Copyright © 2010, 2020, 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 .................................................................................................................. vii
  Audience ........................................................................................................ vii
  Customer Support ........................................................................................ vii
  Documentation ............................................................................................... vii
  Revision History ............................................................................................. vii

1 Pre-Installation ............................................................................................... 1-1

2 Installing the OPI ........................................................................................... 2-2

3 Upgrading the OPI .......................................................................................... 3-1
  OPI Upgrade Steps ........................................................................................ 3-1

4 Configuring OPI ............................................................................................... 4-4
  Certificates ....................................................................................................... 4-9
    PSP - Client Side Certificates ........................................................................ 4-9
    OPI - Server Side Certificates ...................................................................... 4-13
    OPI - Client Side Certificates ...................................................................... 4-15

5 Opera Configuration ......................................................................................... 5-16
  Creating an EFT Interface ................................................................................ 5-16
  Configuring the CC Vault ................................................................................ 5-20
  Cashiering Overview ....................................................................................... 5-21
    Credit Card Payment Transaction Codes .................................................... 5-21
  Overview of Credit Card Payment Types ....................................................... 5-22
  Credit Card Type Payment Setup Information ............................................. 5-23
    Sample List of Card Types ........................................................................... 5-23
    Individual Card Functions ............................................................................ 5-25
    Important Considerations ............................................................................ 5-27
    Update OPI Configuration Merchant Tenders ............................................. 5-27
    Update Functionality settings for Chip & Pin and PayOnly ......................... 5-28
  Configuring the Workstation .......................................................................... 5-28
  Configuring the Hotel Property Interface (IFC8) Instance to the OPERA Hotel
    Property Interface (IFC) ............................................................................... 5-29
  Configuring Authentication for the Hotel Property Interface (IFC8) with OPI .. 5-30
  Perform a Tokenization ................................................................................... 5-32
    Certificate Import using Microsoft Management Console .......................... 5-33
Preface

This document is to guide users attempting to configure Oracle Payment Interfaces On Premise Token Exchange Service.

Audience

This document is intended to cover the additional steps required to setup OPI to handle the On Premise Token Exchange functionality.

This document covers only the configuration of the additional On Premise Token Exchange functionality, it does not cover in detail, installation of the OPI software and IFC8 merchant configuration, separate documentation already exists to cover this.

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 http://docs.oracle.com/en/industries/hospitality/

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2017</td>
<td>• Initial publication</td>
</tr>
<tr>
<td>March 2019</td>
<td>• Documentation Updates</td>
</tr>
<tr>
<td>December 2019</td>
<td>• Updated OPERA client side certificates section and added content for Credit Card Payment Types.</td>
</tr>
</tbody>
</table>
1 Pre-Installation

Consider the following guidelines before installing Oracle Payment Interface (OPI):

**IF UPGRADING OPI, YOU MUST READ THE UPGRADING THE OPI SECTION FIRST.**

- OPERA Property Management System release 5.0.05.11 is the minimum release you can use to integrate with OPI.
- OPI 6.2 does not install a database. If doing a clean install of OPI, a database must be installed first.
- Upgrading to OPI 6.2 from OPI 6.1 and higher is supported but MPG versions are not supported. Prior to upgrading from OPI 6.1 to OPI 6.2 all credit card transactions must be finalized and closed as the schema upgrade will not include the migration of old transaction data to OPI side.
- Any previous version of MPG should be uninstalled prior to installing OPI 6.2.
- You cannot upgrade from MGDH 6.1.1.X to Native Driver 6.2 (must upgrade then switch to Native configuration).
- You cannot run upgrade from 6.1.1.X to 6.2 as unattended/silent (due to 6.1.1.X installation program differences between 6.2)
- The application requires Microsoft.NET Framework version 4.0 or higher.
- OPI requires at least 6 GB of free disk space and you must install OPI as a System Administrator.

During the installation you must confirm the following:

- Merchant IDs
- IP address of the OPI Server
- If there is an existing MySQL database installed, then the SQL root password is required.
- Workstation IDs and IPs that integrate with the PIN pad.
2 Installing the OPI

1. Copy OraclePaymentInterfaceInstaller_6.2.0.0.exe, double click it to launch the install.

2. Select your language, and then click OK.

3. Click Next on the Welcome to the InstallShield Wizard for Oracle Payment Interface screen.

4. Click Next on the OPI Prerequisites screen appears.

The Setup Type screen appears.

- Complete: All program features will be installed. (Requires the most disk space.)
- Custom: Select which program features you want installed. Recommended for advanced users only.

5. Make a selection, and then click Next.
If you selected the Custom install option, the Select Features screen appears with the following options:

a. Database Schema
b. OPI Services
c. Configuration Tool

All three of these features must be installed. It is just a matter of whether they are all installed on the same computer or on separate computers.

6. Select the features to install on this computer, and then click Next.

   The Choose Destination Location screen appears.

7. Accept the default installation location or click Change… to choose a different location, and then click Next.

8. Click Install on the Ready to Install the Program screen.

   The Setup Status screen displays for a few minutes.

9. The Setup Type screen appears.
10. Select the database type being used, and then click Next.

Note: OPI does not install any database, so the database must already be installed.

The Database Server screen appears.
The Name/IP: field defaults to localhost. This should be left as localhost if the OPI database is installed on the same computer. If the database is installed on another computer, the Name or IP address of that machine should be entered here.

**Note:** If the database type is MySQL, and you cannot use localhost for the Name/IP field, then some commands must be run manually on that MySQL database before proceeding. See MySQL command link in the OPI Basic Install doc for instructions. Setup will not complete if this is not done.

11. Accept the default Port # of 3306 (for MySQL), and then click Next.

The **Database Server Login** screen appears.

12. Enter the credentials for the DBA user of the database type selected, and then click Next.
   - For MySQL the Login ID: = root
   - For other database types the DBA user name/Login ID may be different.
   - Enter the correct password for the DBA user.

The **Database User Credentials** screen appears.
- **User Name**: Create a new user.
- **Password**: Create a password.
  - Password is case sensitive
  - Should be at least 8 characters in length
  - Must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#$%^&*

13. Confirm the password, and then click **Next**.

14. Click **OK** on the **Database connection successful** dialog.

15. Click **OK** on the **Database Configuration operation successful** dialog.

   The **Configuration Tool Superuser Credentials** screen appears.
• **User Name**: This can be any user name. It does not have to be a Windows account user.

• **Password**: Create a password.
  - Password is case sensitive
  - Should be at least 8 characters in length
  - Must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#$%^&*

16. Confirm the password, and then click **Next**.

17. Click **OK** on the *Create SuperUser operation successful* dialog.

The **Configuration Tool Connection Settings** screen appears.
• **Host**: May be left at 127.0.0.1 if the OPI configuration server is installed on this PC. Otherwise, specify the name or IP address of the PC where the OPI configuration server will be installed.

• Leave the default **Port** of 8090.

18. Click **Next**.

The **Configuration Tool Passphrase** screen appears.

19. **Passphrase**: The passphrase is case sensitive, should be at least 15 characters in length and must have at least one upper case letter, one lower case letter, one number and one special character from the following list: !@#$%^&*
20. Enter a passphrase, confirm it, and then click **Next**.  

After a brief pause, the **Configuration Wizard** launches.

21. Select **PMS**, Click **Next**.
3 Upgrading the OPI

VERY IMPORTANT: Read and follow the upgrade directions.

Note: OPI 6.1 and higher can be upgraded to OPI 6.2.

OPI Upgrade Steps

1. Right-click and Run as Administrator the OraclePaymentInterfaceInstaller_6.2.0.0.exe file to perform an upgrade.

2. Select a language from the drop-down list, and then click OK.

3. Click Next on the Welcome screen to proceed with the installation.

Prerequisites for the installation will be checked, including the required free drive space, details of the host environment, and the Java version that is present.

4. Click Next on the OPI Prerequisites screen.

5. Click OK on the OPI Upgrade screen.
6. **WARNING!** You must click **Yes**.
   
   **IF YOU CLICK NO, YOU WILL HAVE BOTH OPI 6.1 AND OPI 6.2 INSTALLED AND NEITHER WILL WORK.**
   
   Explanation: OPI will migrate the existing MySQL configuration information, but all previous OPI applications will be removed before the new files are installed.

7. Choose a Destination Location. Accept the default installation location or click **Change**... to choose a different location.

8. Click **Next**.
   
   The *Ready to Install the Program* screen displays.

9. Click **Install**.
   
   The *Setup Status* screen displays for a few minutes.

**Setup Type**

For database type, select **MySQL**. No other database type is supported for upgrades.

**Database Server**

Name/IP – The Hostname or IP Address used for communication to the MySQL database. This must be left at the default of localhost.

Port # – The Port number used for communication to the database

**Database Server Login**

DBA user
Login ID: root
Password: root user password for MySQL database.

**Database User Credentials**

User Name: This must be a new user name. It cannot be the same user from the 6.1 install.
Password: Password for the new database user.

**Configuration Tool Superuser Credentials**

User Name: This can be any user name. It does not have to be a Windows account user.
Password: Create a password, and then confirm it.
Configuration Tool Connection Settings
Host: May be left at 127.0.0.1 if the OPI configuration server is installed on this PC. Otherwise, specify the name or IP address of the PC where the OPI configuration server will be installed.
Port: Leave at 8090.

Configuration Tool Passphrase
Enter and confirm a passphrase.
Click Next.
The Configuration Wizard launches.
Continue to follow on-screen directions, verifying settings as you go.

POS Merchants
On the Merchants screen, click the wrench icon to the right of the existing merchant.
Verify the merchant settings are correct.

Merchant Pay At Table Configuration
If using Pay@Table, review the tender settings carefully as there are new fields that will not be pre-populated from the previous OPI install.
Continue to follow the on-screen directions.

InstallShield Wizard Complete
Click Finish to allow a reboot.
If you cannot immediately reboot, you must stop and then start the OPI Service for the current settings to take effect.
1. If manual start is required, run \\
\texttt{OraclePaymentInterface\V6.2\Config\LaunchWizard.exe}.
2. Login as the Super user you created during OPI installation.

![Oracle Payment Interface Configuration Wizard](image)

**OPI Interface**

Turn PMS on, and select the \textit{Enable Token Exchange Support} box. The Token Exchange functionality is separate to the IFC8 merchant functionality.

**OPI to PSP Communication Configuration**

- From the **OPI Mode** drop-down list, select the **Terminal** for the PED direct connection or select **Middleware** for middleware connection.

- Enable Mutual Authentication, this supports two-way authentication. The PSP partner needs to provide a set of .cer and .pfx files. Load the .cer file into JKS, and copy both root certificate and pfx to the key folder of OPI. Put the relative password here for Private key and root certificate key.

- Enter the third-party payment service provider middleware Host IP address if Middleware mode is selected. If Terminal mode is selected OPI configuration will populate another window in further steps to input Workstation ID and IP address.
Below is terminal mapping if you select terminal mode.

3. Click the blue + icon to add a new merchant configuration for OPERA.
4. To configure the OPERA merchant, enter the following information:

- The OPERA Vault Chain Code & Property Code; will form the SiteId value in the Token request messages.
- Select Generate Key. You must use this key to configure the Hotel Property Interface (IFC8). Add “FidCrypt0S\” to the generated key as prefix. For example: FidCrypt0S\xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- Enter the IFC8 IP address and port number for the Hotel Property Interface (IFC8) server.
- Enter the Merchant name, city, and country information.
- Click Next.

Although the other populated settings are not directly related to the Token Exchange Service configuration, Token Exchange will not be possible if the IFC8 interface is not running, as OPI will not progress past the IFC8 startup if the IFC8 connection is not possible.
5. Enter the OPERA payment code for each card type & next.

6. The top half of the *Token Exchange Configuration* screen allows you to configure the Header Authentication credentials used in communications from Opera->OPI.

- The details entered must match the details entered in the OPERA Interface Custom Data page (OPERA PMS Configuration | Setup | Property Interfaces | Interface Configuration | edit EFT IFC OPI | Custom Data tab)
Certificates

OPI on Premise Token Exchange requires the below sets of certificates:
- OPI > PSP - (PSP - Client Side Certificates)
- Opera > OPI - (OPI - Server Side Certificates)

Refer to the sections below for further details.

PSP - Client Side Certificates

The communication from OPI to the PSP for token exchange uses 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.

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

- A client side certificate file in the name of “OPI_PSP_1.pfx”, this is a PKCS#12 Certificate file that contains a public key and a private key and will be protected by a password. If the file provided by PSP has a different name, rename to “OPI_PSP_1.pfx” before deploying it to OPI.
- 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. For the demo purpose in this document, we assume the file has the name “ca-cert.crt”.

Handling the Client Side Certificate

To deploy the client certificate on the OPI side, place the file in folder \OraclePaymentInterface\v6.2\Services\OPI\key\n
The passwords set by the PSP must meet the minimum complexity requirements discussed below or it will not be possible to enter the details to the OPI configuration. Note: The PSP Client Side Certificates 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.

Handling the Root Certificate File
In order to load the root certificate file for the PSP server certificate into the Java key store, perform the following steps:

Creating a JKS
From a command prompt change to the JRE bin folder, in order for the keytool command to be recognized.
The exact path of your JRE bin folder will depend on the environment on which you are running the commands, and the JRE version you have installed, but may be similar to the example path shown below;

The three commands below, when run in sequence;
- Create a new Java keystore,
- Delete the default key created inside the Java Key Store
- Import the supplied root certificate in its place:

In the following example, the root .cer / .crt file is named ca-cert.crt, and is located in the folder C:\Certificates. Adjust file names and paths to be relevant to your details. OPI expects that the Java key store file that contains the root certificate for PSP server certificate to be in the name of “OPI_PSP_1Root”.

keytool -genkey -alias tempalias -keystore C:\Certificates\OPI_PSP_1Root

You must supply some basic information during the creation of the Java keystore, including a password.
You should use the same key password as for the keystore password when prompted. (i.e. RETURN if same as keystore password – Press Enter)
Verify the new Java keystore’s details by running the following command if required;

```
keytool –list –keystore c:\Certificates\OPI_PSP_1Root
```

![Command Prompt](image)

OPI_PSP_1.pfx & OPI_PSP_1Root must be located in the following folder:

\OraclePaymentInterface\v6.2\Services\OPI\key\n
![Windows Explorer](image)

**Updating a JKS with a new PSP certificate**

If this is an existing OPI On Premise Token Exchange installation, and you are importing a new PSP certificate prior to an existing key expiring, the current OPI_PSP_1.pfx & OPI_PSP_1Root, should be deleted from the \OraclePaymentInterface\v6.2\Services\OPI\key\ folder prior to following the steps above to import new certificate file.
OPI - Server Side Certificates

The lower half of the page relates to generating server side certificate used in communication from Opera to OPI.

1. Click Create OPI Token Server Certificates to proceed.

2. Populate the fields with the relevant information. The password fields validate the passwords are complex, so the passwords will need to meet these requirements;
   - Min 8 characters in length
   - Min 1 Alpha Character
   - Min 1 Numeric Character
   - Min 1 Special Character from the following list !@#$%^&*
3. Click **Generate** to continue.

This process will generate the `MICROS_OperaToken.pfx` & `MICROSOperaToken.cer` files in the following folder:
`\OraclePaymentInterface\v6.2\Services\OPI\key\`

**Note:** The OPI Server Side Certificates have a default expiration date of five years from the date of creation. Check the expiration date in the properties of the certificate files. The OPI Server Side Certificates must be updated prior to the expiration date to avoid downtime to the interface.

Copy the `MICROSOperformToken.cer` files to all of the Opera registered terminals that you will run the Token Exchange process from, and then import to Trusted Root Certification Authorities, using **mmc.exe** (Refer to section Certificate Import using Microsoft Management Console for more details)

Close the Certificate generation screen. You should now see ✅ under Certificate Created.
OPI - Client Side Certificates

Note: For the below OPERA versions, the Mutual Authentication requirement was removed for an OPI TPS communication.

- OPERA V5.5.0.23 and V5.6.4.0.
- OPERA Cloud 19.2.0.0 and 1.20.16.0.
5 Opera Configuration

Creating an EFT Interface

Log in to OPERA and go to Configuration. Select the menu option Setup | Property Interfaces | Interface Configuration. If there is no active EFT or CCW IFC Type, select New to add configuration for a new EFT interface.

1. Enter the following options, and then click OK:
   - **IFC Type**: EFT
   - **Name**: Oracle Payment Interface
   - **Product Code**: OPI
   - **Machine**: Select the machine
   - **License Code**: License code for interface
   - **IFC8 Prod Cd**: XML_OPI
2. Select the check box to enable the **CC Vault Function**.

3. Define the **Timeout** value as 210.

4. Select the **Translation** tab and then click **Merchant ID**.

5. Select **New** to add the Merchant ID. This must be the same as previously configured in OPI (MPG) Configuration.

---

**Configuring CHIP AND PIN (EMV)**

To configure the Functionality Setup:

1. Go to **Setup | Application Settings | IFC Group > Parameters**, and enable **CHIP AND PIN**.
2. Go to Setup | Property Interfaces | Credit Card Interface | Functionality Setup.
- **Online Settlement.** Select this check box to allow online settlement. OPI is an online settlement. This must be checked to activate the Chip and PIN Application Setting.

- **Authorization at Check In.** Select the payment methods that will trigger an automatic credit card authorization at check-in.

- **Authorization Reversal Allowed.** Select the payment methods that can process authorization reversals. This provides a request transaction to the Payment Partner to remove the existing authorization on a guest credit card or debit card if the folio payment type is changed or at check-out a different payment method is used. For example, a guest checks in on a reservation for a 5-night stay using a Visa credit card for payment type. At the time of authorization, a hold is put on the Visa credit card for the total cost of the stay. If the payment type is changed to another type on the reservation or the guest checks out using cash or a different brand of credit card, OPERA will send a reversal request for the originally selected Visa credit card authorization. A partial reverse authorization is not supported.

- **Authorization During Stay/Deposit.** Select the payment methods that allow manual and automatic authorizations following check-in and prior to check-out and settlement. This option must be enabled in order to allow authorizations by the end-of-day routine.

- **Authorization Settlement at Check-Out.** Select the payment types that use credit card authorization and settlement in one transaction request. These are payment types that do not allow an authorization separate from the settlement/sale.
  - The payment types that are available in the multi-select list of values are only payment types configured as EFT payment types. Any one payment type can be selected for credit card specific rules of Authorization at check-in, Authorization Reversal, and Authorization during Stay/Deposit. If they are selected for these card specific rules, then the payment types will not be available for Authorization During Stay/Deposit.

- **Chip and PIN Enabled Payment Types.** When the IFC | Chip and PIN application parameter is set to Y, this option is visible and selected by default. You may not unselect the check box. Select the LOV to choose the credit card payment types that will trigger a Chip and PIN message with or without credit card data to the EMV Device. Payment types that are configured here will not require that a credit card number or expiration date to be entered when selected as a payment method on the Reservation screen or on the Payment screen. This data can be provided in the response message from the Payment Partner.
Configuring the CC Vault

Go to Setup | Application Settings | IFC Group | Functions, and enable CREDIT CARD VAULT.

Configuration -> Setup -> Application Settings -> IFC -> Settings

OPERA uses the CREDIT CARD VAULT CHAIN CODE for the certificate lookup and should be populated with what was entered during the OPI configuration for PMS. The CREDIT CARD VAULT WEB SERVICE URL should be in the format: https://OPIHostIP:OPITokenPortNumber/TokenOPERA

The CREDIT CARD VAULT ID is currently not used.

The CREDIT CARD MAX CC PROCESSED is set to what the Payment Partner can support for the number of rows sent in one Token (GetID/GetCC) request. This is used during the bulk tokenization process and when multiple folio windows exist on OPERA Reservations. 50 is the default used when nothing is set here.

The CREDIT CARD VAULT TIMEOUT is set to the timeframe to wait for a response from the Token Proxy Service. At least 45 is recommended.
Cashiering Overview

Credit Card Payment Transaction Codes

1. In OPERA, go to Configuration | Cashiering | Codes | Transaction Codes to view the Credit Card Payments transaction codes setup.
2. Information for credit card payment transaction codes:

- **EFT** selection is necessary to send credit card transactions out to the integrated payment partner for the specific Payment type.

- **Manual** selection will not send out any transactions to the integrated payment partner.

- **CC Code** will auto-populate once the transaction code is associated to a Payment Type.

- **Display Code** can be populated to display a button when payment screen is accessed in OPERA PMS.

**Overview of Credit Card Payment Types**

The credit card payment types link with the transaction code:

1. In OPERA, go to **Configuration | Cashiering | Payment Types**.

   - The **IFC CC Type** field has the credit card code used such as MC, VA, AX.
   - The **Trn Code** field has the credit card transaction code.
Credit Card Type Payment Setup Information

In order to link Card Types, the Credit Cards types below will need to be created and available in OPERA PMS.

Sample List of Card Types

<table>
<thead>
<tr>
<th>Payment Types - Customer Present (Chip &amp; PIN)</th>
<th>Description</th>
<th>Capture Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA</td>
<td>Visa</td>
<td>CP can be used. Transaction will go to the EMV (Chip &amp; PIN) device.</td>
</tr>
<tr>
<td>MC</td>
<td>Mastercard</td>
<td>CP can be used. Transaction will go to the EMV (Chip &amp; PIN) device.</td>
</tr>
<tr>
<td>AX</td>
<td>American Express</td>
<td>CP can be used. Transaction will go to the EMV (Chip &amp; PIN) device.</td>
</tr>
<tr>
<td>DC</td>
<td>Diners Club</td>
<td>CP can be used. Transaction will go to the EMV (Chip &amp; PIN) device.</td>
</tr>
<tr>
<td>JC</td>
<td>JCB</td>
<td>CP can be used. Transaction will go to the EMV (Chip &amp; PIN) device.</td>
</tr>
<tr>
<td>CU</td>
<td>China Union Pay</td>
<td>CP can be used. Transaction will go to the EMV (Chip &amp; PIN) device.</td>
</tr>
<tr>
<td>VD</td>
<td>Visa Debit</td>
<td>CP cannot be used, manual card type selection is required. If CP is used, OPERA will default to Visa. Transaction will go to the EMV (Chip &amp; PIN) device.</td>
</tr>
<tr>
<td>MD</td>
<td>Mastercard Debit</td>
<td>CP cannot be used, manual card type selection is required. If CP is used, OPERA will default to Mastercard. Transaction will go to the EMV (Chip &amp; PIN) device.</td>
</tr>
<tr>
<td>Payment Types - Customer Present (Chip &amp; PIN)</td>
<td>Description</td>
<td>Capture Method</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------</td>
<td>----------------</td>
</tr>
<tr>
<td>CD</td>
<td>China Union Pay Debit</td>
<td>CP cannot be used, manual card type selection is required. If CP is used, OPERA will default to China Union Pay. Transaction will go to the EMV (Chip &amp; PIN) device.</td>
</tr>
<tr>
<td>MS</td>
<td>Maestro</td>
<td>CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip &amp; PIN) device. Customer present ONLY!</td>
</tr>
<tr>
<td>VP</td>
<td>V-Pay</td>
<td>CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip &amp; PIN) device. Customer present ONLY!</td>
</tr>
<tr>
<td>BC</td>
<td>GiroCard</td>
<td>CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip &amp; PIN) device. Customer present ONLY!</td>
</tr>
<tr>
<td>AB</td>
<td>AliPay</td>
<td>CP can be used, but PayOnly recommended. Transaction will go to the EMV (Chip &amp; PIN) device. Customer present ONLY!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payment Types - Customer NOT Present (Keyed)</th>
<th>Description</th>
<th>Capture Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>KVA</td>
<td>Visa Keyed</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
<tr>
<td>KMC</td>
<td>Mastercard Keyed</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
<tr>
<td>KAX</td>
<td>American Express Keyed</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
<tr>
<td>KDC</td>
<td>Diners Club Keyed</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
<tr>
<td>KJC</td>
<td>JCB Keyed</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
<tr>
<td>KCU</td>
<td>China Union Pay Keyed</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
<tr>
<td>KVD</td>
<td>Visa Debit Keyed</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
<tr>
<td>KMD</td>
<td>Mastercard Debit</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
<tr>
<td>Payment Types - Customer NOT Present (Keyed)</td>
<td>Description</td>
<td>Capture Method</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>KCD</td>
<td>China Union Pay Debit</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payment Types - One Shot Cards (Keyed)</th>
<th>Description</th>
<th>Capture Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>VVA</td>
<td>Visa Virtual</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
<tr>
<td>VMC</td>
<td>Mastercard Virtual</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
<tr>
<td>VAX</td>
<td>American Express Virtual</td>
<td>Card not present transaction (CNP, MO/TO, Mail Order / Telephone Order, MOTOEC)</td>
</tr>
</tbody>
</table>

**Individual Card Functions**

<table>
<thead>
<tr>
<th>Payment Types - Customer Present (Chip &amp; PIN)</th>
<th>Authorization at Check-in</th>
<th>Pay Only (no Authorization)</th>
<th>Deposit Y/N</th>
<th>Cashier Payment Y/N</th>
<th>A/R Payment Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>MC</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>AX</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>DC</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>JC</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>CU</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>VD</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>MD</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>CD</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>MS</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>VP</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>BC</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Payment Types - Customer Present (Chip &amp; PIN)</td>
<td>Authorization at Check-in</td>
<td>Pay Only (no Authorization)</td>
<td>Deposit Y/N</td>
<td>Cashier Payment Y/N</td>
<td>A/R Payment Y/N</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------</td>
<td>----------------------------</td>
<td>-------------</td>
<td>---------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>AB</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payment Types - Customer NOT Present (Keyed)</th>
<th>Authorization at Check-in</th>
<th>Pay Only (no Auth)</th>
<th>Deposit Y/N</th>
<th>Cashier Payment Y/N</th>
<th>A/R Payment Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>KVA</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>KMC</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>KAX</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>KDC</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>KJC</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>KCU</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>KVD</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>KMD</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>KCD</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payment Types – One Shot Cards (Keyed) OPTIONAL!!!</th>
<th>Authorization at Check-in</th>
<th>Pay Only (no Authorization)</th>
<th>Deposit Y/N</th>
<th>Cashier Payment Y/N</th>
<th>A/R Payment Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td>VVA</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>VMC</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>VAX</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
Important Considerations

- Transaction codes for Chip & PIN, KEYED and VIRTUAL cannot be the same!
- SOLO cards do not exist anymore, and cannot be used.
- VISA ELECTRON and VISA DELTA should not be created as separate transaction / payments codes, these cards will fall under VISA.
- DISCOVER cards now fall under DINERS CLUB.
- VIRTUAL cards can only be VISA, MASTERCARD and AMERICAN EXPRESS.
- V-Pay, GiroCard and AliPay can only be Chip & PIN.

Update OPI Configuration Merchant Tenders

Enter the OPERA payment code for each card type, and then click Next.
Update Functionality settings for Chip & Pin and PayOnly

- Selection for Chip & Pin and PayOnly cards

Configuring the Workstation

If the workstation is connected to a Chip & Pin terminal, the Chip & Pin Device Available check box must be enabled.

1. In OPERA | Setup | Workstations | edit your workstation.
2. Select the Chip & Pin Device Available check box to enable the device for this workstation (this allows the generic CP Payment Type to display in the LOV for a reservation).
Configuring the Hotel Property Interface (IFC8) Instance to the OPERA Hotel Property Interface (IFC)

To configure the link between the interfaces:

1. In the Hotel Property Interface, go to the PMS1 tree and select OPERA in the application layer.
2. Enter the OPERA IFC number in the parameter IfcNum value.

You can find the OPERA IFC number in OPERA on the IFC Configuration of the related Hotel Property Interface (IFC) (Row_ID).

3. Go to the PMS1 tree in the Physical Layer.
4. Enter the port number into Parameter value Port. This is the port IFC8 uses to communicate with the opera IFC controller.
5. Select Enter and Apply to re-initiate IFC8, and then click Save.
Configuring Authentication for the Hotel Property Interface (IFC8) with OPI

You must secure the connection between OPI and Hotel Property Interface (IFC8) by exchanging encryption keys at startup. This authentication key must be defined by OPI. The corresponding key must be entered in the Hotel Property Interface (IFC8) configuration.

1. In the Hotel Property Interface (IFC8) configuration, go to the IFC1 tree, and then in the Application Layer, select the XML_OPI option.

2. Copy the generated key from Configuring OPI - OPERA merchant step 3, and add “FidCrypt0S|” to the generated key as prefix. For example: FidCrypt0S|xxxxxxxxxxxxxxxxxxxxxxxxx

3. Copy this string into IFC8 Parameter IfcAuthKey value field.
4. Go to **IFC1** tree and select the **Physical Layer**.

5. Enter the port number in port value. This is the same port that was configured in OPI.

6. Click **Apply**, IFC8 reinitiates.

7. The **IfcAuthKey** value now shows an encrypted key and the entered string is now encrypted by IFC8.

8. Click **Save**, and then click **OK** to close the IFC8 Configuration form.

IFC8 now connects with OPI and OPERA IFC Controller. To verify IFC8 successful status, confirm that all 6 status indicators are green.
Perform a Tokenization

Utilities -> Convert CC -> Convert Vault CC Information -> Test Client

Complete the Test Client conversion to enable the Credit Card Vault Conversion functions.

OPI only supports the Convert CC function; the other conversion options are not currently supported.
Certificate Import using Microsoft Management Console

1. Find and open mmc.exe from start menu
2. Go to File | Add or Remove Snap-ins, add certificates to Selected snap-ins, and then click OK.

3. Expand Certificates, expand Personal or Trusted Root as required, and then select Certificates.

4. Right-click Certificates, select All Tasks, and then select Import.
On the Certificate Import Wizard Welcome page, click Next.
Browse to the location of the certificate file, and then click Next.
If required enter the password relevant to the certificate you are importing, and then click Next.
If imported is successful the certificates Common Name will be listed under the folder that was selected during import.