, Tools and Eclipse plug-in must be downloaded and installed individually.

- See the Downloading the Specification Documents topic of the *Java Card Platform Specification Release Notes, Version 3.2* for more details on how to download the Java Card Specification bundle.
- See the Installation topic of the *Java Card Development Kit User Guide* for more details on how to install the Java Card Development Kit Simulator and Java Card Development Kit Tools.

Contents of the Development Kit Simulator

This release of the Java Card Development Kit Simulator contains Java Card simulation environment.

The following table describes the files and directories that are installed in the root installation directory (*JC_HOME_SIMULATOR*).

Directory/File	Description
`client`	Contains client components: an application management service API (`AMService.jar` file and javadoc documentation), a communication smartcardio API `(socketprovider.jar` file) and a debugger proxy (`jc-debug-proxy.jar` file) to manage, communicate, and debug Java Card applications.
`drivers`	It is only for the Linux version. It contains the IFDHandler (`libjcsdkifdh.so`) for PCSCLite allowing an application to communicate with the Java Card Development Kit Simulator based on PC/SC.
`legal`	Contains license files.
`runtime`	Contains the Java Card Development Kit Simulator binary executable.
`samples`	Contains sample applets and applications.
`tools`	Contains a tool to configure the Java Card Development Kit Simulator (`Configurator.jar`) with a secure channel protocol key set and a Global PIN.

Known Issues

There are no known issues.

Documentation

The Java Card Documentation web site provides online product documentation for the Java Card Platform.

Document	Description
Java Card Platform Specifications.	The following specification documents are available for the Java Card Platform, Version 3.2: • *Java Card Platform Runtime Environment Specification, Classic Edition, Version 3.2* (PDF format) • *Java Card Platform Virtual Machine Specification, Classic Edition, Version 3.2* (PDF format) • *Java Card Platform Application Programming Interface, Classic Edition, Version 3.2* (HTML format) • *Java Card Platform Specification Release Notes, Version 3.2* (HTML and PDF formats)
Java Card Options List	This document describes the list of options available to implement a Java Card platform, based on the Java Card Specifications.
Java Card Development Kit Simulator - User Guide	This document describes how to use the Java Card Development Kit Simulator and Eclipse plug-in to develop, test and debug applications for Java Card Platform, Version 24.0. It is available in HTML and PDF formats.
Java Card Development Kit Tools - User Guide	This document describes how to use the Java Card Development Kit Tools to convert and verify applications for Java Card Platform, Version 24.0. It is available in HTML and PDF formats.

Product Information

The Java Card Technology website provides useful information about the Java Card product.

Visit the Java Card Technology website to access the most up-to-date information on the following:

- Product news and reviews
- Release notes and product documentation

Documentation Accessibility
For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `https://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 `https://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `https://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.