Oracle® Payment Interface Token Proxy Service

Security Guide
Release 6.1.2
F19414-01

May 2019

ORACLE

Contents

Preface

This document provides security reference and guidance for the Token Proxy Service.

Audience

This document is intended for end users and system administrators installing Token Proxy Service.

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
- Screen shots of each step you take

Documentation

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

Revision History

Date	Description of Change
Feb 2019	Initial publication

1 Token Proxy Service Security Overview

This chapter provides an overview of the Token Proxy Service 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 to it.
- **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. Performing a Secure Token Proxy Service Installation has more information on installing the software securely.
- **Learn about and use the Token Proxy Service security features.** Implementing Token Proxy Service Security has more information on the Token Proxy Service security features.
- **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. Oracle's Critical Patch Updates and Security Alerts website has more information on security-related patch updates and security alerts: http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Token Proxy Service Security Overview

Token Exchange Proxy Service

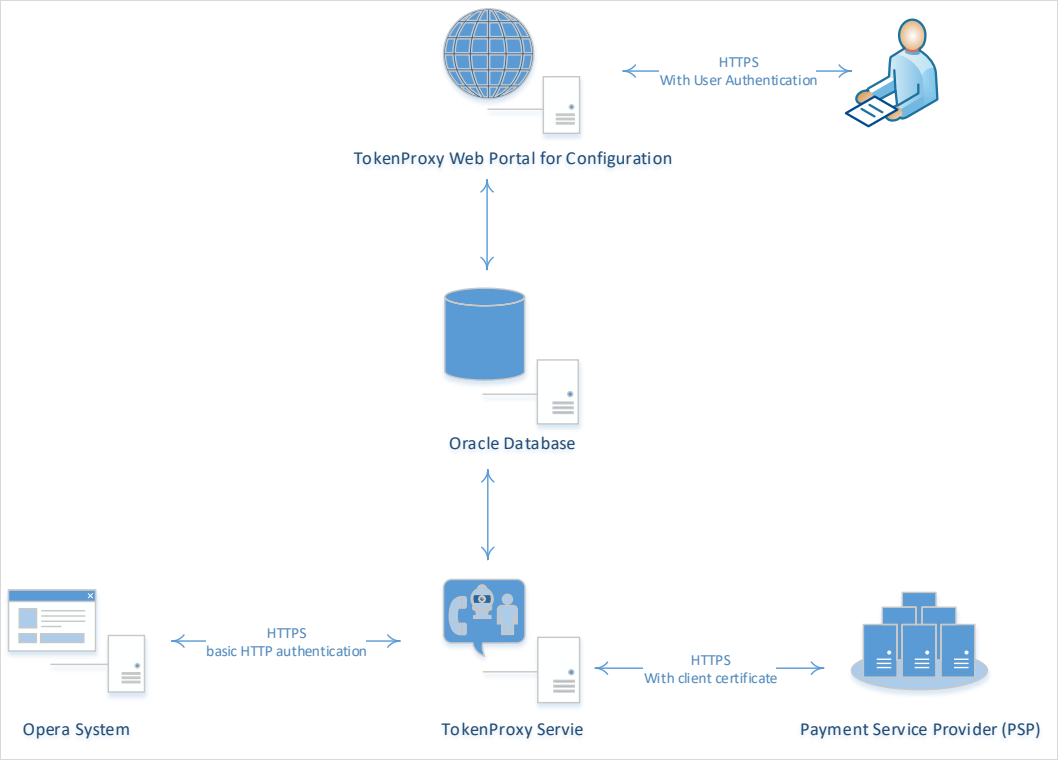
The Token Exchange Proxy Service is a proxy interface for the hosted OPERA application. This proxy service only processes the token or PAN exchange. The Oracle Hospitality partner payment service providers contain the actual token functionality. As a result, no financial transactions are exchanged and no PCI data saves in the Token Exchange Proxy Service system.

The Token Exchange Proxy system has three main components:

- The Database is used to store the configuration from the web portal, and the service will read from it.
- The Token Proxy Exchange Web Portal is used to configure the settings used by the service. It is a web application supplied in a WAR file suitable for hosting in Web Logic.

- The Token Proxy Exchange Service is a standalone application that can be run from a shell (or started automatically as a service in Windows). This application creates a listener to listen on a TCP port (configured in the database but default to 443) to listen for XML messages posted over HTTPS. This listener must be exposed to the client (for example, Opera systems).

Figure 1-1 – Token Exchange Proxy Service Architecture



Opera system communicates with Token Proxy Service using a HTTPS TLS 1.2 connection. TPS uses basic HTTP authentication to validate the request comes from a trusted client.

The Token Proxy Service communicates securely with third-party payment service providers by using HTTPS TLS 1.2 with client certificates.

Authorized datacenter administrators can use the Token Exchange Proxy Service web portal to configure the service, like the merchant account and payment provider information.

Recommended Deployment Configurations

The Token Exchange Service web portal deploys on an Oracle WebLogic server. The Token Exchange Proxy Service runs as a windows service or a standalone application that can be run from a shell in Linux. The database server runs an Oracle 12c Database.

The Token Exchange Service's listener manages its own use of the certificates provide by the datacenter using TLS1.2, so a firewall or load balancer (if present) must not offer any

form of HTTPS to HTTP bridging functionality, and instead the connection must be passed directly to the Token Proxy Exchange Service. The certificates provided must be installed on all servers running the Token Proxy Exchange Service in the event the service is installed on multiple machines for load balance or fail over. In the case if the certificate has to be deployed at load balancer, then a certificate should also be deployed at TPS app server to establish HTTPS connection from load balancer to TPS server. It is highly recommended to use CA signed certificates.

The service will also make outgoing connections to the Payment Service Provider. This outgoing connection will be to a URL specified by the payment service provider and the host/port will be specified by the PSP. Port 443 is the requested and recommended standard.

This outgoing connection can be over the internet or over VPN but must be using HTTPS with TLS1.2 or greater. HTTPS over a VPN connection is recommended for security reason.

Component Security

Operating System Security

The *Secure Configuration of Red Hat Enterprise Linux 5 Guide* and the *Hardening Tips for the Red Hat Enterprise Linux 5 Guide* documents contain more information about the operating system security.

Oracle Database Security

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

Oracle WebLogic Server Security

The *Securing a Production Environment for the Oracle WebLogic Server Guide* from Oracle Fusion Middleware contains more information.

By default, WebLogic Server is configured with two keystores, which are located in the `DOMAIN_HOME\security` and `WL_HOME\server\lib` directories, respectively:

- `DemoIdentity.jks`—Contains a demonstration private key for WebLogic Server. This keystore contains the identity for WebLogic Server.
- `DemoTrust.jks`—Contains the trusted certificate authorities from the `WL_HOME\server\lib\DemoTrust.jks` and the JDK `cacerts` keystores. This keystore establishes trust for WebLogic Server.

You should never use these demonstration keystores in a production environment. In production we recommend to use CA signed certificate. It is also fine to use self-signed certificate behind firewall for internal communication.

For information about how to configure keystores for use in a production environment, see Obtaining and Storing Certificates for Production Environments; Steps to create a

self-signed certificate and configure Custom Identity and Custom Trust with Weblogic Server using Keytool.

PII Data Security

Personally identifiable information (PII) identifies or can be used to identify, contact, or locate the person to whom the information pertains.

Token Proxy Service only collects minimal data (first name, last name and email) for the person who is assigned to manage the configuration. Token Proxy Service Configuration Web Portal provides a user profile page which shows the user's information in the system and allow the user to update/delete them.

The user account profile data can be deactivated but cannot be immediately deleted to maintain the integrity of the audit trail. The deactivated user can be permanently removed from the database after a configurable retention period. Please note the user account profile data is very limited (first name, last name and email) and only limited to users who are assigned responsibility to manage the configuration. The data once purged, cannot be re-created, accessed or read.

Based on the secure connection from TPS to PSP, PII data is encrypted during the process of communication.

2 Performing a Secure Token Proxy Service Installation

This chapter describes how to plan for installing the Token Proxy Service.

The *Oracle Hospitality Token Proxy Service Installation Guide* contains more information.

Configuring for the Installation

Before you install the Token Exchange Service, you must complete the following tasks:

- Have Java JDK 1.8 installed and apply latest Java update
- Have Oracle Database installed
- Have WebLogic 12 c installed
- Apply critical security patches to the operating system.
- Apply critical security patches to the database server application.
- Apply latest patch to WebLogic 12 c

For details, please refer to *Oracle Hospitality Token Proxy Service (Self-hosted) Prerequisite Installation Notes*

Installing the Token Proxy Service

You can perform a custom installation or a complete installation. You can install using the custom installation option to avoid installing options and products not required for your environment. The *Oracle Hospitality Token Proxy Service Installation Guide* contains more information.

Installing the Token Proxy Service consists of three parts:

- Database
- Token Proxy Web Portal
- Token Proxy Service

During the database install, a database user will be created for Token Proxy Service. The password must follow the Oracle GPS guidelines and contain:

- At Least 8 characters
- At least 1 capital and 1 lowercase letter
- At least 1 number
- 1 special character ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` | ~

Post-Installation Configuration

This section describes additional security configuration steps to complete after Token Proxy Service installs.

Applying Software Patches

- Apply critical security patches to the operating system.
- Apply critical security patches to the database server application.
- Apply latest patch to WebLogic 12 c
- Apply the latest Token Proxy Service patches available on My Oracle Support.

Follow the installation instructions included with the patch.

Configuring the Token Exchange Service

To configure the Token Exchange Service follow these guidelines:

- To manage the Token Exchange Service use the web portal and create a system administrator account. Enter the user name as the employee's email, then an email sends a token to enable the user to create a password. Create a password following the password requirements.
- After you create the system administrator account, you can create the other users and clients. Use the client user accounts to configure the third-party payment service provider connections. Define the user name and password for basic HTTP authentication in OPERA.
- You must change the password frequently following GIS guidelines for:
    - database user
    - web portal user
    - HTTP authentication
- The PSP Client Side Certificates expiry date will vary depending on what the PSP set during creation of the certificate. Check the expiry date in the properties of the certificate files. Be aware the PSP certificates will need to updating, prior to the expiry date to avoid downtime to the interface.

Data Purging

Audit data save to database. Purge data according to the merchant's contract policy.

3 Implementing Token Proxy Service Security

Token Exchange Service Security

Managing Users

Access to Token Proxy Configuration Web Portal is secured through Form-Based Authentication. The user is required to have a valid username and password in order to have access to the Portal.

Users are not allowed to create accounts by themselves; instead, the Web Portal administrator will be responsible for creating the accounts and assigning the appropriate permissions to the accounts. By default, user accounts get created without a predefined password, instead, users will be asked to define a password when logging in for the first time.

Token Proxy Configuration Portal uses Role-based Authorization in order to control the access to the different areas in the web portal, a Role is basically a named collection of privileges which can be assigned to users.

The system administrator role can access all functionality including:

- Creating or maintaining users
- Creating or modify any client
- Maintaining the card type translation
- Viewing or maintaining the audit logs

A client user can only log in and manage existing clients that they are specifically assigned to by a system administrator user. The client user role cannot create or view the details of other clients.

The Security mechanism in Token Proxy Configuration portal implements the following features:

- You must use an email as the user ID for the Token Exchange Service web portal.
- Create passwords using a reset password link containing a unique random token sent by email.
- The database stores passwords using a salt hash format. The hash algorithm is SHA256
- All password values are validated to ensure they meet the required minimum complexity.
- The system administrator and the client user roles are created during the installation.
- Configurable password expiration (default value: 90 days)

- Configurable account locking mechanism based on failed logging attempts (default: 3 failed attempts, default lock time: 240 minutes)
- Configurable Password History validation (users will not be able to repeat passwords used in the past, default: last 4 passwords)
- One-time-token-based reset password mechanism with configurable token expiration time

Authenticating the Service

The connection from Opera to Token Proxy Exchange Service is secured using Basic HTTP authentication over SSL (TLS 1.2 or later). Any client application interacting with Token Proxy Service will need to present a username and password in the request, Token Proxy Service will then validate the credentials presented by the client application/system and proceed to accept or reject the message according to outcome of the validation process.

The authorization credentials that the client application or system will use to communicate with Token Proxy Service are defined in Token Proxy Web Portal, these credentials (password) are stored in a salted-hashed form in Token Proxy DB to be used during the Client Authentication phase

The communication between Token Exchange Proxy Service and the Payment Service Providers is secured by using Certificate-based Mutual 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 Token Proxy Service side. Token Proxy Service will present this client certificate during HTTPS communication with PSP so that PSP can authenticate the service properly.

The mechanism is based on the following actions:

1. Token Proxy Service sends a requests to the Payment Service Provider (PSP)
2. PSP presents its certificate to Token Proxy Service
3. Token Proxy Service verifies the PSP certificate
4. If successful, Token Proxy Service sends its certificate to the PSP
5. PSP verifies the Token Proxy certificate
6. If successful, PSP accepts the requests, process it and sends the response back to Token Proxy Service

For details about the certificate requirements, please refer to *Certificate Requirements for OPI Communication to PSP,* section *Certificate Requirements for Token Exchange functionality.*

Note: The PSP Client Side Certificates expiry date will vary depending on what the PSP set during creation of the certificate. Check the expiry date in the properties of the certificate files. Be aware the PSP certificates will need to updating, prior to the expiry date to avoid downtime to the interface.

Using the Audit Trail

Token Proxy Configuration Portal also features an Auditing mechanism that allows to keep record of actions performed by users, actions such as:

- Successful user login/logout
- Failed user logging attempts
- Configuration updates
- Authorization/Authentication updates

The system records the configuration changes as the before and after states and records the data in the audit log table by serializing the record into a JSON string. All passwords hashes are stored in binary format and excluded from the serialization process. Using the Token Exchange Service web portal, you can view the audit records and export the audit records to a spreadsheet.

The audit records save in the database for a minimum of 90 days. The Auditing mechanism allows exporting the data from Database into .xls files for long term storage or, for analysis with tools such as Splunk. You can manually purge the audit records from the application. Purge data according to the merchant's contract policy.

Appendix Secure Deployment Checklist

This appendix lists actions that need to be performed to create a secure system. The following is an example:

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

- Install only what is required.
- Lock and expire default user accounts.
- Enforce password management.
- Practice the principle of least privilege.
    - Grant necessary privileges only.
    - Revoke unnecessary privileges from the PUBLIC user group. iii. 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.