Copyright © 2002, 2019, 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 ............................................................................................................................... 5
  Audience ......................................................................................................................... 5
  Customer Support .......................................................................................................... 5
  Documentation .............................................................................................................. 5
  Revision History ........................................................................................................... 5

1 EFT Tokenization ........................................................................................................ 6
  Introduction .................................................................................................................. 6
  Feature Availability ....................................................................................................... 6
  Prerequisites .................................................................................................................. 6

2 Configuration ............................................................................................................... 7
  User Right to Enable the Feature .................................................................................. 7
  Global Settings ............................................................................................................. 7

3 Bulk Credit card tokenization .................................................................................... 9
  OPI Certificates ........................................................................................................... 9
  The Bulk credit card tokenization process .................................................................... 9
    User right to execute the bulk tokenization process ................................................... 9
    Run the bulk tokenization process ........................................................................... 9

4 Reservation ................................................................................................................ 11
  Entering a credit card into Reservation (Card not present) .......................................... 11

5 EFT IFC8 Interface with OPI ..................................................................................... 12
  Card present transactions ............................................................................................. 12
    Example for a card present authorization .................................................................. 12
    Example for an additional authorization .................................................................. 13
    Example for a settlement: ......................................................................................... 13
  Card not present transactions ....................................................................................... 13
    Example for a settlement: ......................................................................................... 13

6 Suite8 Online Interface ............................................................................................. 15

7 Authorization Reversal and RRN Number Handling ................................................. 16
  Global Settings: ............................................................................................................ 16
    Send Auth Code option: ............................................................................................. 16
    Send RRN in Authorization/Settlements: .................................................................... 17
  Send RRN number in IFC Messages: ............................................................................ 17
  Reservation – Credit Card grid: ................................................................................... 18
  XCAP table changes: .................................................................................................... 19
If Payment Partner supports handing out RRN Number for manual Authorization (e.g. via Phone) it is possible to add this RRN number into Manual Authorization screen together with the manual Authorization code.

8 Appendix

Reporting
Offline Credit Card Type
Online/Present Credit Card Type
Not Present Card Type
Debit Card Type
Preface

Audience

EFT Tokenization Guide is intended for system administrators, support and users familiar with the Suite8 and POS8 modules.

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>August, 2018</td>
<td>• Initial publication</td>
</tr>
<tr>
<td>March, 2019</td>
<td>• Release 8.14.0.0</td>
</tr>
<tr>
<td>July 2019</td>
<td>• Update for terminology changes</td>
</tr>
</tbody>
</table>
1 EFT Tokenization

Introduction

With release of Suite8 8.12.0.0 the new feature **EFT token handling** is available to support the integration with **Oracle Payment Interface** (OPI) which is a payment card processing interface that integrates with the Oracle Hospitality Point-of-Sale (POS) and the Oracle Hospitality PMS systems.

**OPI** defines a standard interface that partner payment service providers can implement to provide credit card processing functionality to Oracle Hospitality OPERA and Suite8 PMS, POS systems and also Oracle Retail Point of Sale (POS) Systems.

With activation of the new feature no credit card number will be stored in Suite8 anymore. Instead of this, a credit card number will be replaced with a **token ID**. Only the last 4 digits of the credit card number will be stored for informational purposes in the known credit card number fields all over the Suite8 application. All EFT transaction requests will only contain the token ID.

---

**Note:** The tokenization functionality supports the integration with OPI only.

It is not intended to use token handling with other legacy EFT Interfaces to vendor who might support token handling.

Feature Availability

The functionality is only available with the activated global setting **Enable Credit Card Tokenization** under Setup > Configuration > Global Settings > Interfaces > 2 Interfaces (IFC8) > Credit Card Interface.

Prerequisites

Suite8 Version 8.12.0 and higher.
2 Configuration

User Right to Enable the Feature

Activate the user rights under Setup > Configuration > User Rights > Configuration > Global Settings security related to enable the activation of the guest de-identification.

**Note:** This user right is not only required for this specific feature but also for other items in configuration

Global Settings

1. Activate the setting Enable Credit Card Tokenization under Global Settings > Interface > 2 Interfaces (IFC8) > Credit Card Interface.

2. As soon as you have activated the setting, another fields come up.

3. Configure the connection to the OPI token proxy service which is typically installed with the OPI service on a PC On-premise.

   Suite8 PMS always sends a token ID request through this connection whenever a credit card number is entered into the credit card number field in the Suite8 application (card not present) or a credit card is received from external systems (CRS). It is also used to request token ID when the bulk tokenization function is executed.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token Server URL</td>
<td><a href="https://IP">https://IP</a> Address of PC OPI is installed on:5012 /TokenOPERA</td>
<td>URL of the OPI on-premise Token Proxy Service Values displayed in black font are hardcoded values.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Version</td>
<td>3.2</td>
<td>This is a hardcoded value.</td>
</tr>
<tr>
<td>Timeout</td>
<td>30</td>
<td>The timeout time waiting for response from OPI Token Proxy. Enter the value in seconds.</td>
</tr>
<tr>
<td>Chain Code</td>
<td>EU</td>
<td>As defined in OPI configuration.</td>
</tr>
<tr>
<td>Max Requests</td>
<td>50</td>
<td>The number of credit cards to be sent in one bulk tokenization request. Enter a value between 1 and 50.</td>
</tr>
<tr>
<td>Property Code</td>
<td>EU</td>
<td>As defined in OPI configuration.</td>
</tr>
</tbody>
</table>

Example:

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>3.2</td>
</tr>
<tr>
<td>Chain Code</td>
<td>EU</td>
</tr>
<tr>
<td>Property Code</td>
<td>EU</td>
</tr>
<tr>
<td>Time out</td>
<td>30</td>
</tr>
<tr>
<td>Max Requests</td>
<td>50</td>
</tr>
</tbody>
</table>
3  Bulk Credit card tokenization

OPI Certificates

Certificates are created within OPI application. They are required for secure connection between PMS and OPI for the HTTPS connection. Server and Client certificates need to be installed on all Suite8 workstations that run.

1. The bulk tokenization process.
2. Token request for card not present credit card (manually entered by user or received by external system).

**Note:** Related certificates (a .cer and a .pfx) have to be delivered by OPI installer.

The Bulk credit card tokenization process

Once the Tokenization is active, the bulk credit card tokenization process is used to exchange all credit card numbers within the Suite8 Database with a token. This deletes all credit card numbers from the system; only token ID’s are stored representing the credit card number in further EFT Interface transactions.

Before Suite8 starts working with the tokenization functionality this bulk tokenization process should be executed.

User right to execute the bulk tokenization process

Go to Setup > Configuration > Users > User Definition > Rights > Cashiering > Move Postings and activate the user right Run bulk Credit card Tokenization.

![User Rights for Demonstration User](image)

**Note:** The user right is only available if the global setting is activated.

Run the bulk tokenization process

1. Go to Setup > Miscellaneous > System Maintenance > Cashiering and select Tokenize Existing Credit Cards to replace all existing credit cards with token ID’s.
2. A new window opens:

3. Select Yes to start the process and all existing credit card numbers stored in the Suite8 database are exchanged with a token ID. The process sends out a request message to OPI containing max 50 credit card numbers (depending on the defined values in global settings) & Expiry Date and expects a response message with a token ID. In case a credit card does not receive a token ID, the existing credit card is masked automatically and stored without a token ID. A credit card which is already expired retrieves no token ID but is also masked automatically and stored without a token ID.

**Note:** After the successful replacement of credit card numbers with token ID’s the process should **NOT** be executed again.

4. Go to user rights and deny the user right Run bulk Credit card Tokenization as this process should only be executed at time of activation of EFT tokenization handling.
4 Reservation

Entering a credit card into Reservation (Card not present)

1. Go to Reservation and edit the credit card.
2. Click the new option Get Token to request a token ID for the entered credit card number. This button is visible once the **Enable Credit Card tokenization** Parameter is active.

![Credit Card Details](image1)

3. You can still enter a not present credit card number and expiry date in the Add Credit Card section.

![Credit Card Details](image2)

4. When you click the **OK** or the **Get Token** button after entering the credit card number a get token request is sent out to the OPI Token Proxy service.
5. The OPI token proxy service connects with the Token Server (of the EFT vendor or Token server vendor).
6. In corresponding response message, Suite8 receives a token ID and a masked number with only the last 4 digits of the credit card number in the response message. This masked number is stored in the credit card number field as well as in the database to identify the credit card being used without showing the full number.

![Credit Card Details](image3)

7. When you click **OK** the token ID and the masked credit card number is stored in the Suite8 database.
8. Both values, the masked credit card number and the token ID are stored encrypted.
9. In addition, a notification shows that this credit card number is a tokenized card.

**Note:** The token ID is currently not visible to a user. The Card Type is not changed in this form and even the response message contains a different card type. Here the user’s choice is overwritten. So it is important that the user selects the correct Payment type/card type prior to entering the credit card number.
**5 EFT IFC8 Interface with OPI**

**Card present transactions**

The new IFC8 attribute **CardId** is used to receive the token ID in EFT transactions for CpAuthor, CpSettl or CpPayOnly action when the credit card is present and the card is entered into EMV device by the guest.

In addition instead of the full credit card number only the last 4 digits of the credit card number is received in the response message. This masked number is stored in the credit card number field of the application as well as in the database to enable the users to identify the credit card being used without showing the full number.

**Example for a card present authorization**

1. The request is sent without card details:

   ```xml
   <CpAuthor xmlns="x-schema:CpAuthorSchema_O" GuestNum="1011" GuestName="Token2" GuestFormattedName="Timo Token2" SequenceNum="02412" TotalAmount="50,00" GuestArrival="170825" GuestDeparture="170825" RequestType="4" WSNum="MBOESEL-DE" MerchantId="EU | EU" CardType="VA" />
   ``

2. The following response is received with token ID and masked credit card number:

   ```xml
   <CpAuthor xmlns="x-schema:CpAuthorSchema_I" PrinterPort="0" CreditcardNum="FidCryptAB|qnTGaSMTmBWTxlNqF2lC/Q==du5IiIXReXBljQkMjvugXcnNgYVTik4cd5miEioPdrlM" ExpyDate="1812" CardId="1645270703010266" GuestNum="1011" SequenceNum="02412" TotalAmount="50,00" WSNum="MBOESEL-DE" CardType="VA" AnswerStat="OK" CardType="VA" ClearText="FidCryptAB|Q4OYin4jIL0CPxtXyWuXw==4FrQaVLzWz6lytvX7tbnmmxTqKq7il1EPY4Ov+S4TLgY3L1bBc2TSfL1k9L5cB05kir7n15lYh/C6480xxRa7bq6nXCKTlps/XVzYjuxM/Rq880xzqe+r+yTLAgc21+qDuU21+q6Fa3sd1Ua5l1Mq20h1Vn2uRDFNgCw+scpMGL4Kf0vBLC22ZM3PqN/AdH0qyOpcGo7v7rPd10xW9BYvBxvqxdGxj2UvW9DTHpHIS/4QWTN6ejLLjZVTirhpoZFl0NX/xs+y+4aArUNWipVPFNa9pltM+bU6kRVMaM0Lki+FiviZn4hUTUCM5fGItvOnubh0Tiv1g0Nq2LGaICLq6OhMNHBgJEKA94lmpeoX5s6Wr0c0L+VD38naMgak9bIxeG5QRrCtCtJUtCsTRKxv21k0h49lIQMrPvXtGCuTshBwzwG9y0Ieevcd0boyw1hV2AvwZnxWw7qgKF+6ntoYp1V4RSc6h0QF+JDu/fb9c8gBQ3nMLAY8kFnhVcE3aq7s3M2xA7qKRN715FEHJ8DFBmf4Cm53CCqGdm24mhnhoEj5eApKRMYdRyGkHmw7x+f+kA1PbYwQumrX2fj+jU6uUrTRkpuULWq+H131nbk6240lhEHewngwX9KoKoWuy+yRxEsNmsw06nzbY5x+r7U/s9YIfA+4tlFUWz+xZ5z6fe7j5z6ps6h7f3+7z4A7h0e8Jm05f76875/5Y4MOzHx1CZnfJb8nbfGz0G58Xj98s6xqU1JBCOxM5dzUwSbuczSuC5WHk3p5YKD7qez6hTVPlH3yxeGENIT+UQ/3SgrnjDeNKh3juxnGD/rmlf59UrIP8QT7+4fV58Sk77LInNvsofny2h1a4AYBN1/BFG+Ar5BhWpckELg7hY1GLKTXvaLPXSCQBkdkKZrj08h5DFTCTN/7HVxyfz50lAeVCgFEBjMV6Q=" GuestNum="1011899" />
   ```

3. The following string shows the masked credit card number being received together with the token ID.

   ```xml
   <CpAuthor xmlns="x-schema:CpAuthorSchema_I" AnswerStat="OK" PrinterPort="0" ClearText="MerchantCopy
   CopyMerchant ID: 1234XXXXX1234567890
   Terminal ID: 1234567890
   TransType: AUTH
   Card No.: XXXXXXXXXXXX
   Expy Date: XX/XX
   Card Type: VISA
   Time: 11/1XXXXX 02:29
   Trace No.: 00000002916
   Auth Code: XXXXX
   AMOUNT: $XXXXXX
   Signature: ____________
   agree to the terms of my credit agreement.
   Customer Copy
   Merchant ID: 1234XXXXX1234567890
   Terminal ID: 1234567890
   TransType: AUTH
   Card No.: XXXXXXXXXXXX
   Expy Date: XX/XX
   Card Type: VISA
   Time: 11/1XXXXX 02:29
   Trace No.: 00000002916
   Auth Code: XXXXX
   AMOUNT: $XXXXXX
   Approved with Signature: ____________
   agree to the terms of my credit agreement.
   GuestNum="1011" SequenceNum="02412" WSNum="MBOESEL-DE"
   CardId="1645270703010266" CreditcardNum="XXXXXXXXXXXXX0266"
   ExpyDate="1812" CardType="VA" />
   ```

4. In the following transactions related to this reservation and credit card only the token ID is sent out in requests. The masked credit card number is not sent!
Example for an additional authorization

```xml
<CpAuthor xmlns="x-sch:schema:CpAuthorSchema_O" GuestNum="1011" GuestName="Token2"
GuestFormattedname="Timo Token2" SequenceNum="02413" TotalAmount="110,00" GuestArrival="170825"
GuestDeparture="170825" RequestType="4" WSNum="MBOESEL-DE" MerchantId="EU|EU" ExpyDate="1812"
CardId="1645270703010266" SecondAuth="60,00" AuthNum="101899" CardType="VA"/>
```

Example for a settlement:

```xml
<CpSettl xmlns="x-sch:schema:CpSettlSchema_O" ExpyDate="1812" CardId="1645270703010266" GuestNum="1011"
GuestName="Token2" GuestFormattedname="Timo Token2" SequenceNum="02414" TotalAmount="110,00"
GuestArrival="170825" GuestDeparture="170825" RequestType="4" WSNum="MBOESEL-DE" MerchantId="EU|EU"/>
```

Card not present transactions

Transactions for credit cards which are not present (e.g. Deposit payments, authorizations or settlements for credit cards which have been entered manually in the PMS) also contain only the token ID instead of the credit card number.

```xml
<CcAuthor xmlns="x-sch:schema:CcAuthorSchema_O" ExpyDate="1905" CardId="45391053399718652"
GuestNum="9122" GuestName="Kurth" GuestFormattedname="Esther Kurth" SequenceNum="02478"
TotalAmount="202,00" GuestArrival="171204" GuestDeparture="171204" RequestType="4"
WSNum="MBOESEL-DE" CardType="VAS" MerchantId="EU|EU"/>
```

The corresponding response messages do not contain any token ID or credit card number by default.

```xml
<CcAuthor xmlns="x-sch:schema:CcAuthorSchema_I" AnswerStat="OK"
ClearText="FidCryptAB|+6pmxvpgQtA687u/XseMdw==UEqw/52S0sPBr9F6zAAXS2TwPxNWkv4YBsg3RNcdx
NXdiGnLuOqvo56d5rV8xJWv9L+rV7FISEWEYLN7gfc/h4KWy6yov9H8B5ayubKxXdrTS5zmz9HG7VM
b6uykwrl+1dAdcvxwDG4sCo858vYLo8Lv4eEp9kpoB4NYQPoiEpP+xzruq2IDCvF998g9yTiz3A26jeGQ1Dz
BRex38JkgDd3PUW83okHrOE5C8mCag9MR33a383e080x9yPrlwnc6ZBw6GCF8s7Bex8d4WVSJzuY8fNeO
ivDkrxDUX++qQG1IKCWW0FL4MBGsePG8nzZE9DngNlxFIrDwW93C9d+irLeq41w5MCTZJRUAOGqks0fjrr4U
5xSNyjyQIIs7tbnI97MDA5/okCengXn866OdLJHgReoQDDBYI9PQDNTvJvk9uzfXs0e2A6HGB5Wj
A11QWCPn9dv4G/eXH5seScuFr2Oz2H2UTj9wY6UplgDgSj88RNg0PnZOD8qA9b1FU9b2Hse2J2s9e97Nm
LhuyYPZ8NOd53X20C88syNdMAbswv0qR61E8X8Fplp3MEmtr+cV7jvUUtqW9e8hS4qBhpMBw4/
Yx4h9j0l9h0w9XqBi8DeRaMHMt4e2p2BlQHuzzFrpm6jvDeom8MRiteHMWCSs4Jhvr4xne6nTv1H6eC3
NnHxJqDmaqkNANygMYJl8jSc8d8EhPrqgVAdLhKvrXmCDDqjziIpmS6r7HkuX5pEGzdF/P6fb5r5OX
rH09n9hkC1I3ltsf1w2CQNj5CD3ogt3j1Pc8Qk3F1jFaZeD8yDjVsOaezzBk32mPOLFbOk9/952GZJl4ET+t
N186l.b9m950/WIBFgYlUx40w7aCa5N8ZY/Xrgg=" PrinterPort="0" AuthNum="349272" GuestNum="9122"
SequenceNum="02478" WSNum="MBOESEL-DE" TotalAmount="202,00"/>
```

Example for a settlement:

```xml
<CcSettl xmlns="x-sch:schema:CcSettlSchema_O" ExpyDate="1905" CardId="45391053399718652" GuestNum="9122"
GuestName="Kurth" GuestFormattedname="Esther Kurth" SequenceNum="02478"
TotalAmount="202,00" GuestArrival="171204" GuestDeparture="171204" RequestType="4"/>
```
With the active EFT tokenization all credit card numbers within messages from Online Interface are replaced with a token ID through the OPI token Proxy Service.

**Example:**

The new reservation with the credit card number via Online IFC:

```xml
<Guarantee GuaranteeType="GuaranteeToCreditCard">
    <GuaranteesAccepted>
        <GuaranteeAccepted>
            <PaymentCard CardType="1" CardCode="MC" CardNumber="5266850134970843" ExpireDate="2018-12">
                <CardHolderName><![CDATA[Andrea Lehner]]></CardHolderName>
            </PaymentCard>
        </GuaranteeAccepted>
    </GuaranteesAccepted>
</Guarantee>
```

The related reservation in Suite8 shows the masked credit card number and notes that this card has been tokenized.
7 Authorization Reversal and RRN Number Handling

Global Settings:

Adding Global Setting parameter to 2Interface (IFC8) tab – Credit Card Interface

- Define Auth Code option
- Enable/disable handling of RRN Number

Send Auth Code option:

Defines if PMS sends the Last Received Authorization code or the first received Authorization code (from initial Authorization) in all following transactions (add. Authorizations, Settlements).

Last Received Auth Code
Original Auth Code
Authorization Reversal and RRN Number Handling

Send RRN in Authorization/Settlements:

Enable this parameter when RRN number is sent in outgoing transaction message. Define to send Original RRN (from initial Authorization response) or Last Received RRN (from last Authorization response) in all following outgoing transaction messages.

<table>
<thead>
<tr>
<th>Send RRN in Authorization/Settlements</th>
<th>Original RRN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Credit Card Tokenisation</td>
<td>Original RRN</td>
</tr>
<tr>
<td></td>
<td>Last Received RRN</td>
</tr>
</tbody>
</table>

Token Server URI: http://10.165.120.105:8992

Send RRN number in IFC Messages:

Suite8 sends out RRN number in AuthNum attribute for all Cp and Cc messages. If RRN Number is available it is sent in the AuthNum attribute together with AuthCode value separated by ‘|’ character. Format will be: [AuthNum] | [RRN]

Sample message:

Add. Authorization Request outgoing from PMS to IFC:

Add. Authorization Request outgoing from PMS to IFC:

[09.06/10:02:01]#0/0 -> TCP(idx:1/WS:10.165.120.100[50840])<CpAuthor xmlns="xsd:CpAuthorSchema_O" TotalAmount="160,00" ExpyDate="2212" CardId="4929263009781018" SecondAuth="10,00" AuthNum="A1235|001236" StartDate="171122" Cryptogram="12345678" GuestNum="9705" GuestName="Singer" GuestFormattedname="Anne Marie Singer" SequenceNum="02562" WSNum="MBOESEL-DE"/>

Incoming response from IFC to PMS:

[09.06/10:02:24]#1/0 < TCP(idx:1/WS:10.165.120.100[50840])<CpAuthor xmlns="xsd:CpAuthorSchema_I" AnswerStat="OK" ClearText="FidCryptAB|JTR26D2Enp5xMFKC0NspQ==+fYD0YWjC0ZPESyFWayUxg==" RequestType="0" CreditcardNum="FidCryptAB|sk6OZQN9oDBfXrCdVQSQ==kg11363tCx6L3oi74RWuFejrkoj61oQ0rG10erU4vQ=" ExpyDate="2212" CardId="4929263009781018" AuthNum="A1236|001237" CardType="VA" Cryptogram="12345678" GuestNum="9705" PaymentMethod="16" SequenceNum="02562" PrinterPort="0" WSNum="MBOESEL-DE" PathId="1" TotalAmount="160,00"/>

Settlement request outgoing from PMS to IFC:

[09.06/10:04:40]#0/0 -> TCP(idx:1/WS:10.165.120.100[50840])<CpSettl xmlns="xsd:CpSettlSchema_O" AuthNum="A1235|001236" ExpyDate="2212" CardId="4929263009781018" TotalAmount="20,00" GuestNum="9705" GuestName="Singer" GuestFormattedname="Anne Marie Singer" SequenceNum="02563" Date="180906" Time="100201" WSNum="MBOESEL-DE"/>
Reservation – Credit Card grid:

Enhanced the Authorization/Settlement grid in Reservation – Credit Card tab:
• added further columns
• option to now show all transactions for all credit cards for all folio windows, successful and failed transactions
• filter transactions by Billing Window
• show history
• show all cards
• show approvals only, show settlements only, show both

Show all cards and history for all Billing windows:

Show all cards and history for Billing Window 1:

Show all cards and history for Billing Window 2:

Show all Authorization transactions for all cards for Billing Window 2:
Choose Card by clicking on Credit card listed in Reservation Credit Card grid:

### XCAP table changes:

To enhance the Grid we added related fields to XCAP table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XCAP_TRANSACTION</td>
<td>VARCHAR</td>
<td>30</td>
<td>20 Stores RRN Number received from EFT</td>
</tr>
<tr>
<td>XCAP_TRANSACTION</td>
<td>NUMBER</td>
<td>10</td>
<td>211. Initial Authorization</td>
</tr>
<tr>
<td>XCAP_ADDAUTHAMENT</td>
<td>NUMBER</td>
<td>10</td>
<td>22 Authorization Top up account</td>
</tr>
<tr>
<td>XCAP_IFCMESSAGE</td>
<td>VARCHAR</td>
<td>200</td>
<td>23 Clear text received from EFT</td>
</tr>
<tr>
<td>XCAP_SUCCESSSTATUS</td>
<td>NUMBER</td>
<td>10</td>
<td>24 Success status 1.Success 2. Failed</td>
</tr>
<tr>
<td>XCAP_XCAP_TD</td>
<td>NUMBER</td>
<td>10</td>
<td>25 User ID</td>
</tr>
<tr>
<td>XCAP_TERMINAL</td>
<td>VARCHAR</td>
<td>60</td>
<td>26 Terminal/Workstation name</td>
</tr>
</tbody>
</table>

For successful Authorizations/Settlements/payments PMS stores fix message in XCAP_IFCMESSAGE

As to provide status message to display in the Credit card tab of a reservation. Currently this message text is fix and cannot be changed.

For failed transactions PMS stores message from IFC ClearText (if available) in XCAP_IFCMESSAGE
Added option to open the Authorization/Settlements grid on reservation level via Reservations grid - Options – Credit Card Authorization – Authorization/Settlement List:

It offers the same filter options than the grid within Reservations – Credit cards. It is possible to filter by credit card.

Same is available for Financial Accounts:

To access the list, navigate to In house guests Financial Account tab – Financial Account Settings (Edit) - Credit Cards button:
Manual Authorization screen

If Payment Partner supports handing out RRN Number for manual Authorization (e.g. via Phone) it is possible to add this RRN number into Manual Authorization screen together with the manual Authorization code.
8 Appendix

Reporting

Reporting stays untouched, it does not matter that "xxxxx" is overwritten by "xxxxx" - and ensures once more that under no circumstance a clear number is presented to the user.

Offline Credit Card Type

This is used for credit card numbers, which are not sent to an EFT system through EFT Interface. This is usually used in case EFT Interface is not operating or it is not intended to send transaction to EFT System.

Suite8 Code = free definable 3 letter code

Send to Interface = unticked – no message sent to IFC.

Online/Present Credit Card Type

This is used for credit cards which are present at front desk. You or the guest is able to enter the credit card into EMV Device at time of authorization payment.

- PMS Code = free definable 3-letter code
- IFC Credit card type = 2-letter code as setup in OPI (e.g. VA for VISA)
- Chip & Pin only = active for Chip&Pin transaction
- Authorization rule:
  - Authorization Type = At check-in - will use CpAuthor messages to IFC8
  - Settlement type = Online - will use CpSettl messages to IFC8
Not Present Card Type

This is used for credit cards which are not present (like card provided by phone, letter, mail, fax, external system) = card is not able to be entered into the pin pad by you or a guest. The card number needs to be entered directly into related field in Suite8.

- **PMS Code** = 2-letter code as setup in OPI (e.g. VA for VISA)
- **Send to Interface** = ticked
- **Chip & Pin Only** = unticked
- **Authorization rule:**
  - Authorization Type = At check in - will use CcAuthor messages to IFC8
  - Settlement type = On line - will use CcSettl messages to IFC8
Debit Card Type

This is used for card types where the authorization is not allowed, usually for Debit cards, Maestro, Girocard, V-Pay, any Mobile Payment card type (AliPay, PayPal) etc…

- **PMS Code** = 2-letter code – freely definable
- **IFC Credit card type** = 2-letter code as setup in OPI (e.g. MD for Maestro Debit)
- **Chip & Pin only** = active for Chip&Pin transaction
- **Authorization rule:**
  - Authorization Type = No Authorization
  - Settlement type = Online- will use CpPayOnly messages to IFC8