

Oracle® Payment Interface
Security Guide
Release 6.2
E92437-01

December 2017

Copyright © 2010, 2017, Oracle and/or its affiliates. All rights reserved.

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 software or related documentation 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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	1-1
Audience	1-1
Customer Support.....	1-1
Documentation.....	1-1
Revision History.....	1-1
1 Oracle Payment Interface Security Overview	1-2
Basic Security Considerations	1-2
Oracle Payment Interface Security Overview	1-2
Establishing Secure Connections	1-4
Recommended Deployment Configurations	1-4
Component Security	1-5
Oracle Database Security	1-5
2 Installing a Secure Oracle Payment Interface	2-1
Configuring for the Installation	2-1
Installing the Oracle Payment Interface.....	2-1
Configuring the Connection.....	2-1
Post-Installation Configuration.....	2-2
Applying Software Patches	2-2
Configuring the Oracle Payment Interface Service	2-2
Rotating the Keys Protecting Communications.....	2-3
Changing Database Passwords.....	2-3
Purging Data.....	2-3
3 Implementing Oracle Payment Interface Security	3-4
Oracle Payment Interface Service Security	3-4
Managing Users	3-4
Authenticating the Service.....	3-4
Audit Trail Logging.....	3-4
Appendix A Secure Deployment Checklist	1

Preface

This document provides security reference and guidance for the Oracle Payment Interface (OPI).

Audience

This document is intended for:

- System administrators installing the Oracle Payment Interface
- End users

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

<https://support.oracle.com>

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received and any associated log files
- Screenshots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at the following URL: <http://docs.oracle.com/en/industries/hospitality/>

Revision History

Date	Description of Change
December 2017	Initial publication

1 Oracle Payment Interface Security Overview

This chapter provides an overview of the Oracle Payment Interface security and explains the general principles of application security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and secure passwords.
- **Learn about and use the Oracle Payment Interface security features.** See *Implementing Oracle Payment Interface Security* for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. The *Critical Patch Updates and Security Alerts* website contains more information at the following URL:
<http://www.oracle.com/technetwork/topics/security/alerts-086861.html>

Oracle Payment Interface Security Overview

The Oracle Payment Interface (OPI) integrates with the Point-of-Sale (POS) and the Property Management Systems (PMS) to manage the connections with third-party payment service providers (PSP) and payment processors. It is an interface bridging POS/PMS and processors/partner PSP. It shields POS/PMS from credit card processing details and from details of interfacing with different payment terminals and processors/3rd party payment service providers. It is a semi-integrated solution that can reduce or remove POS/PMS out of PADSS. It also provides a common platform that facilitates the adoption of new payment technologies/solutions.

The Oracle Payment Interface deploys on-premise with the POS and PMS client to transfer transaction data between the POS, PMS, and third-party payment service provider (PSP) hosts and terminals.

The following diagrams show how OPI bridges between POS/Opera and 3rd party PSPs for credit card processing.

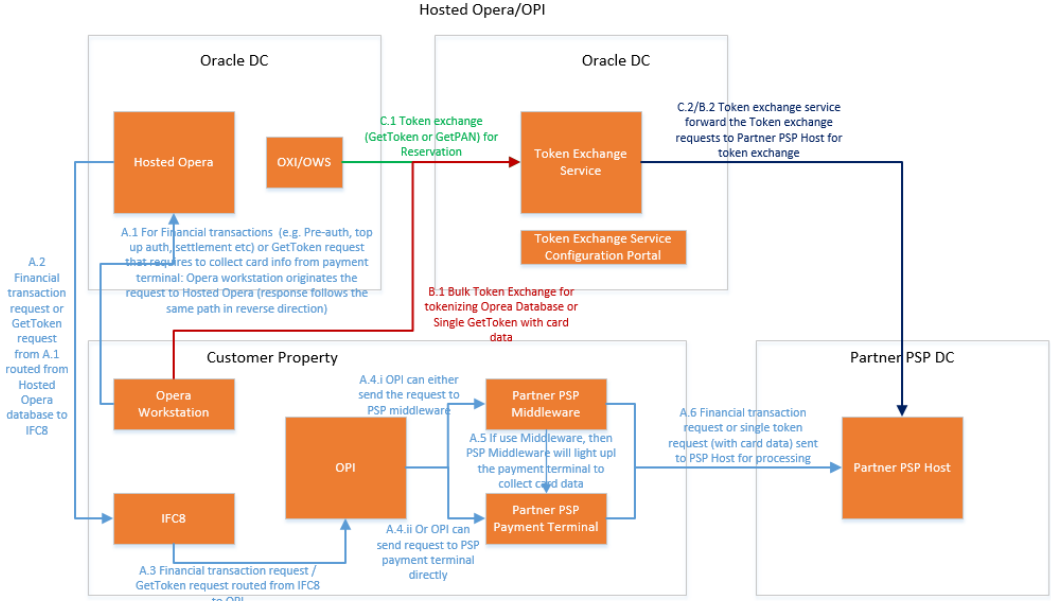


Figure 1. Hosted Opera integrates with OPI and PSP

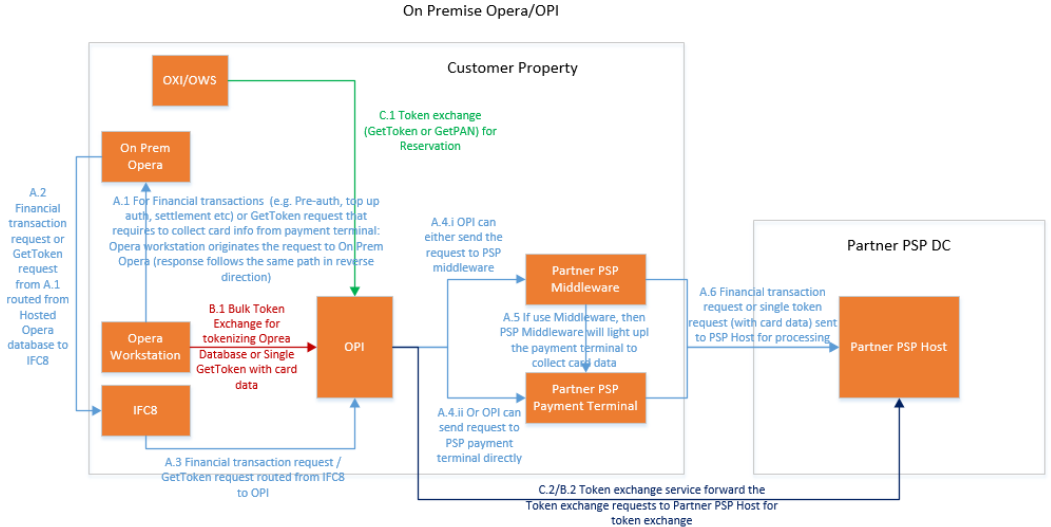


Figure 2. On Premise Opera integrates with OPI and PSP

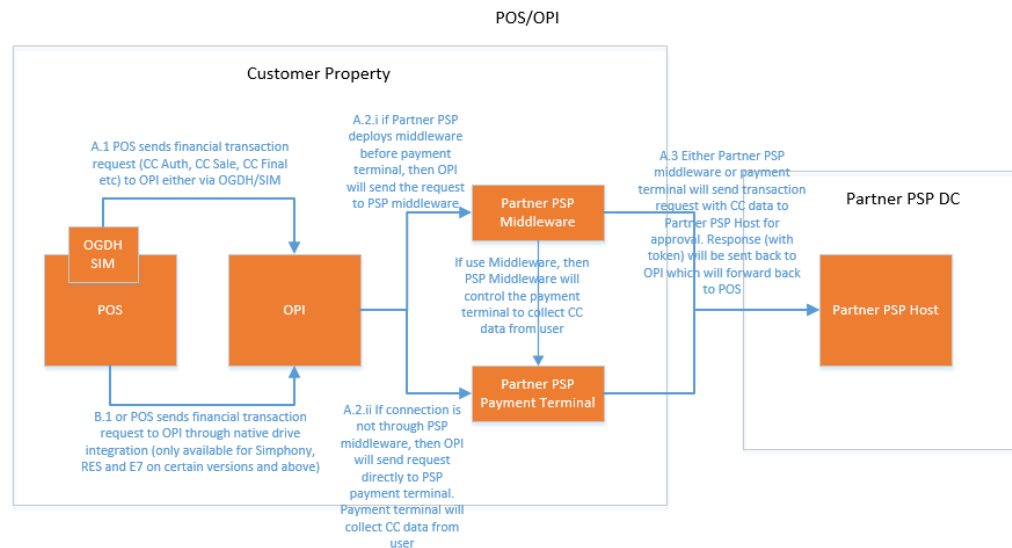


Figure 3. POS integrates with OPI and PSP

Establishing Secure Connections

- The Property Management System (PMS) Hosted or On Premise both use IFC8 to connect with OPI. IFC8 provides a shared key protected mechanism to secure the connection.
- PMS uses HTTPS with TLS 1.2 to connect to OPI for Token Exchange Services.
- POS has two ways to connect to OPI depending on what type of interface between POS and OPI. POS systems with OGDH use HTTPS with TLS 1.2 to connect to OPI and POS with native driver use HTTP with encrypted data to connect to OPI.
- OPI uses HTTPS with TLS 1.2 to connect to PSP with an option of two-way authentication for financial transactions.
- OPI uses HTTPS with TLS 1.2 to connect to PSP with two-way authentication for Token Exchange Services.
- OPI Configurator and Wizard use HTTP with encrypted data to connect to OPI Configuration Service.

Recommended Deployment Configurations

The Oracle Payment Interface (OPI) deploys on-premise with the POS and the PMS. The Oracle Payment Interface service deploys as a Microsoft Windows Service and listens to a configurable port for requests. The system/merchant administrator can use the OPI Configurator, a windows application to configure the Oracle Payment Interface Service.

A configuration service is also available for the client applications such as POS and PMS to configure OPI. The Oracle Payment Interface service uses Java KeyStore to save the communication certificates.

Component Security

Oracle Database Security

The *Oracle Database Security Guide* contains more information about the security best practices.

2 Installing a Secure Oracle Payment Interface

This chapter describes how to plan for installing the Oracle Payment Interface. The *Oracle Payment Interface Installation Guide* contains more information.

Configuring for the Installation

Before you install the Oracle Payment Interface, you must complete the following tasks:

- Apply critical security patches to the operating system.
- Apply critical security patches to the database server application.
- Install Microsoft .Net Framework. You must install Microsoft .Net Framework release 4.0.30319 or higher.
- Install Java Runtime Environment (JRE), version 1.8 or above
- Install Database Server, the databases OPI 6.2 supports are
 - MySQL 5.6
 - SQL Server 2008 R2 or later
 - SQL Server Express 2008 R2 or later
 - Oracle 12c or later
- Confirm database root /system administrator's password follows the Oracle GIS Guidelines and contains:
 - 8 characters
 - 1 letter
 - 1 number
 - 1 special character !@#\$\$%^&*
- Confirm the memory size contains at least 1024 MB of free space.
- Confirm the hard drive contains at least 6 GB of free space.

Installing the Oracle Payment Interface

Refer to the *Oracle Payment Interface Installation Guide* for more information.

POS

Configuring the Connection

When integrating with the Oracle Hospitality POS with the native driver, the Oracle Payment Interface Service Installer requests a POS Key or passphrase to authenticate the connection request from the native POS driver. This passphrase must contain at least 15 characters with at least one alphabet, one special character, and one number character.

The following Oracle Hospitality POS systems support connecting using a native driver:

- Symphony release 2.9 or higher
- RES 3700 release 5.5 MR1 or higher

When connecting to the Oracle Hospitality POS with an OGDH connection, during the installation process you must configure a POS certificate password when setting up a property. The POS certificate password must follow the Oracle GIS guidelines. The following systems support the use of OGDH connection.

- Symphony release 2.7 MR4 or higher
- Symphony First Edition release 1.6 MR6 or higher
- RES 3700 release 5.0 or higher
- 9700 Point-of-Sale release 4.0 or higher

For POS, it is recommended to use the native driver, if supported.

When connecting to PMS, during the installation process, you must create a key to secure the communication to IFC8. The key must also be input into the PMS IFC8 configuration. The following Oracle Hospitality PMS systems support connecting to the Oracle Payment Interface:

- Oracle Hospitality OPERA Property Management release 5.5.0.11 or higher
- Oracle Hospitality OPERA Cloud release 1.21 or higher

OPI on Premise Token Exchange requires three sets of certificates for the HTTPS communications (Please see the *Oracle Payment Interface Installation Guide* for details on how to deploy the certificates):

- OPI > PSP - (PSP - Client Side Certificates)
- Opera > OPI - (OPI- Server Side Certificates)
- Opera > OPI - (OPI – Client Side Certificates)

Post-Installation Configuration

This section describes additional security configuration steps to complete after you install the Oracle Payment Interface.

Applying Software Patches

Apply the latest Oracle Payment Interface patches available on My Oracle Support. Follow the installation instructions included with the patch.

Configuring the Oracle Payment Interface Service

During the installation, the Oracle Payment Interface Configuration Wizard launches to configure the Oracle Payment Interface Service. You can access the Configuration Wizard manually to add or update connections after the installation. Please refer to the *Oracle Payment Interface Installation Guide* for the detailed steps.

OPI provides an optional feature to communicate with PSP with two-way authentication. In this case, OPI communicates to the PSP using HTTPS with a client certificate for client authentication. That is, while a server side certificate is expected to be deployed at PSP (server side) for HTTPS communication, PSP is also expected to provide a client side certificate to be deployed at OPI side. OPI will present this client certificate during HTTPS communication with PSP so that PSP can authenticate OPI properly. Please refer to the *Oracle Payment Interface Installation Guide* for the detailed certificate handling steps.

In order to achieve this, PSP is required to provide two files:

- A client side certificate file with file type .pfx, this is a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password.
- The root certificate file for the server side certificate that is deployed at PSP side. OPI needs to load this root certificate file into the Java Key store so that OPI can properly recognize and trust the server side certificate deployed at PSP side. We expect the root certificate file provided by PSP to be in the format of .cer or .crt.

Rotating the Keys Protecting Communications

System administrators must update the password and rotate the POS Key frequently by following the PCI Guidelines for rotating encryption keys.

To rotate the POS key for POS with native driver:

1. Launch the OPI Configuration Tool.
2. Go to POS Configuration tab to update the key.

To rotate the shared security key for PMS IFC8,

1. Run Configuration Wizard to recreate the key.
2. Update PMS IFC8 configuration to have the new key.

To rotate the shared passphrase between OPI configuration service and tools:

1. On the OPI installation directory, go to the Services\ConfigService directory
2. Launch **LaunchSettingsAdminTool.bat** as administrator
Select Configuration Passphrase Tab
Update Passphrase
3. Go to the Services\ConfigService directory
4. Launch **RotatePassphrase.bat** as administrator
Update Passphrase for the tool

The PSP Client Side Certificates (for both financial transactions and token proxy service) expiration date will vary depending on what the PSP set during creation of the certificate. Check the expiration date in the properties of the certificate files. Be aware the PSP certificates must be updated prior to the expiration date to avoid downtime to the interface.

Changing Database Passwords

The Oracle Payment Interface Service Installer creates a database user. You must change this password frequently.

Purging Data

Audit data, logs, and transaction records save to database. Purge data according to the merchant's contract policy.

3 Implementing Oracle Payment Interface Security

Oracle Payment Interface Service Security

Managing Users

The Oracle Payment Interface Configuration Tool and the Wizard has its own user/password mechanism for authentication and authorization. The SuperUser is created when the configuration service is installed. Other users can be created/viewed/updated by the Configuration Tool. Make sure the password follow the Oracle GIS guidelines.

Authenticating the Service

Authentication means verifying the identity of a user, device, or other entity who wants to use data, resources, or applications. Validating that identity establishes a trust relationship for future interactions and applies to the entity accessing the service and to the entity providing the service.

In this release, the native POS driver communicates from the POS to Oracle Payment Interface using a shared passphrase to generate a Server Key encrypting the communication between client and server. Only the server/client which has the shared passphrase configured is an authenticated server/client.

PMS IFC8 communication channel uses shared key to authenticate server and client.

OPI Configuration Service and Tools communicate each other with shared key to authenticate server and clients.

Audit Trail Logging

When a user makes changes to the Oracle Payment Interface settings, the changes save in the database. Using the Oracle Payment Interface Configuration Tool the System Administrator can review, filter, and purge the audit log records. For security, no audit log information shows in the debug log files.

Purging Audit Trail Data

The audit records save in the database for minimum 90 days. You can manually purge the records older than 90 days using the Configuration tool.

To purge Audit records:

1. Log in to the configuration tool as a System Administrator.
2. Go To Audit page
3. Select the **Start date** and **End Date** to view the audit record.
4. Select the **View** option to view the records from the date range defined.
5. Select the **Purge** option to purge the Audit records.

Appendix A Secure Deployment Checklist

This appendix lists best practices to create a secure system.

The following security checklist includes guidelines that help secure your database:

- Install only what is required.
- Enforce password management.
- Practice the principle of least privilege.
 - Grant necessary privileges only.
 - Revoke unnecessary privileges from the PUBLIC user group.
 - Restrict permissions on run-time facilities.
- Restrict network access.
- Apply all security patches and workarounds.
 - Use a firewall.
 - Never poke a hole through a firewall.
 - Protect the Oracle listener.
 - Monitor listener activity.
 - Monitor who accesses your systems.
 - Check network IP addresses.