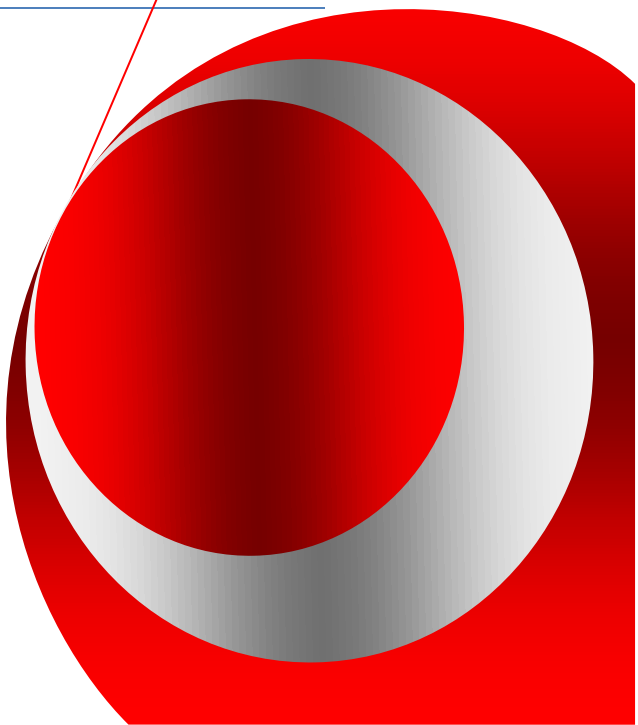
Security Measures in FLEXCUBE

Private Banking



Document Version Control

Document Name	Security measures - FLEXCUBE Private Banking	
Organization	Oracle Financial Services and Software Ltd.	
Version Number	1.0	☐ Draft ☑ Final
Last Modified	10-Sep-2017	
Document Author	Mahendran Pandian	

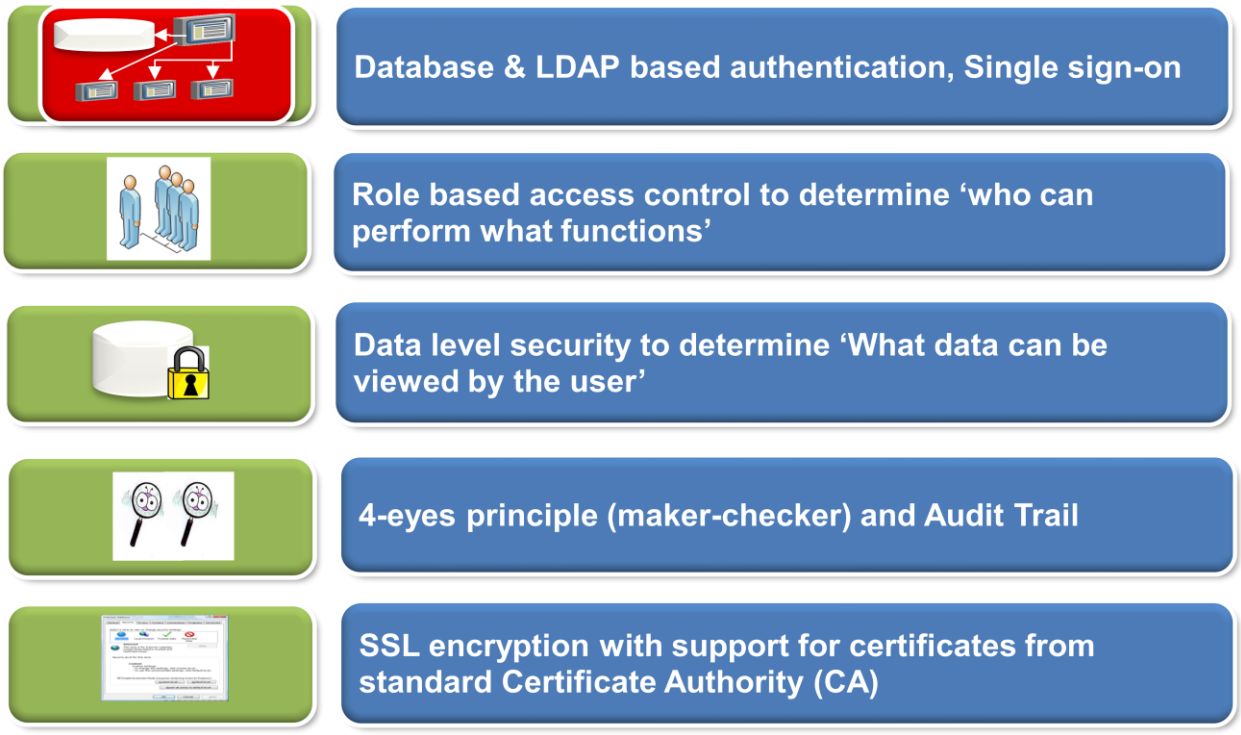
Document Revision History			
Revision Date	**Reviser**	**Reviewer**	**Changes Performed**
06-AUG-2013	Mahendran	Rajeev Radhakrishnan	External document links are updated
06-Sep-2017	Prakash Parte	Orjun Thengdi	Updated document for cookies used in application

Table of Contents

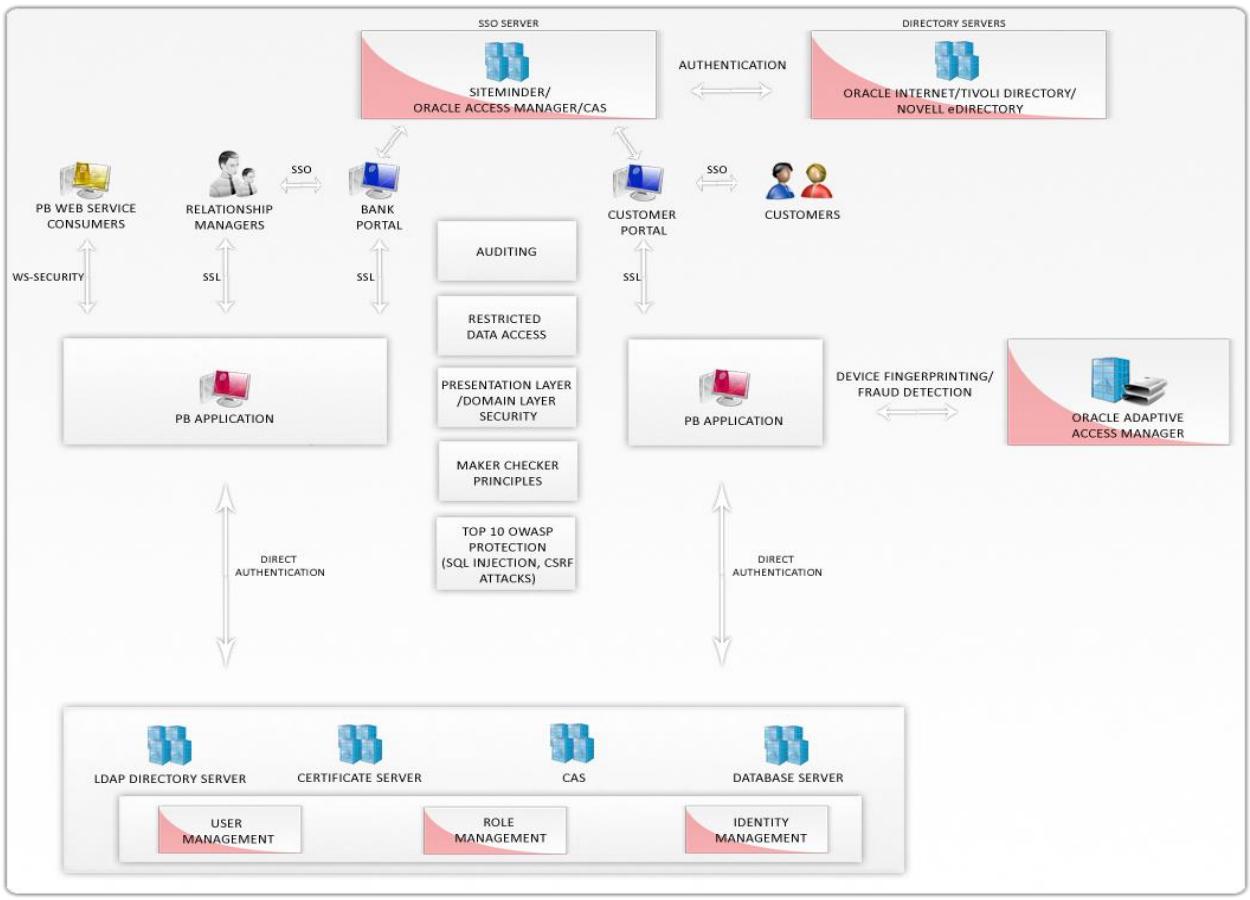
Details of FLEXCUBE Private Banking Security Measures

1. Overview

This document covers FCPB security Key Features. FCPB follows the security measures to protect the system and customer data.



1.1.1 Security Architecture Diagram



2. Validation

FCPB mainly has four types of validations.

1. Client side JavaScript validation
2. Server side hard coded validation
3. Server side annotation based validation.
4. Server side validation framework (SVF)
    - JavaScript Validation:

FCPB uses prototype JavaScript library for accessing DOM, binding events and DWR framework for making and processing Ajax requests and responses. Prototype JS executes the respective JS functions while the registered events (change/blur/click/submit etc) have been triggered.

- Server side hard coded validation:

FCPB Server side validations are java based, and these validations hardcoded in java classes at web and service layers.

- Server side annotation based validation:

Annotation based validations are mainly used to prevent the security breaches by intercepting and changing the critical request attributes.

Currently the annotations being used only at Order Managements action classes and DWR proxy classes. Refer given link for more detail

http://ofss220012.in.oracle.com:18080/svn/FCPBS_REPOSITORY/trunk/PWM Documents/Design/Architecture/Framework Documents/FCPB_Data_Validation_Framework.docx

- Server side validation framework:

FCPB server side validation framework (SVF) is a XML based configurable plug and play framework for doing the input validation and business validation as well. Using server side validations, users/consultants can configure the validations using Regular expressions, SQL queries and pre-existing java methods.

Currently the SVF is implemented only for Order Management and Transaction Management screens only. Refer the given link for more detail.

http://ofss220012.in.oracle.com:18080/svn/FCPBS_REPOSITORY/trunk/PWM Documents/Design/Architecture/Framework Documents/FCPB_Server_Side_validations.docx

2.1 White list

All UI based JS validations and SVF are regular expression based white list validations.

2.2 Blacklist

FCPB Server side XSS filter is regular expression based black list validation.

3. Session Management

In FCPB, when the user accesses the login page, application server creates a session, and after successful login the session used for login being invalidated and new session created to prevent the session fixation.

3.1 Cryptography used

FCPB uses SHA256 hashing technique for hashing the user's password, for other encryption needs, uses AES encryption standards.

3.2 Session storage

In FCPB very little non sensitive information being stored in session and destroyed while the session is being invalidated.

3.3 Session logging

FCPB maintains the user's login time (ie, session creation) and while the user logs out/ session being invalidated, the logout time being maintained in login audit table also any invalid login attempts being stored in login audit table.

3.4 Cookies used

FCPB uses following cookies to manage user session and its data during interaction with application.

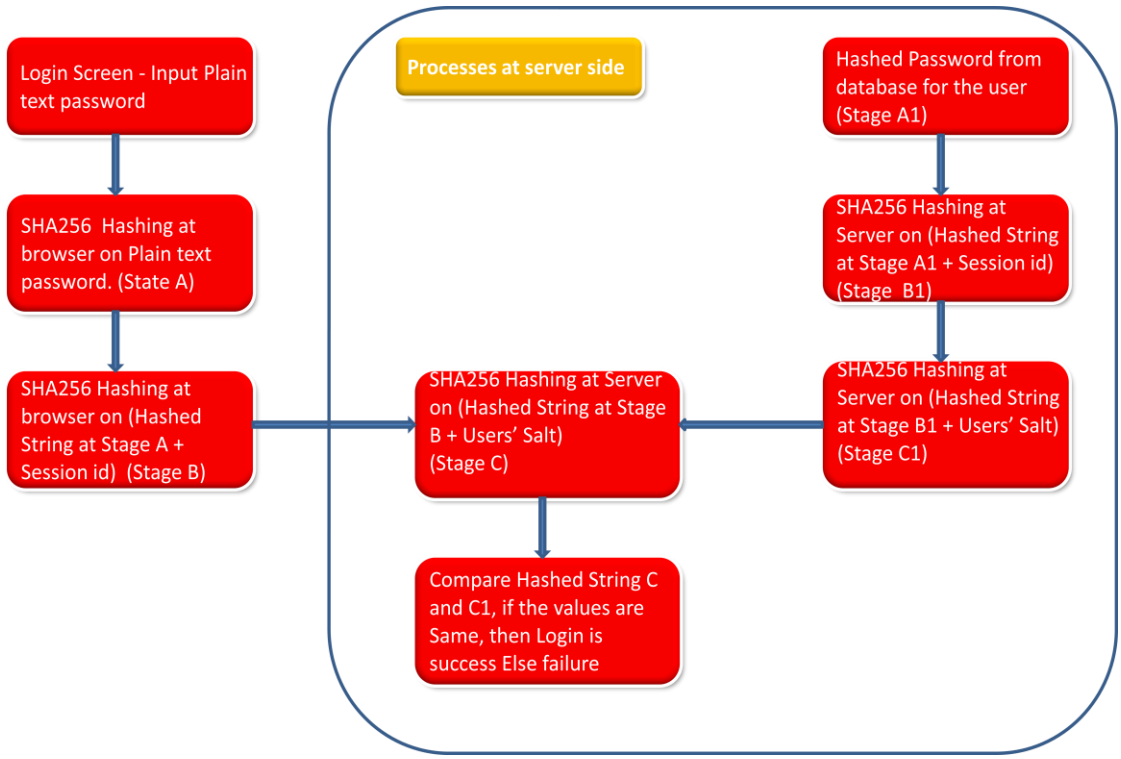
If we disable this cookies application will not function normally, user will not be able to login.

Cookie Name	Usage
JSESSIONID	Used to store user login session information
RANDOM	Used to store session token information

4. Password Management

In FCPB user's password are Hashed using SHA256 and stored in database tables. The password expires automatically based on Number of days to expire" maintained in business parameter table. User account will be locked while the user enters the wrong password continuously based on the number of number of wrong password maintained in business parameter.

Refer the following diagram for Password validation in FCPB.



5. Exception/Error handling

Refer the document:

http://ofss220012.in.oracle.com:18080/svn/FCPBS_REPOSITORY/trunk/PWM Documents/Design/Architecture/Framework Documents/FCPBS_Exception Handling.docx

6. Logging

Refer the document:

http://ofss220012.in.oracle.com:18080/svn/FCPBS_REPOSITORY/trunk/PWM%20Documents/Design/Architecture/Framework%20Documents/FCPBS_Logging.docx

7. Plans for upcoming releases

1. Server side validation framework will be implemented for all the screens of FCPB.

8. Conclusion

Good security practice does not end after installation. Continued maintenance tasks include:

- Install the latest software patches.
- Install latest operating system patches.
- Verify user accounts - delete or lock accounts no longer required.
- Run security software and review output.
- Keep up to date on security issues by subscribing to security mailing lists, reading security news groups and following the latest security procedures.
- Install Tripwire to detect changes to files
- Monitor log files including btmp, wtmp, syslog, sulog, etc. Consider setting up automatic email or paging to warn system administrators of any suspicious behavior. Also check the snort logs.