Oracle Banking Trade Finance Process Management Cloud Service

Product Release Features - Delta Security Guide

Release 14.8.0.0.0
G29905-01
April 2025

Oracle Banking Trade Finance Process Management Cloud Service Product Release Features - Delta Security Guide, Release 14.8.0.0.0

G29905-01

Copyright © 2025, 2025, Oracle and/or its affiliates.

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 is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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

Purpose vi
Audience vi
Documentation Accessibility vi
Diversity and Inclusion vi
Conventions vii
Related Documents vii
Structure vii

1 Export Documentary Collection Booking

1.1 Description 1-1
1.2 Category 1-1
1.3 Document References 1-1
1.4 Security Impact 1-1

2 Export Documentary Collection Update

2.1 Description 2-1
2.2 Category 2-1
2.3 Document References 2-1
2.4 Security Impact 2-2

3 Export Documentary Collection Liquidation

3.1 Description 3-1
3.2 Category 3-1
3.3 Document References 3-1
3.4 Security Impact 3-1

4 Export Documentary Collection Return/Close

4.1 Description 4-1
4.2 Category 4-1

4.3 Document References 4-1
4.4 Security Impact 4-1

5 Import Documentary Collection Update

5.1 Description 5-1
5.2 Category 5-1
5.3 Document References 5-1
5.4 Security Impact 5-2

6 Import Documentary Collection Liquidation

6.1 Description 6-1
6.2 Category 6-1
6.3 Document References 6-1
6.4 Security Impact 6-1

7 Import Documentary Collection Return/Close

7.1 Description 7-1
7.2 Category 7-1
7.3 Document References 7-1
7.4 Security Impact 7-1

8 Import LC Closure

8.1 Description 8-1
8.2 Category 8-1
8.3 Document References 8-1
8.4 Security Impact 8-2

9 Additional Attributes

9.1 Description 9-1
9.2 Category 9-1
9.3 Document References 9-1
9.4 Security Impact 9-1

10 Settlement Details

10.1 Description 10-1
10.2 Category 10-1
10.3 Document References 10-1

10.4 Security Impact 10-1

11 Tracer Facility in Import and Export Process

11.1 Description 11-1
11.2 Category 11-1
11.3 Document References 11-1
11.4 Security Impact 11-1

Preface

- Purpose
- Audience
  This guide is intended for Security Team and Product Development teams.
- Documentation Accessibility
- Diversity and Inclusion
- Conventions
- Related Documents
- Structure
  This manual is organized into the following chapters:

Purpose

This document provides security-related considerations / recommendations for Oracle Banking Trade Finance Process Management Cloud Service (OBTFPMCS). This guide may outline procedures required to implement or secure certain features, but it is also not a general-purpose configuration manual.

Audience

This guide is intended for Security Team and Product Development teams.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve.

Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Related Documents

For more information, you can refer to the following documents:

- Oracle Banking Trade Finance Process Management Pre Installation Guide
- Oracle Banking Trade Finance Process Management Services Installation Guide

Structure

This manual is organized into the following chapters:

- Preface gives information on the intended audience, structure, and related documents for this User Manual.
- The subsequent chapters provide an overview to the module.

1

Export Documentary Collection Booking

This topic consists of following sub-topics:

- Description
- Category
  New Functional requirement.
- Document References
- Security Impact

1.1 Description

Documentary collection is one of the common payment techniques used in international trade to facilitate import/export operations.A documentary collection is a trade transaction in which the seller (or exporter) instructs his bank to forward documents related to the export of goods to a buyer's bank with a request to present these documents to the buyer (or importer) for payment, indicating when and on what conditions these documents can be released to the buyer. In the process, the exporter hands over the task of collecting payment for goods supplied to his bank. The exporter or seller is the originator of the documentary collection. This user story describes how the Remitting Bank handles the documentary collection-booking request from the exporter.

1.2 Category

New Functional requirement.

1.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpageattachments.action?pageId=1918734652&metadataLink=true
User story board	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/F436E8DA224897EBF8A5AF81F6C3FF17C1177A968060/_UserStories
Design document	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/FCADF4E6D941D8258CC653D1F6C3FF17C1177A968060/_DesignDocs

1.4 Security Impact

SECURITY RISK	MITIGATION
SECURITY VULNERABILITIES	Input /output validations would be in place within the services, though it is INFRA component responsibility where ever required.

SECURITY RISK	MITIGATION
Broken Authentication & Session Management	Hard authorizations are introduced for each REST service calls. Session management is not applicable for REST services as they are stateless. JWT token based authentication is used for UI to consume Web APIs only for the known Users / Roles OAuth is introduced for Channel Integration to access the services
API Security	All the API requests are authenticated and used the principle of least privilege
SQL INJECTION	Features would ensure only parameterized queries are used and follow general coding best practices as per SCS guidelines
Security configuration on servers	Proper configurations are in place on application server (Docker, WebLogic server, SOA server, etc.)
DATA TAMPERING	Application has proper server side validations in place

2

Export Documentary Collection Update

This topic consists of following sub-topics:

- Description
- Category
  New Functional requirement.
- Document References
- Security Impact

2.1 Description

Documentary collection is one of the common payment techniques used in international trade to facilitate import/export operations.

A documentary collection is a trade transaction in which the seller (or exporter) instructs his bank to forward documents related to the export of goods to a buyer's bank with a request to present these documents to the buyer (or importer) for payment, indicating when and on what conditions these documents can be released to the buyer. In the process, the exporter hands over the task of collecting payment for goods supplied to his bank.

This user story describes how the Remitting Bank handles acceptance/non- acceptance or non- payment notification received from the collecting bank.

2.2 Category

New Functional requirement.

2.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpageattachments.action?pageId=1918734652&metadataLink=true
User story board	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/F436E8DA224897EBF8A5AF81F6C3FF17C1177A968060/_UserStories
Design document	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/FCADF4E6D941D8258CC653D1F6C3FF17C1177A968060/_DesignDocs

2.4 Security Impact

SECURITY RISK	MITIGATION
SECURITY VULNERABILITIES	Input /output validations would be in place within the services, though it is INFRA component responsibility where ever required.
Broken Authentication & Session Management	Hard authorizations are introduced for each REST service calls. Session management is not applicable for REST services as they are stateless. JWT token based authentication is used for UI to consume Web APIs only for the known Users / Roles OAuth is introduced for Channel Integration to access the services
API Security	All the API requests are authenticated and used the principle of least privilege
SQL INJECTION	Features would ensure only parameterized queries are used and follow general coding best practices as per SCS guidelines
Security configuration on servers	Proper configurations are in place on application server (Docker, WebLogic server, SOA server, etc.)
DATA TAMPERING	Application has proper server side validations in place

3

Export Documentary Collection Liquidation

This topic consists of following sub-topics:

- Description
- Category
  New Functional requirement.
- Document References
- Security Impact

3.1 Description

Documentary collection is one of the common payment techniques used in international trade to facilitate import/export operations.

A documentary collection is a trade transaction in which the seller (or exporter) instructs his bank to forward documents related to the export of goods to a buyer's bank with a request to present these documents to the buyer (or importer) for payment, indicating when and on what conditions these documents can be released to the buyer. In the process, the exporter hands over the task of collecting payment for goods supplied to his bank.

This user story describes how the Remitting Bank handles payment received from the collecting bank.

3.2 Category

New Functional requirement.

3.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpageattachments.action?pageId=1918734652&metadataLink=true
User story board	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/F436E8DA224897EBF8A5AF81F6C3FF17C1177A968060/_UserStories
Design document	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/FCADF4E6D941D8258CC653D1F6C3FF17C1177A968060/_DesignDocs

3.4 Security Impact

SECURITY RISK	MITIGATION
SECURITY VULNERABILITIES	Input /output validations would be in place within the services, though it is INFRA component responsibility where ever required.

SECURITY RISK	MITIGATION
Broken Authentication & Session Management	Hard authorizations are introduced for each REST service calls. Session management is not applicable for REST services as they are stateless. JWT token based authentication is used for UI to consume Web APIs only for the known Users / Roles OAuth is introduced for Channel Integration to access the services
API Security	All the API requests are authenticated and used the principle of least privilege
SQL INJECTION	Features would ensure only parameterized queries are used and follow general coding best practices as per SCS guidelines
Security configuration on servers	Proper configurations are in place on application server (Docker, WebLogic server, SOA server, etc.)
DATA TAMPERING	Application has proper server side validations in place

4

Export Documentary Collection Return/Close

This topic consists of following sub-topics:

- Description
- Category
  New Functional requirement.
- Document References
- Security Impact

4.1 Description

Documentary collection is one of the common payment techniques used in international trade to facilitate import/export operations.

A documentary collection is a trade transaction in which the seller (or exporter) instructs his bank to forward documents related to the export of goods to a buyer's bank with a request to present these documents to the buyer (or importer) for payment, indicating when and on what conditions these documents can be released to the buyer. In the process, the exporter hands over the task of collecting payment for goods supplied to his bank.

This user story describes how the Remitting Bank handles Return of documents due to non-acceptance/non-payment received from the collecting bank/importer.

4.2 Category

New Functional requirement.

4.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpageattachments.action?pageId=1918734652&metadataLink=true
User story board	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/F436E8DA224897EBF8A5AF81F6C3FF17C1177A968060/_UserStories
Design document	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/FCADF4E6D941D8258CC653D1F6C3FF17C1177A968060/_DesignDocs

4.4 Security Impact

SECURITY RISK	MITIGATION
SECURITY VULNERABILITIES	Input /output validations would be in place within the services, though it is INFRA component responsibility where ever required.

SECURITY RISK	MITIGATION
Broken Authentication & Session Management	Hard authorizations are introduced for each REST service calls. Session management is not applicable for REST services as they are stateless. JWT token based authentication is used for UI to consume Web APIs only for the known Users / Roles OAuth is introduced for Channel Integration to access the services
API Security	All the API requests are authenticated and used the principle of least privilege
SQL INJECTION	Features would ensure only parameterized queries are used and follow general coding best practices as per SCS guidelines
Security configuration on servers	Proper configurations are in place on application server (Docker, WebLogic server, SOA server, etc.)
DATA TAMPERING	Application has proper server side validations in place

5

Import Documentary Collection Update

This topic consists of following sub-topics:

- Description
- Category
  New Functional requirement.
- Document References
- Security Impact

5.1 Description

Documentary collection is one of the common payment techniques used in international trade to facilitate import/export operations.

A documentary collection is a trade transaction in which the seller (or exporter) instructs his bank to forward documents related to the export of goods to a buyer's bank with a request to present these documents to the buyer (or importer) for payment, indicating when and on what conditions these documents can be released to the buyer. In the process, the exporter hands over the task of collecting payment for goods supplied to his bank.

This user story describes how the Collecting Bank handles acceptance/non- acceptance or non- payment notification received from the importer and the same is communicated to the Remitting Bank.

5.2 Category

New Functional requirement.

5.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpageattachments.action?pageId=1918734652&metadataLink=true
User story board	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/F436E8DA224897EBF8A5AF81F6C3FF17C1177A968060/_UserStories
Design document	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/FCADF4E6D941D8258CC653D1F6C3FF17C1177A968060/_DesignDocs

5.4 Security Impact

SECURITY RISK	MITIGATION
SECURITY VULNERABILITIES	Input /output validations would be in place within the services, though it is INFRA component responsibility where ever required.
Broken Authentication & Session Management	Hard authorizations are introduced for each REST service calls. Session management is not applicable for REST services as they are stateless. JWT token based authentication is used for UI to consume Web APIs only for the known Users / Roles OAuth is introduced for Channel Integration to access the services
API Security	All the API requests are authenticated and used the principle of least privilege
SQL INJECTION	Features would ensure only parameterized queries are used and follow general coding best practices as per SCS guidelines
Security configuration on servers	Proper configurations are in place on application server (Docker, WebLogic server, SOA server, etc.)
DATA TAMPERING	Application has proper server side validations in place

6

Import Documentary Collection Liquidation

This topic consists of following sub-topics:

- Description
- Category
  New Functional requirement.
- Document References
- Security Impact

6.1 Description

Documentary collection is one of the common payment techniques used in international trade to facilitate import/export operations.

A documentary collection is a trade transaction in which the seller (or exporter) instructs his bank to forward documents related to the export of goods to a buyer's bank with a request to present these documents to the buyer (or importer) for payment, indicating when and on what conditions these documents can be released to the buyer. In the process, the exporter hands over the task of collecting payment for goods supplied to his bank.

This user story describes how the Collecting Bank handles payment under documentary collection received from the importer and the same is remitted to the Remitting Bank.

6.2 Category

New Functional requirement.

6.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpageattachments.action?pageId=1918734652&metadataLink=true
User story board	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/F436E8DA224897EBF8A5AF81F6C3FF17C1177A968060/_UserStories
Design document	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/FCADF4E6D941D8258CC653D1F6C3FF17C1177A968060/_DesignDocs

6.4 Security Impact

SECURITY RISK	MITIGATION
SECURITY VULNERABILITIES	Input /output validations would be in place within the services, though it is INFRA component responsibility where ever required.

SECURITY RISK	MITIGATION
Broken Authentication & Session Management	Hard authorizations are introduced for each REST service calls. Session management is not applicable for REST services as they are stateless. JWT token based authentication is used for UI to consume Web APIs only for the known Users / Roles OAuth is introduced for Channel Integration to access the services
API Security	All the API requests are authenticated and used the principle of least privilege
SQL INJECTION	Features would ensure only parameterized queries are used and follow general coding best practices as per SCS guidelines
Security configuration on servers	Proper configurations are in place on application server (Docker, WebLogic server, SOA server, etc.)
DATA TAMPERING	Application has proper server side validations in place

7

Import Documentary Collection Return/Close

This topic consists of following sub-topics:

- Description
- Category
  New Functional requirement.
- Document References
- Security Impact

7.1 Description

Documentary collection is one of the common payment techniques used in international trade to facilitate import/export operations.

A documentary collection is a trade transaction in which the seller (or exporter) instructs his bank to forward documents related to the export of goods to a buyer's bank with a request to present these documents to the buyer (or importer) for payment, indicating when and on what conditions these documents can be released to the buyer. In the process, the exporter hands over the task of collecting payment for goods supplied to his bank.

This user story describes how the Collecting Bank handles Return of documents as instructed by Remitting Bank due to non-acceptance/non-payment of the importer.

7.2 Category

New Functional requirement.

7.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpageattachments.action?pageId=1918734652&metadataLink=true
User story board	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/F436E8DA224897EBF8A5AF81F6C3FF17C1177A968060/_UserStories
Design document	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/FCADF4E6D941D8258CC653D1F6C3FF17C1177A968060/_DesignDocs

7.4 Security Impact

SECURITY RISK	MITIGATION
SECURITY VULNERABILITIES	Input /output validations would be in place within the services, though it is INFRA component responsibility where ever required.

SECURITY RISK	MITIGATION
Broken Authentication & Session Management	Hard authorizations are introduced for each REST service calls. Session management is not applicable for REST services as they are stateless. JWT token based authentication is used for UI to consume Web APIs only for the known Users / Roles OAuth is introduced for Channel Integration to access the services
API Security	All the API requests are authenticated and used the principle of least privilege
SQL INJECTION	Features would ensure only parameterized queries are used and follow general coding best practices as per SCS guidelines
Security configuration on servers	Proper configurations are in place on application server (Docker, WebLogic server, SOA server, etc.)
DATA TAMPERING	Application has proper server side validations in place

8

Import LC Closure

This topic consists of following sub-topics:

- Description
- Category
  New Functional requirement.
- Document References
- Security Impact

8.1 Description

Letters of Credit (LC) are one of the most versatile and secure instruments available to international traders.

A letter of credit is a commitment by a bank on behalf of the importer (foreign buyer) that payment will be made to the beneficiary (exporter), provided the terms and conditions stated in the letter of credit have been met, as evidenced by the presentation of specified documents.

LC issued by a Foreign Bank (Issuing Bank) can be advised, confirmed by the Beneficiary's Bank called as the Advising Bank.

During the validity of the Letter of Credit the beneficiary can initiate/request closure of the LC. This user story describes how the Issuing Bank handles Import LC closure in OBTFPMCS.

8.2 Category

New Functional requirement.

8.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpageattachments.action?pageId=1918734652&metadataLink=true
User story board	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/F436E8DA224897EBF8A5AF81F6C3FF17C1177A968060/_UserStories
Design document	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/FCADF4E6D941D8258CC653D1F6C3FF17C1177A968060/_DesignDocs

8.4 Security Impact

SECURITY RISK	MITIGATION
SECURITY VULNERABILITIES	Input /output validations would be in place within the services, though it is INFRA component responsibility where ever required.
Broken Authentication & Session Management	Hard authorizations are introduced for each REST service calls. Session management is not applicable for REST services as they are stateless. JWT token based authentication is used for UI to consume Web APIs only for the known Users / Roles OAuth is introduced for Channel Integration to access the services
API Security	All the API requests are authenticated and used the principle of least privilege
SQL INJECTION	Features would ensure only parameterized queries are used and follow general coding best practices as per SCS guidelines
Security configuration on servers	Proper configurations are in place on application server (Docker, WebLogic server, SOA server, etc.)
DATA TAMPERING	Application has proper server side validations in place

9

Additional Attributes

This topic consists of following sub-topics:

- Description
- Category
- Document References
- Security Impact

9.1 Description

In Trade Finance products, as per the bank's requirements additional fields can be incorporated. Such additional attributes are captured under Additional fields section in OBTFPMCS.

This user story describes how such additional attributes can created and used in OBTFPMCS.

9.2 Category

Enhancement.

9.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpageattachments.action?pageId=1918734652&metadataLink=true
User story board	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/F436E8DA224897EBF8A5AF81F6C3FF17C1177A968060/_UserStories
Design document	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/FCADF4E6D941D8258CC653D1F6C3FF17C1177A968060/_DesignDocs

9.4 Security Impact

SECURITY RISK	MITIGATION
SECURITY VULNERABILITIES	Input /output validations would be in place within the services, though it is INFRA component responsibility where ever required.
Broken Authentication & Session Management	Hard authorizations are introduced for each REST service calls. Session management is not applicable for REST services as they are stateless. JWT token based authentication is used for UI to consume Web APIs only for the known Users / Roles OAuth is introduced for Channel Integration to access the services

SECURITY RISK	MITIGATION
API Security	All the API requests are authenticated and used the principle of least privilege
SQL INJECTION	Features would ensure only parameterized queries are used and follow general coding best practices as per SCS guidelines
Security configuration on servers	Proper configurations are in place on application server (Docker, WebLogic server, SOA server, etc.)
DATA TAMPERING	Application has proper server side validations in place

10

Settlement Details

This topic consists of following sub-topics:

- Description
- Category
- Document References
- Security Impact

10.1 Description

Settlement accounts are accounts to be used for particular charges, LC/Bill value to be debited. The settlement accounts for different components are defined in the back office system. The same is simulated and displayed in OBTFPMCS. The user can check the details and if required, can change the corresponding payment details including the correspondent bank accounts.

This user story describes how the settlement details are handled in OBTFPMCS.

10.2 Category

Enhancement.

10.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpageattachments.action?pageId=1918734652&metadataLink=true
User story board	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/F436E8DA224897EBF8A5AF81F6C3FF17C1177A968060/_UserStories
Design document	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/FCADF4E6D941D8258CC653D1F6C3FF17C1177A968060/_DesignDocs

10.4 Security Impact

SECURITY RISK	MITIGATION
SECURITY VULNERABILITIES	Input /output validations would be in place within the services, though it is INFRA component responsibility where ever required.

SECURITY RISK	MITIGATION
Broken Authentication & Session Management	Hard authorizations are introduced for each REST service calls. Session management is not applicable for REST services as they are stateless. JWT token based authentication is used for UI to consume Web APIs only for the known Users / Roles OAuth is introduced for Channel Integration to access the services
API Security	All the API requests are authenticated and used the principle of least privilege
SQL INJECTION	Features would ensure only parameterized queries are used and follow general coding best practices as per SCS guidelines
Security configuration on servers	Proper configurations are in place on application server (Docker, WebLogic server, SOA server, etc.)
DATA TAMPERING	Application has proper server side validations in place

11

Tracer Facility in Import and Export Process

This topic consists of following sub-topics:

- Description
- Category
- Document References
- Security Impact

11.1 Description

Tracers are intimation or follow up messages sent to various parties in a Trade Finance transaction. This user story describes how tracers can be created and used in OBTFPMCS.

11.2 Category

Enhancement.

11.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpageattachments.action?pageId=1918734652&metadataLink=true
User story board	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/F436E8DA224897EBF8A5AF81F6C3FF17C1177A968060/_UserStories
Design document	https://oradocs-corp.documents.us2.oraclecloud.com/documents/folder/FCADF4E6D941D8258CC653D1F6C3FF17C1177A968060/_DesignDocs

11.4 Security Impact

SECURITY RISK	MITIGATION
SECURITY VULNERABILITIES	Input /output validations would be in place within the services, though it is INFRA component responsibility where ever required.
Broken Authentication & Session Management	Hard authorizations are introduced for each REST service calls. Session management is not applicable for REST services as they are stateless. JWT token based authentication is used for UI to consume Web APIs only for the known Users / Roles OAuth is introduced for Channel Integration to access the services
API Security	All the API requests are authenticated and used the principle of least privilege

SECURITY RISK	MITIGATION
SQL INJECTION	Features would ensure only parameterized queries are used and follow general coding best practices as per SCS guidelines
Security configuration on servers	Proper configurations are in place on application server (Docker, WebLogic server, SOA server, etc.)
DATA TAMPERING	Application has proper server side validations in place