Product Release Features - Delta Security Guide
Oracle Banking Trade Finance Process Management
Release 14.5.4.0.0
Part No. F53382-01
[February] [2022]

Delta Security Guide

Table of Contents

1. About this Manual

1.1 Introduction

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

1.2 Purpose

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

1.3 Audience

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

2. Export Documentary Collection Booking

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.
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.

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 Update

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 acceptance/non- acceptance or non-payment notification 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.
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 Liquidation

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 payment received from the collecting bank.

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.
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. Export Documentary Collection Return/Close

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

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 Update

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 acceptance/non- acceptance or non-payment notification received from the importer and the same is communicated 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.
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 Liquidation

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 payment under documentary collection received from the importer and the same is remitted to the Remitting Bank.

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.
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 Documentary Collection Return/Close

8.1 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.

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. Import LC Closure

9.1 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 OBTFPM.

9.2 Category

New Functional requirement

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
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. Additional Attributes

10.1 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 OBTFPM.

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

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.
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. Settlement Details

11.1 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 OBTFPM. 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 OBTFPM.

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
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.

12. Tracer Facility in Import and Export Process

12.1 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 OBTFPM.

12.2 Category

Enhancement

12.3 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

12.4 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.

Security Delta Guide
[February] [2022]
Version 14.5.4.0.0
Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India
Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax: +91 22 6718 3001
www.oracle.com/financialservices/