Product Release Features -Delta Security Guide

Oracle Banking Trade Finance Process Management

Release 14.3.0.0.0

[May] [2019]

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 LC Amendment

2.1 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.

The advised LC can be further amended on request from the Issuing Bank.
This user story describes how the Advising Bank handles an amendment to an Export LC in OBTFPM.

2.2 Category

New Functional requirement

2.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpage.action?pageId=1215777237
User story board	https://confluence.oraclecorp.com/confluence/display/TMOS/User+Story
Design document	https://confluence.oraclecorp.com/confluence/display/TMOS/Design+Document

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 LC Amendment Beneficiary Consent

3.1 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. The advised LC can be further amended on request from the Issuing Bank. In many cases, the beneficiary's consent to that amendment is required to make the amendment operative.

This user story describes how the Advising Bank handles beneficiary response to an amendment to Export LC in OBTFPM

3.2 Category

New Functional requirement

3.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpage.action?pageId=1215777237
User story board	https://confluence.oraclecorp.com/confluence/display/TMOS/User+Story
Design document	https://confluence.oraclecorp.com/confluence/display/TMOS/Design+Document

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 LC Drawings

4.1 Description

The exporter (beneficiary) on receipt of an LC will ship the goods and submit the documents required under the LC with the negotiating bank. Drawings under Export LC deals with handling the documents received from the beneficiary of an LC by the Negotiating bank. The drawings can be for the full value or for part value of the LC based on whether multiple drawings are allowed as per LC terms.

4.2 Category

New Functional requirement

4.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpage.action?pageId=1215777237
User story board	https://confluence.oraclecorp.com/confluence/display/TMOS/User+Story
Design document	https://confluence.oraclecorp.com/confluence/display/TMOS/Design+Document

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 LC Update Drawings

5.1 Description

Update of Drawings under Export LC deals with making updates to a drawing already booked in the date can happen because of

a. Receiving Response for Discrepancies / Notification of Discrepancies (MT 752, MT 732, and MT 734).

b. Changes to the drawing information received from the Beneficiary on account of additional documents/ replacement documents.

c. Registering Acceptance of Usance Drawings.

5.2 Category

New Functional requirement

5.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpage.action?pageId=1215777237
User story board	https://confluence.oraclecorp.com/confluence/display/TMOS/User+Story
Design document	https://confluence.oraclecorp.com/confluence/display/TMOS/Design+Document

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. Export LC Liquidation

6.1 Description

Export LC Liquidation is initiated when the proceeds for the drawing are received from the issuing bank/ reimbursing bank.

6.2 Category

New Functional requirement

6.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpage.action?pageId=1215777237
User story board	https://confluence.oraclecorp.com/confluence/display/TMOS/User+Story
Design document	https://confluence.oraclecorp.com/confluence/display/TMOS/Design+Document

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 Collection Booking

7.1 Description

The handling of import documents by the collecting bank is taken care in this process. An exporter submits the documents direct to the Collecting bank or through his bank (Remitting Bank) to the collecting bank for collection of proceeds from the importer. The collecting bank in turn will handle the documents for collection as instructed by the drawer/ remitting bank.

7.2 Category

New Functional requirement

7.3 Document References

Business Requirement document	https://confluence.oraclecorp.com/confluence/pages/viewpage.action?pageId=1215777237
User story board	https://confluence.oraclecorp.com/confluence/display/TMOS/User+Story
Design document	https://confluence.oraclecorp.com/confluence/display/TMOS/Design+Document

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.

Security Delta Guide
[May] [2019]
Version 14.3.0.0.0

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/

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 failsafe, 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.

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.

This software or hardware and documentation may provide access to or information on 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. 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.