eMudhra emCA
Security Target
TOE Version: V4.0.3

Document Version 7.3
November 02, 2021

Prepared for:
eMudhra Limited
Sai Arcade, 3rd Floor, No.56,
Outer Ring Road, Devarabeesanahalli,
Bangalore - 560103

Copyright

Disclaimer

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between eMudhra and the customer. However, eMudhra has made all reasonable efforts to ensure that the instructions contained in the document are adequate and free of material errors and omissions. eMudhra will, if necessary, explain issues, which may not be covered by the document.

Feedback

eMudhra welcomes customer comments as a part of the process of continuous development and improvement of the documentation.

Trademarks and Registered Trademarks

Products and product names mentioned in this document may be trademarks or registered trademarks of their individual proprietors.

Published by
eMudhra
www.emudhra.com | info@emudhra.com

Table of Contents

1 ST Introduction (ASE_INT)

1.1 ST Reference

ST title	eMudhra emCA v4.0.3 Security Target
Version	v 7.3
Author	eMudhra Limited
Date	November 2, 2021

1.2 TOE Reference

TOE identification	eMudhra emCA
Version	v 4.0.3
Build no.	32512
Release date	07/06/2021

1.3 TOE Overview

emCA is a comprehensive certificate life-cycle management software that helps organisations to setup digital certificate issuance platform for generating various types of digital certificates that can be used in used in wide variety use PKI use cases. emCA is platform agnostic i.e. it is compatible with Operating systems such as Windows and Linux, applications servers such as Tomcat, Weblogic etc and database servers such as MySQL, DB2, MS SQL etc. But under CC scope of evaluation, emCA was tested on Windows OS with Tomcat application server and MySQL Database.

1.3.1 TOE usage and major security features

emCA is an enterprise-class Public Key Infrastructure (PKI) certificate life-cycle management software application for large enterprises built on Jakarta Enterprise Edition (JEE) technology. emCA is to be deployed within a networked and physically secure environment.

emCA consists of two components i.e. emCA application and emCA websocket. emCA application performs the core functionality of PKI certificate life-cycle management. It is deployed within a server machine and works with a Hardware Security Module (HSM) (out of TOE scope). The HSM is required to

- generate and store cryptographic keys.
- perform cryptographic operations such as generate certificates and sign CRLs.

emCA websocket is deployed within a client machine. emCA websocket facilitates user interaction with emCA application via a web browser. Both the emCA application and emCA websocket requires a set of external IT products to support their overall functionality. Figure 1 illustrates an abstraction of the relationship between emCA application and emCA websocket.

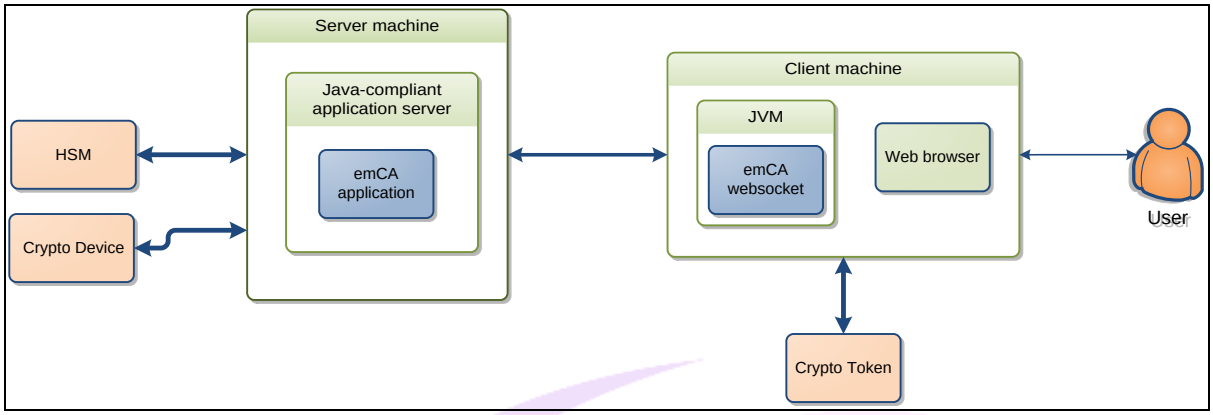

Figure 1: TOE usage

emCA supports the following security functionalities. Users can access these security functionalities via a web browser on the client machine facilitated by the emCA websocket:

- User data protection
  - Certificate management
  - Certificate and CRL profile management
  - Certificate and CRL integrity protection
- Identification and authentication.
- Security audit.
- Export and import user and TSF data.
  - Certificate Signing Request (CSR)
  - Certificate Revocation List (CRL)
  - CA Certificates
  - Certificate owners' certificates
  - User certificates
  - Audit logs
  - TOE configurations.
- Password policy
- Cryptographic operation
- Security management.
  - Roles and user management[1]
  - Audit management
  - Integrity protection for exported backup archives

1.3.2 TOE Type

emCA is a PKI certificate life-cycle management software application.

1.3.3 Required non-TOE hardware/software/firmware

The table below states the hardware and software requirements to support emCA operations.

Hardware

[1] User profile creation with soft token is out of TOE scope.

Application Server	Processor	Quad core processors
	RAM	8 GB
	HDD	200 GB
Database	Processor	Quad core processors
	RAM	8 GB
	HDD	500 GB SAS HDDs
HSM	PKCS #11 compliant	
Crypto Token	PKCS #11 compliant	
Software		
OS	Windows Server 2012 or higher version for emCA application Windows 10 for emCA websocket	
Application Server	Apache Tomcat 9.0.30 or higher	
Database	MySQL Community Server 5.1.55 or higher version	
JDK	Oracle JDK 11	
Crypto token	PKI client	
LDAP	Open LDAP v2.4	
FTP	FTP v2.4 (64 bit)	

Table 1: Hardware and software requirements

The following sections elaborate how each non-TOE component supports emCA operations. Figure 2 provides an overview of how the various non-TOE components interact and supports emCA operations:

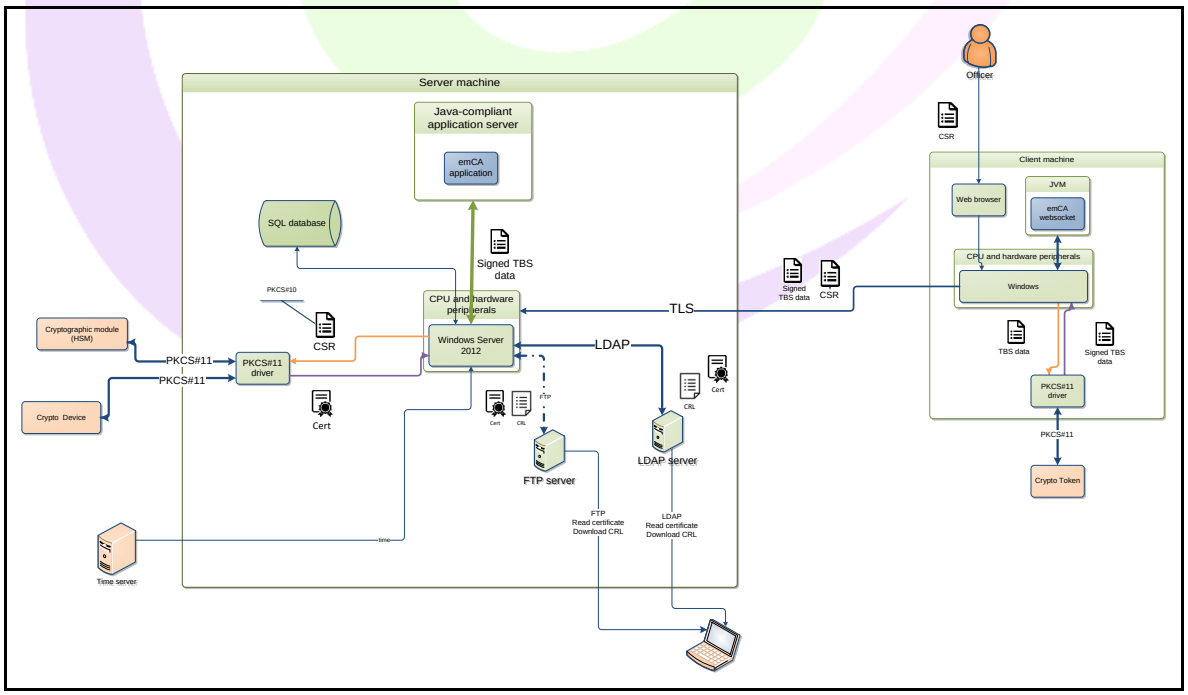

Figure 2: Non-TOE components

1.3.3.1 Java-compliant Application Server

emCA application being a Java-based application can be deployed on a Java-compliant application server, which provides several resources and services to emCA application, namely:

- Database connectivity services (e.g. object mappings and connection pooling).
- Component creation and management (e.g. Session bean pooling and life-cycle management)
- Communication interfaces (e.g. HTTP/HTTPS and JEE).

These resources and services not only make development and maintenance more efficient, but also enable high performance, scalability, and availability.

1.3.3.1.1 Lightweight Directory Access Protocol (LDAP) Server

The emCA application can publish certificates and CRLs to LDAP servers. The emCA application uses LDAP for connecting to the LDAP server where the certificates and CRLs are maintained.

1.3.3.2 File Transfer Protocol (FTP) Server

The emCA application can publish certificates and CRLs to FTP servers. The emCA application uses FTP for connecting to the FTP server where the certificates and CRLs are maintained.

1.3.3.3 SQL Database

An SQL database is the default data storage of emCA application. emCA application stores the following information in the SQL database:

- Certificate Profile
- Key Profile
- CRL Profiles
- CRL Publication information
- Certificate Revocation information
- CRLs and Public Key Certificates
- emCA Application license information
- emCA TOE user registration data and roles
- Service configuration
- Approval information
- CA instance configuration
- TOE configuration
- emCA user hard token information and issuer configuration (e.g. Information about crypto tokens issued to emCA users)
- Authentication data, such as emCA TOE user information
- Audit logs of all security relevant operations

1.3.3.4 Java Virtual Machine

emCA websocket is developed in Java programming language and, as such, runs in a Java Virtual Machine (JVM). Additionally, since the JVM specifications are public, it can be implemented by independent vendors.

1.3.3.5 PKCS #11 Driver

PKCS #11 is the programming interface to interact with cryptographic tokens and HSM. PKCS #11 allows emCA users to access cryptographic operations and cryptographic materials that are stored in the cryptographic tokens and HSM.

1.3.3.6 Windows and Windows Server Operating System (OS)

The emCA websocket and emCA application runs on JVM and application server, respectively. In turn, JVM and application server runs on Windows and Windows Server, respectively.

1.3.3.7 Time Server

emCA application requires reliable time source to generate certificate profile and certificates (Root, CA and User) and generate audit logs.

1.3.3.8 CPU and hardware peripheral

CPU and hardware peripheral are the underlying hardware platform that runs Windows and Windows Server OS.

1.3.3.9 HSM

emCA application relies on the HSM to generate/store cryptographic key material and perform cryptographic operations such as generate certificates and sign CRLs.

1.3.3.10 Cryptographic Token

Each emCA user carries a cryptographic token. The cryptographic token generates/stores cryptographic material and performs cryptographic operations such as key generation and digital signature generation. The emCA websocket interacts with the cryptographic token as part of user identification and authentication to emCA application.

1.3.3.11 emCA Token

HSM password and Secret Key (HMAC-SHA256 key for MAC generation) is stored encrypted in the emCA application's external database. This cryptographic token is required to encrypt/decrypt the HSM password and Secret Key that is stored in the emCA Configuration file.

1.4 TOE Description

1.4.1 Physical Scope

The TOE consists of two components i.e. emCA application and emCA websocket – these components shall be collectively known as the TOE in the subsequent sections of this document. emCA application is a Java application that provides the core functionality of certificate life-cycle management. emCA websocket is a Java application that facilitates user interaction with emCA application via a web browser. Figure 2 illustrates the physical scope of the TOE.

The table below lists the TOE deliverables and their corresponding delivery methods.

Items	Description	Format	Delivery method
Preparative user guidance	eMudhra Certificate Authority Preparative Procedures (AGD_PRE), Version 2.0, June 15th 2021	PDF	By hand in the form of CD or by email
Operational user	eMudhra Certificate Authority	PDF	By hand in the form of

guidance	Operational User Procedures (AGD_OPE), Version 1.0, May 4th 2021		CD or by email
Utility manual	emCACertificateUtility Manual, Version 1.0, 2021	PDF	By hand in the form of CD or by email
emCA application Solution	emCAv4Solution Folder contains following sub folders and files: • Folder: emCA-> Sub Folders: ○ Sub Folder: CertificateProfile ○ Sub Folder: emCAPKSC11 ○ Sub Folder: emCAProperties -> config.properties & log4j.xml ○ Sub Folder: emCAWebsocket -> Files: emCAWebscoket.msi ○ Sub Folder: emCACertificateUtility->File CertMgr2021.cer emCACertificateUtility.jar eToken.cfg ServerToken.cfg Token.cfg ○ Sub Folder: LocalRepositoryForCRL ○ Sub Folder: logs • Folder: emCADBScripts -> Files: DatabaseUsersCreation_emCA.sql, Createtables_emCA.sql GrantAccess_emCA.sql • Folder: emCAPKCS11Sample -> Files: HSMPKCS11.cfg • Folder: emCASRC-> Files: emCA.war • Folder: SignatureVerifier-	war,jar, cfg, xml, sql, MSI	By hand in the form of CD

	SetupFiles -> File: SignatureVerifier.msi		
Cryptographic token for CA administrator	Not applicable	Hardware	By hand.
emCA crypto device	Not applicable	Hardware	By hand.

Table 2: TOE deliverables and delivery methods

1.4.2 Logical Scope

This section describes the logical security features of TOE.

1.4.2.1 User data protection

emCA application enforces access control using predefined roles i.e. CA Administrator, Administrator, Officer, Auditor and Operator. Each role has predefined access rights as shown in Table 3. In the context of CC, these roles are also known as subjects.

Role	Access rights
CA Administrator	Initial setup and configure recover the TOE. Restore TOE – import user and TSF data Create and manage Administrator accounts. Search user and CA certificates. View Reports. Key Generation[2](AES256 key and Signing Key) Define 'm' out of 'n' authentication matrix
Administrator	Configure certificate and CRL profiles. Configure key profiles Audit management. Search user and CA certificates. Certificate and CRL Management. View Reports. Create and manage Officer, Auditor and Operator accounts. Key store management (out of TOE scope)
Operator	Perform TOE backup – export user and TSF data
Officer	Key generation for enrolment of user and CA certificates (out of TOE scope). Sign CSR (out of TOE scope). Revoke, suspend and reinstate user certificates. Revoke CA certificates. Reinstate user certificates. Search user and CA certificates Create, manage, update, publish and certificate and CRL. Key management (out of TOE scope) View reports Request or approve certificates.
Auditor	View and manage audit logs

Table 3: Roles

[2] Key generation resides on the external HSM; thus, this function is out of TOE scope, however, the TOE controls access to this function

1.4.2.1.1 Certificate and CRL Management

As an enterprise-class Certificate Life-cycle Management software, emCA application can maintain the several CA and user certificate profiles in the same emCA application instance. The emCA application stores the CA and user certificates in the external database. The emCA application

- works with HSM (out of TOE scope) to issue, reissue, renew, revoke, suspension, reinstate and delete certificates and generate CRLs.
- reports certificate status.
- can publish on LDAP or FTP servers.
- allows users can view certificates and CRLs.

1.4.2.1.2 Certificate, CRL and Key profile management

Certificate and CRL profiles store X.509 certificate and CRL attributes such as fields, extensions, cryptographic algorithms, key sizes, key usage, certificate lifetime and default values. emCA application allows users to create, view, edit, delete, export the X.509 certificates and CRLs profiles.

Similarly, key profiles contain attributes such as user key algorithm and size, certificate signature algorithm, created date, key store, etc. emCA application allows users to create, view, edit, delete, and export these key profiles.

Users use these profiles as templates for creating certificates and CRL.

1.4.2.1.3 Certificate and CRL integrity protection

The certificate owner's and CA certificates and CRL stored in the external database are protected by HMAC-SHA256 digest. Each time the emCA application loads the certificate owner's and CA certificate or CRL as requested by users, the emCA application verifies the integrity of these information using the HMAC-SHA256 digest that are appended to them.

1.4.2.2 Identification and Authentication.

The TOE enforces Challenge-Response protocol for user identification and authentication. For user identification and authentication, the TOE requires the user to insert the user's cryptographic token into the client machine. The emCA application in the server machine then issues a challenge to the (user + cryptographic token) on client machine facilitated by the emCA websocket. In turn, the (user + cryptographic token) return a response. If emCA application determines that the response is expected, the user shall have access to appropriate services as depicted in Table 3.

1.4.2.3 Security Audit

The emCA application generates audit logs for user actions, user authentication failures, and modifications to configuration. The audit logs are digitally signed real-time by the HSM (out of TOE scope) to protect data integrity. The audit logs are stored in the external database. emCA application also allow users to check the integrity and review the audit logs. Integrity protection of audit logs is enforced by the HSM (out of TOE scope) using digital signature.

1.4.2.4 Password Policy

The emCA application enforces pre-defined password policy on the token PIN and PDF password.

1.4.2.5 Export and import user and TSF data

emCA application allows export and import of user and TSF data. They are as follows:

Data	Description	Data type
CSR	This is submitted by the Officer to the emCA application for issuance of certificate. The issuance of certificate is done by HSM (out of TOE scope). CA CSR can also be generated and exported by emCA application.	User data
CRL	A CRL contains the list of revoked and suspended certificates – it determines the validity of a certificate owner's or CA certificate.	User data
CA certificates	Certificates contain information to prove the identities of CA.	User data
Certificate owners' certificates	Certificates contain information to prove the identities of certificate owners.	User data
User certificates	Certificates that are used as part of TOE user identification and authentication	TSF data
Audit log	Record of auditable events.	TSF data
TOE configuration	The rest of TOE configuration that affects the TOE security behaviour.	TSF data

Table 4: Export and import of user and TSF data.

1.4.2.6 Cryptographic operation

The emCA application performs HMAC-SHA256 generation and verification on trust store (consists of certificate owner's certification, user's certificates, CA certificates and CRL), security audit logs, backup and restore archives to protect the integrity of these assets.

1.4.2.7 Security management

1.4.2.7.1 Roles and user management[3]

emCA application has predefined roles i.e. CA Administrator, Administrator, Officer, Operator and Auditor. emCA application allows the creation and management of user accounts based on the hierarchy depicted in Figure 3. In the context of CC, these roles are also known as subjects.

In addition, CA administrator can

- define M of N authentication matrix for each role during the initial setup process.
- manage the Administrator roles by making each user account active or inactive and its related security attributes.

Similarly, Administrator can manage the Officer, Operator and Auditor role by making each user account active or inactive and their related security attributes.

[3] User profile creation using soft token is out of TOE scope.

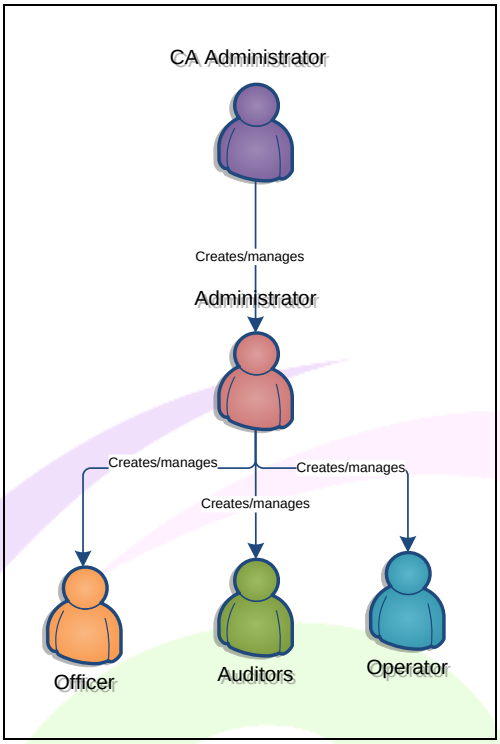

Figure 3: Role hierarchy

1.4.2.7.2 Audit Management

emCA application allows users to view and export audit logs.

1.4.2.7.3 Integrity protection for exported backup archives

emCA application generated HMAC-SHA256 digest for exported backup archives and as well as password protected. When backup archives are required to be imported by the emCA application to restoration purpose, the emCA application shall verify the HMAC-SHA256 digest & password that is appended to the backup archive to ensure its integrity.

2 Conformance Claims (ASE_CCL)

2.1 CC Conformance

The Security Target and its TOE conforms with:

- Common Criteria Information Technology Security Evaluation Version 3.1, Revision 5
  - Part 2 conformant[CC2]
  - Part 3 conformant[CC3]

2.2 PP Conformance

The Security Target and its TOE does not conform to any Protection Profile (PP).

2.3 Package Conformance

The Security Target and its TOE conforms to Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.2 component.

3 Security Problem Definition (ASE_SPD)

3.1 Introduction

This section shall define TOE's assets, subjects, external entities, and threat agent.

3.1.1 Assets

Name	Description	Type of protection
CSR	Certificate owners' CSR are submitted by the Officer to the emCA application for issuance of certificate. The issuance of certificate is done by HSM (out of TOE scope). CA CSR can also be generated and exported by emCA application.	Integrity
Username and user token PIN	This is entered into the web browser during user identification and authentication by the emCA application.	Confidentiality
emCA crypto device PIN	The emCA crypto device stores the private key that is used to encrypt the HSM password that is stored in the emCA application's external database. The emCA crypto device PIN is required for the user to authenticate to the emCA crypto device. Once the user is authenticated, the emCA crypto device shall decrypt the encrypted HSM password. In turn, the decrypted HSM password is used to authenticate the emCA application to the HSM. The emCA crypto device PIN is a transient data. The emCA crypto device PIN is also used to decrypt the encoded & encrypted HMAC key present in emCA configuration file, emCA key is also required for signing the emCA login users certificate.	Confidentiality
HSM password	This is required by emCA application to access the cryptographic operations provided by the HSM (out of TOE scope).	Confidentiality
PDF password	The emCA application password-protect the exported PDF reports with this password. This is a transient data.	Confidentiality
Zip password	The emCA application password-protect the exported backup archive with this password. This is a transient data.	Confidentiality
LDAP password	This is required by emCA application to authenticate itself to the LDAP server.	Confidentiality
Remote system password	This is required by emCA application to authenticate itself to a remote backup server where backup archives are stored.	Confidentiality
Database password	This is required by emCA application to authenticate itself to the SQL database.	Confidentiality
CA certificates	Certificates contain information to prove the identities of CA.	Integrity
Certificate owners' certificates	Certificates contain information to prove the identities of certificate owners.	Integrity
Status of CA and	This reflects the i.e. active, suspend or revoked status of CA	Integrity

certificate owners' certificates	and certificate owners' certificates	
CRL	A CRL contains the list of revoked and suspended certificate owners' certificates – it determines the validity of a certificate owner's certificate.	Integrity
Certificate, CRL and Key profile	These profiles determine the attributes that a given certificate or CRL should contain.	Integrity

Table 5: User data

Name	Description	Type of protection
User certificates	Certificates that are used as part of TOE user identification and authentication	Integrity
Audit log	Record of auditable events.	Integrity
Username-role association information	Contains information related to username and role association. This would control TOE access control behaviour.	Integrity
Authentication matrix	This determines the number of users of each role that are required to be present to perform identification and authentication to emCA application.	Integrity
TOE configuration	The rest of TOE configuration that affects the TOE security behaviour.	Integrity

Table 6: TSF data

3.1.2 Subjects

The subjects that the TOE can perceive are shown below. A TOE user is associated to one of these subjects. Please see section 10.1 of Annex for more details on the role-based access control matrix.

Subjects	Access rights
CA Administrator	Install and configure recover the TOE. Restore TOE – import user and TSF data Create and manage Administrator accounts. Search user and CA certificates. View Reports. Key Generation [4](AES256 key and Signing key) Define 'm' out of 'n' authentication matrix
Administrator	Configure certificate and CRL profiles. Configure key profiles Audit management. Search user and CA certificates. Certificate and CRL Management. View Reports. Create and manage Officer, Auditor and Operator accounts. Key store management (out of TOE scope[5])

[4] Key generation resides on the external HSM; thus, this function is out of TOE scope, however, the TOE controls access to this function

[5] Key store function resides on the external HSM; thus, this function is out of TOE scope, however, the TOE controls access to this function.

Operator	Perform TOE backup – export user and TSF data
Officer	Key generation for enrolment of user and CA certificates (out of TOE scope). Sign CSR (out of TOE scope[6]). Revoke, suspend and reinstate user certificates. Revoke CA certificates. Reinstate user certificates. Search user and CA certificates Create, manage, update, publish and certificate and CRL. Key management (out of TOE scope[7]) View reports Request or approve certificates.
Auditor	View and manage audit logs

Table 7: Subjects

3.1.3 External entities

External entity	Description
System administrator	This human entity may or may not be a user of the TOE, however, it is a collective entity who is responsible for the setting up and management of the IT environment.
Certificate owner	The human or IT entity that is a non-TOE user but submits CSR to TOE users for certificate signing by the (TOE + HSM) i.e. the Certificate Authority.
User	The human entity that uses the TOE a.k.a. TOE user. The entity assumes one of the roles within the TOE i.e. CA Administrator, Administrator, Officer, Auditor and Operator.

Table 8: External entities

3.1.4 Threat agent

Threat agent	Description
Attacker	A human or IT entity that does not hold any authorized role to operate or interact with the TOE. This entity may operate through the remote or local interfaces of the TOE. Examples of this threat agent are unauthorized TOE user, cybercriminals, and hackers in general.

Table 9: Threat agent

3.1.5 Threat scenario

Figure 4 illustrates the intended threat scenario in which the subsequent sections of SPD are based on; the attacker only has access to Human-Machine Interface (HMI) to interact with client machine.

[6] The signing of CSR is performed by the external HSM; hence, this function is out of TOE scope, however, the TOE controls access to this function.

[7] Cryptographic keys are generated by and stored in the external HSM; hence, this function is out of TOE scope, however, the TOE controls access to this function.

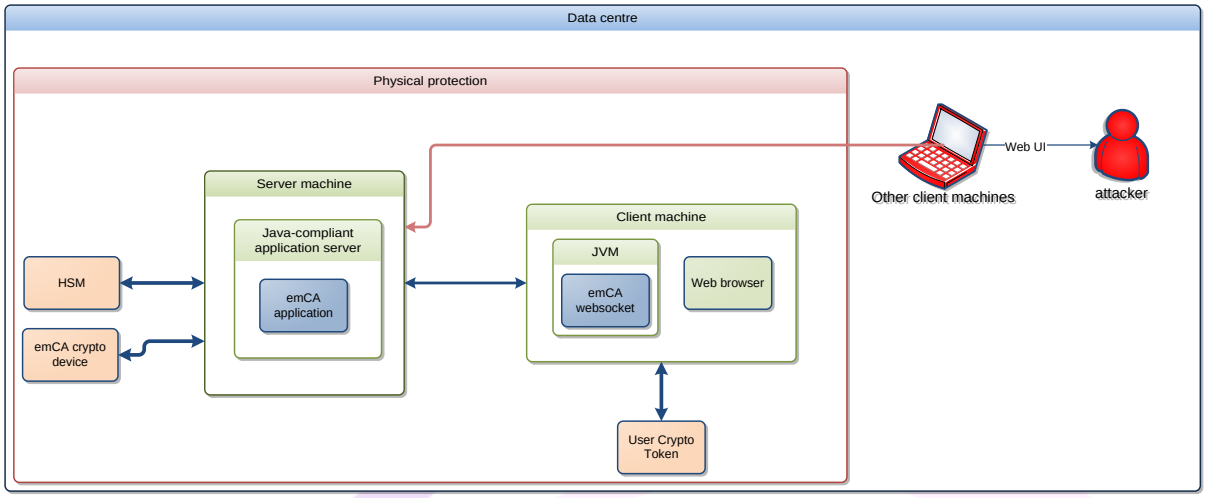

Figure 4: Threat scenario

3.2 Threats

Threat	Description
T.Password	An attacker may brute-force the token PIN and zip password of backup archive to gain unauthorised access to assets (see Table 5 and Table 6).
T.User_Masquerade	An attacker may steal user credentials (username, token PIN and user certificates) to access gain unauthorised access to assets (see Table 5 and Table 6)
T.Tamper	An attacker may tamper the TOE to gain unauthorised access to assets (see Table 5 and Table 6). An attacker may also tamper the assets which requires integrity protection.
T.Modify_Backup	An attacker may modify exported or imported assets (see Table 5 and Table 6) meant for backup or restore, respectively.

Table 10: Threats

3.3 Assumptions

Assumption	Description
A.Trusted_User	TOE users are well-trained to operate the TOE securely in accordance with the operational guidance. System administrators are well-trained to setup the IT environment in accordance with the preparative guidance. Both TOE users and system administrators are trusted.
A.Trusted_CPU	The CPU and hardware peripherals on the server and client machine that the Windows Server and Windows OSes run on, respectively, are trusted and secure i.e. in compliance with organisation's security policy.
A.Trusted_OS	The Windows Server and Windows OSes that runs on the server and client machine, respectively, are trusted and secure i.e. in compliance with organisation's security policy.

A.Trusted_IT_Products	The following external IT products that support the TOE operations are trusted and secure i.e. in compliance with organisation's security policy.
	• Server side
	  ○ Java-compliant application server
	  ○ LDAP server
	  ○ FTP server

	○ SQL database ○ HSM ○ PKCS #11 driver ○ HSM-password cryptographic token ○ Time server • Client side ○ JVM ○ Web Browser ○ Cryptographic token ○ PKCS #11 driver
A.Physical	The TOE and external IT products are deployed in physically secure environment where only authorised TOE users and system administrators have physical access. The interconnect between the server machine and client machine is physically protected from tamper. The TOE shall be deployed in an isolated network.
A.Trusted_Channel	The application server and web browser shall establish a trusted channel.
A.Reliable_Time	A time server shall be deployed to provide reliable timestamp to the TOE.

Table 11: Assumptions

3.4 Organisation Security Policies (OSP)

OSP	Description
P.Approved_HSM	The HSM complies with TOE users' organisation security policies.
P.Approved_Token	The cryptographic token (including emCA crypto device) complies with TOE users' organisation security policies.

Table 12: OSP

4 Security Objectives (ASE_OBJ)

This section identifies the security objectives for the TOE and the operational environment. Security objectives counters the identified threats, upholds the identified OSPs and fulfils the assumptions.

4.1 Security Objectives for the TOE.

Security Objectives	Descriptions
O.ID_n_Auth	The TOE shall identify and authenticate TOE users to ensure they are authorised to access the TSF and assets.
O.Reauth	The TOE shall enforce re-authentication for every user-initiated TSF operation.
O.Access_Control	The TOE shall ensure each TOE user has access to authorised TOE operations and assets only, based on their associated subject (role).
O.Integrity	The TOE shall protect the integrity of CA/certificate owner's certificates and CRL. The TOE shall also protect the integrity of exported backup archives which contains the TOE configuration.
O.Password_Policy	The TOE shall enforce password complexity policy on the user token PIN and Zip password of backup archive.
O.Duty_Separation	The TOE shall enforce separation of duties for critical operations such as: • backup and restore. • audit management. • roles and user management. • certificate, CRL and profile management.
O.Audit	The TOE shall generate audit logs for security relevant events.

Table 13: Security Objectives for TOE

4.2 Security Objectives for the Operational Environment

Security Objectives	Descriptions
OE.Trusted_User	The operational environment shall ensure: • TOE users are well-trained to operate the TOE securely in accordance with the operational guidance. • System administrators are well-trained to setup the IT environment in accordance with the preparative guidance. • Both TOE users and system administrators are trusted.
OE.Trusted_CPU	The System Administrator shall ensure the CPU and hardware peripherals on the server and client machine that the Windows Server and Windows OSes run on, respectively, are trusted and secure i.e. in compliance with organisation's security policy.
OE.Trusted_OS	The System Administrator shall ensure the Windows Server and Windows OSes that runs on the server and client machine, respectively, are trusted and secure i.e. in compliance with organisation's security policy.

OE.Trusted_IT_Products	The System Administrator shall ensure the following external IT products that support the TOE operations are trusted and secure i.e. in compliance with organisation's security policy.
	• Server side
	  ○ Java-compliant application server
	  ○ LDAP server
	  ○ FTP server

	○ SQL database ○ HSM ○ PKCS #11 driver ○ emCA crypto device ○ Time server • Client side ○ JVM ○ Cryptographic token ○ PKCS #11 driver
OE.Physical	The System Administrator shall ensure the: • TOE and external IT products are deployed in the same physically secure environment where only authorised TOE users and system administrators have access. • Interconnect between the server machine and client machine is physically protected from tamper. • The TOE shall be deployed in an isolated network.
OE.Trusted_Channel	The System Administrator shall ensure the following: • The application server and web browser shall establish a trusted channel.
OE.Reliable_Time	The System Administrator shall deploy a time server to provide reliable timestamp to the TOE.
OE.Approved_HSM	The System Administrator shall ensure that the HSM complies with TOE users' organisation's security policies.
OE.Approved_Token	The System Administrator shall ensure that the cryptographic token (including emCA crypto device) complies with TOE users' organisation's security policies.

Table 14: Security Objectives for Operational Environment

4.3 Security Objective Rationale

4.3.1 Tracing between security objectives and security problem definition

Threats-OSPs-Assumptions / Security Objectives	O.ID_n_Auth	O.Reauth	O.Access_Control	O.Integrity	O.Password_Policy	O.Duty_Separation	O.Audit	OE.Trusted_User	OE.Trusted_CPU	OE.Trusted_OS	OE.Trusted_IT_Products	OE.Physical	OE.Trusted_Channel	OE.Reliable_Time	OE.Approved_HSM	OE.Approved_Token
T.Password					X		X	X				X		X		X
T.User_Masquerade			X				X	X				X	X	X		X
T.Tamper	X	X	X	X		X	X	X	X	X	X	X	X	X	X	
T.Modify_Backup	X	X	X		X		X	X	X	X	X	X	X	X		
A.Trusted_User								X								
A.Trusted_CPU									X							
A.Trusted_OS										X						

A.Trusted_IT_Products											X					
A.Physical												X				
A.Trusted_Channel													X			
A.Reliable_Time														X		
P.Approved_HSM															X	
P.Approved_Token																X

Table 15: Tracing between security objectives and SPD

4.3.2 Justification for tracing

This section explains the tracing illustrated in Table 15.

4.3.2.1 Threats-Security Objective Justification

T.Password	An attacker may brute-force the token PIN and zip password of backup archive to gain unauthorised access to assets (see Table 5 and Table 6).
O.Password_Policy	The TOE enforces password complexity policy on token PIN and zip password of backup archive makes it difficult for brute-force attack to be successful.
OE.Trusted_User	Trusted and well-trained TOE users ensure secure use of username, token PIN and token. This reduces the risk of attackers performing offline brute-force attack on the token PIN on the token.
OE.Physical	The deployment of TOE in a physically secure environment ensures that only authorised TOE user have access to the TOE and backup archive. This removes the risk of attacker performing offline brute-force attack on the zip password of backup archive. The deployment of TOE in an isolated network also reduces the exposure of TOE logical interfaces being exposed to the external network, thereby reducing the risk of brute-force attack on token PIN.
OE.Approved_Token	This ensures that the token has implemented sufficient security measures to fend against brute-force attack on the token PIN. This reduces the risk of attackers attempting to obtain the token PIN by brute-force.
O.Audit, OE.Trusted_User and OE.Reliable_Time	With timely audit log review by TOE user (**OE.Trusted_User**) and **OE.Reliable_Time**, **O.Audit** can help to mitigate the effects of the threat by timely detecting the adverse actions so that appropriate actions can be taken.

T.User_Masquerade	An attacker may steal user credentials (username, token PIN and user certificates) to access gain unauthorised access to assets (see Table 5 and Table 6)
O.Access_Control	Each role (subject) has limited access to authorised TOE operations and assets. This mitigates the risk of tampering the assets (Table 5 and Table 6) in case user credentials are compromised.

OE.Trusted_User	Trusted and well-trained TOE users ensure secure use of username, token PIN and token (where user certificate is stored). This removes the risk of attackers tampering the user token to access the token PIN and user certificate.
OE.Physical	The deployment of TOE in a physically secure environment ensures that only authorised TOE user have access to the TOE. This removes the risk of attacker attempting to tamper the TOE or sniff the traffic between server and client machines to steal user credentials. The deployment of TOE in an isolated network also reduces the exposure of TOE logical interfaces being exposed to the external network, thereby reducing the risk of user masquerade.
OE.Approved_Token	This ensures that the user token has implemented sufficient security measures to protect token PIN and user certificates that are stored in it. This reduces the risk of attackers attempting to extract the user certificates and token PIN from the token. The use of username, token and token PIN together shall reduce the risk of user's credential being masqueraded.
OE.Trusted_Channel	This removes that risk that the traffic between various external IT products and parts of TOE from being tampered or sniffed physically or logically.
O.Audit, OE.Trusted_User and OE.Reliable_Time	With timely audit log review by TOE user (**OE.Trusted_User**) and **OE.Reliable_Time**, **O.Audit** can help to mitigate the effects of the threat by timely detecting the adverse actions so that appropriate actions can be taken.

T.Tamper	An attacker may tamper the TOE to gain unauthorised access to assets (see Table 5 and Table 6). An attacker may also tamper the assets which require integrity protection.
O.ID_n_Auth	The TOE identifies and authenticates all users with their username, token, and token PIN. This ensures that only authorised users have access to the assets (Table 5 and Table 6) hence reducing the risk of attackers tampering the assets (Table 5 and Table 6).
O.Reauth	For every user-initiated action after user authentication, users must perform re-authentication to confirm that the authorised users are still performing the TSF-mediated action. This further reduces the risk of attackers tampering the assets (Table 5 and Table 6).
O.Access_Control	Each role (subject) has limited access to authorised TOE operations and assets (Table 5 and Table 6). This mitigates the risk of tampering the assets (Table 5 and Table 6) in case user credentials are compromised.
O.Integrity	CA/certificate owner's certificates, CRL and backup archives are integrity protected. This diminishes the risk of attackers tampering the said assets (Table 5 and Table 6).
O.Duty_Separation	This will reduce the risk of authorised users tampering assets (Table 5 and Table 6) with an intent to perform fraud.

OE.Trusted_User	Trusted and well-trained TOE users ensure secure use of username, token PIN and token and shall not tamper the TOE. This reduces the risk of TOE users tampering the asset (Table 5 and Table 6) and TOE.
OE.Trusted_CPU, OE.Trusted_OS and OE.Trusted_IT_Products	These supporting components shall not tamper the TOE and assets (Table 5 and Table 6). In turn, this reduces the risk of TOE tamper by the supporting components.
OE.Physical	The deployment of TOE in a physically secure environment ensures that only authorised TOE user have access to the TOE. This removes the risk of attacker attempting to tamper the TOE. The deployment of TOE in an isolated network also reduces the exposure of TOE logical interfaces being exposed to the external network, thereby reducing risk of tamper to TOE.
OE.Trusted_Channel	This removes that risk that the traffic between various external IT products and parts of TOE from being tampered physically or logically.
OE.Approved_HSM	The TOE relies on an external HSM to provide cryptographic operations for protection of TOE assets such as digital signing of certificate, digital signing of audit log, etc. An approved-HSM ensures correct cryptographic operations and adequate self-protection.
O.Audit, OE.Trusted_User and OE.Reliable_Time	With timely audit log review by TOE user (**OE.Trusted_User**) and **OE.Reliable_Time**, **O.Audit** can help to mitigate the effects of the threat by timely detecting the adverse actions so that appropriate actions can be taken.

T.Modify_Backup	An attacker may modify exported or imported assets (see Table 5 and Table 6) meant for backup or restore, respectively.
O.ID_n_Aut	The TOE identifies and authenticates all users with their username, token, and token PIN. This ensures that only authorised users have access to the assets (Table 5 and Table 6) hence reducing the risk of attackers tampering the assets (Table 5 and Table 6).
O.Reauth	For every user-initiated action after user authentication, users must perform re-authentication to confirm that the authorised users are still performing the TSF-mediated action. This further reduces the risk of attackers tampering the assets (Table 5 and Table 6).
O.Access_Control	Each role (subject) has limited access to authorised TOE operations and assets (Table 5 and Table 6). This mitigates the risk of tampering the assets (Table 5 and Table 6) in case user credentials are compromised.
O.Password_Policy	The TOE enforces password complexity policy on token PIN and zip password of backup archive makes it difficult for brute-force attack to be successful.
O.Audit, OE.Trusted_User and OE.Reliable_Time	With timely audit log review by TOE user (**OE.Trusted_User**) and **OE.Reliable_Time**, **O.Audit** can help to mitigate the effects of the threat by timely detecting the adverse actions so that appropriate actions can be taken.

OE.Trusted_User	Trusted and well-trained TOE users ensure secure use of username, token PIN and token. This reduces the risk of user tampering the backup archive.
OE.Trusted_CPU, OE.Trusted_OS and OE.Trusted_IT_Products	These supporting components shall not tamper the TOE, its user data and TSF data. In turn, this reduces the risk of TOE tamper by the supporting components.
OE.Physical	The deployment of TOE in a physically secure environment ensures that only authorised TOE user have access to the TOE. This removes the risk of attacker attempting to tamper the TOE. The deployment of TOE in an isolated network also reduces the exposure of TOE logical interfaces being exposed to the external network, thereby reducing risk of tamper to TOE.

4.3.2.2 Assumptions-Security Objective Justification

A.Trusted_User	TOE users are well-trained to operate the TOE securely in accordance with the operational guidance. System administrators are well-trained to setup the IT environment in accordance with the preparative guidance. Both TOE users and system administrators are trusted.
OE.Trusted_User	This directly upholds the assumption.

A.Trusted_CPU	The CPU and hardware peripherals on the server and client machine that the Windows Server and Windows OSes run on, respectively, are trusted and secure i.e. in compliance with organisation's security policy.
OE.Trusted_CPU	This directly upholds the assumption.

A.Trusted_OS	The Windows Server and Windows OSes that runs on the server and client machine, respectively, are trusted and secure i.e. in compliance with organisation's security policy.
OE.Trusted_OS	This directly upholds the assumption.

A.Trusted_IT_Products	The external IT products that support the TOE operations are trusted and secure i.e. in compliance with organisation's security policy.
OE.Trusted_IT_Products	This directly upholds the assumption.

A.Physical	The TOE and external IT products are deployed in the same physically secure environment where only authorised TOE users and system administrators have access. The TOE shall be deployed in an isolated network.
OE.Physical	This directly upholds the assumption.

A.Trusted_Channel	Trust channel is established for internal TOE transfer and inter TSF

	transfer.
OE.Trusted_Channel	This directly upholds the assumption.

A.Reliable_Time	A time server shall be deployed to provide reliable timestamp to the TOE.
OE.Reliable_Time	This directly upholds the assumption.

4.3.2.3 OSP-Security Objective Justification

P.Approved_HSM	The HSM complies with organisation's security policies.
OE.Approved_HSM	This directly upholds the OSP.

P.Approved_Token	The cryptographic token (including HSM password token) complies with organisation's security policies.
OE.Approved_Token	This directly upholds the OSP.

5 Security Requirements (ASE_REQ)

This chapter gives the security functional requirements and the security assurance requirements for the TOE.

Security functional requirements components are stated in section 5.1 Security Functional Requirements. Security assurance components are stated in section 5.2 Security Assurance Requirements in are drawn from Common Criteria Part 3[CC3].

Operations for iteration, assignment, selection and refinement have been made. The following textual conventions are used in this chapter as part of every SFR:

- Iteration is represented by a slash ('/') followed by an identifier placed at the end of the component. For example, FDP_ACF.1/Signer.
- Assignment is represented by **bold text**.
- Selection is represented by *italic text*.
- Refinement is represented by underlined text.

5.1 Security Functional Requirements

5.1.1 User data protection

5.1.1.1 FDP_ACC (Access control policy)

FDP_ACC.1 **Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the **User Data Access Control Policy** on **see Table 16**.

Subjects	CA Administrator, Administrator, Officer, Auditor and Operator.
Objects	CA CSR, certificate owners' CSR, certificate owners' certificates, CA certificates and CRL
Operations	Search, create, revoke, suspend, reinstate and export certificate owners' certificate
	Import certificate owners' CSR
	Search, create, revoke and export CA certificates
	Create and export CA CSR
	Create, modify and export CRL
	Create, modify and read CRL, Key and Certificate profiles

Table 16: Subjects, objects and operations.

5.1.1.2 FDP_ACF (Access control functions)

FDP_ACF.1 **Security attribute based access control**

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the **User Data Access Control Policy** to objects based on the following: **see Table 17**.

Subjects	CA Administrator, Administrator, Officer, Auditor and Operator.
Objects	CA CSR, CA/certificate owners' certificates, CRL and CRL/key/certificate profiles
Security Attributes	Roles

Table 17: Security attributes

Application note: After the TSF identifies and authenticates the user, the user identity shall be associated to one of the pre-defined roles i.e. CA Administrator, Administrator, Officer, Auditor or Operator. The TSF shall base on the associated role determine the operations that can be performed on an object.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **see Table 18**.

Operations	CA Administrator	Administrator	Officer	Auditor	Operator
Create, revoke, suspend, reinstate, export certificate owners' certificate			X		
Search certificate owners' certificate	X	X	X		
Import certificate owners' CSR			X		
Search, create, revoke and export CA certificates			X		
Search CA certificates	X	X	X		
Create and export CA CSR			X		
Create and modify CRL			X		
Export CRL	X	X	X	X	X
Create, modify and read CRL, certificate and key profiles		X			

Table 18: User Data Access Control Policy Rules

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

5.1.1.3 FDP_SDI (Stored data integrity)

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors** on all objects, based on the following attributes: **HMAC-SHA256 digest**.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall

- **terminate the Certificate owner/CA certificates and CRL export action**
- **displayed an error message**
- **generate an audit log.**

Application notes: Certificate owner and CA certificates and CRL stored in the external database protected are protected by HMAC-SHA256 digest. The TOE verifies the integrity of this information whenever it fetches this information from the external database.

5.1.2 Identification and Authentication

5.1.2.1 FIA_ATD (User attribute definition)

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **username**
- **roles**
- **username-role association information**
- **authentication matrix**
- **user certificates**.

Application note: User certificates are authentication data. User certificates are digitally signed according to the chain of trust as depicted in Figure 3.

5.1.2.2 FIA_UAU (User authentication)

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FDP_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.6 Re-authenticating

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_UAU.6.1 The TSF shall re-authenticate the user under the conditions **user-initiated TSF-mediated actions that requires modifying or adding of user data and/or TSF data**.

Application notes: TSF-mediated actions related to viewing of user data and/or TSF data does not require re-authentication.

5.1.2.3 FIA_UID (User identification)

FIA_UID.2 **User identification before any action**

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FDP_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.2.4 FIA_USB (User-subject binding)

FIA_USB.1 **User-subject binding**

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **username and roles**.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **a username shall not assume more than one role**.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **none**.

5.1.3 Security Audit

5.1.3.1 FAU_GEN (Security audit data generation)

FAU_GEN.1 **Audit data generation**

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *minimal, basic, detailed and not specified* level of audit; and

c) See Table 19.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **see 'Additional info' column of Table 19**

Event	SFR Component	Detail level	Additional info
Security attribute based access control	FDP_ACF.1	Detailed: The specific security attributes used in making an access check.	Changes are made to key, certificate and CRL profiles. Request to change certificate status is accepted or rejected.

Stored data integrity monitoring and action	FDP_SDI.2	Detailed: The type of integrity error that occurred.	
User authentication before any action	FIA_UAU.2	Basic: All use of the authentication mechanism.	
Re-authenticating	FIA_UAU.6	Basic: All re-authentication attempts.	
User identification before any action	FIA_UID.2	Basic: All use of the user identification mechanism, including the user identity provided.	
User-subject binding	FIA_USB.1	Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	
Export of user data without security attributes	FDP_ETC.1	Basic: All attempts to export CSR and certificate owners' certificates.	
Import of user data without security attributes	FDP_ITC.1	Basic: All attempts to import CSR as part of certificate requesting process, including any security attributes.	If the CSR is accepted, a copy of the issued certificate is recorded. If CSR is rejected, the reason for rejection is recorded e.g. invalid date, rejected by Officer, etc.
Audit generation	FAU_GEN.1	Not specified: Audit signing	Digital signature shall be included in the audit log.
Audit review	FAU_SAR.1	Basic: Reading of information from the audit records.	
Restricted audit review	FAU_SAR.2	Basic: Unsuccessful attempts to read information from the audit records.	
Selectable audit review	FAU_SAR.3	Detailed: the parameters used for the viewing.	
Prevention of audit data loss	FAU_STG.4	Basic: Action taken due to the audit storage failure.	
Verification of secrets	FIA_SOS.1	Basic: Rejection or acceptance by the TSF of any tested secret.	
Cryptographic operations	FCS_COP.1	Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	
Management of	FMT_MOF.1	Basic: All modifications in the	

security functions behaviour		behaviour of the functions in the TSF.	
Management of security attributes	FMT_MSA.1	Basic: All modifications of the values of security attributes i.e. • username • roles • username-role association information • authentication matrix • user certificates	
Static attribute initialisation	FMT_MSA.3	Basic: Modifications of the default setting restrictive rules. Basic: All modifications of the initial values of security attributes.	
Specification of Management Functions	FMT_SMF.1	Minimal: Use of the management functions.	
Security roles	FMT_SMR.1	Minimal: modifications to the group of users that are part of a role.	
Management of TSF data	FMT_MTD.1	Basic: All modifications to the values of TSF data.	
Integrity of exported TSF data	FPT_ITI.1	Minimal: the detection of modification of transmitted TSF data.	

Table 19: Auditable events

FAU_GEN.2 **User identity association**

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.3.2 FAU_SAR (Security audit review)

FAU_SAR.1 **Audit review**

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide **Auditor** with the capability to read **function category, status, event, event ID status, IP address, user and time stamp** from the audit records.

Application notes: *'function category'* is referred to as *'module'* throughout the ADV design documents. *'event'* contains description of the event. *'status'* refers to the success or failure of an event. *'event ID'* refers to a unique number identifying the event. '*user*' contains the username i.e. user identity that originated the event.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply **search** of audit data based on **function category, status, event, status, IP address, user and time stamp**.

5.1.3.3 FAU_STG (Security audit event storage)

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall *prevent audited events, except those taken by the authorised user with special rights* and **none** if the audit trail is full.

5.1.4 Export and import user data

5.1.4.1 FDP_ETC (Export from TOE)

FDP_ETC.1 Export of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1 The TSF shall enforce the **User Data Access Control Policy** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes

Application note: The Officer can export certificate owner's certificate, CA CSR and CRL. The CA administrator can set the schedule to publish CRL.

5.1.4.2 FDP_ITC (Import from outside the TOE)

FDP_ITC.1 Import of user data without security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FMT_MSA.3 Static attribute initialisation

FDP_ITC.1.1 The TSF shall enforce the **User Data Access Control Policy** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **none**.

Application notes: The Officer can import certificate owner's CSR.

5.1.5 Password Policy

5.1.5.1 FIA_SOS (Specification of secrets)

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **at least**

- **1 uppercase**
- **1 Lowercase**
- **1 numeric digit**
- **1 special character i.e. '@', '#', '%' and '$'**
- **8 characters long**

Application note: This quality metric applies to user token PIN, emCA crypto device PIN, HSM password, PDF password, Zip password, LDAP password and Remote System password.

5.1.6 Cryptographic operations

5.1.6.1 FCS_COP (Cryptographic operation)

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform **digest generation and verification** in accordance with a specified cryptographic algorithm **HMAC-SHA256** and cryptographic key sizes **256 bits** that meet the following: **none**.

5.1.6.2 FCS_CKM (Cryptographic key management)

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key

destruction method **zeroization** that meets the following: **none**.

5.1.7 Security Management

5.1.7.1 FMT_SMF (Specification of Management Functions)

FMT_SMF.1 **Specification of Management Functions**

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **see 'Management function' column of Table 20**.

5.1.7.2 FMT_SMR (Security management roles)

FMT_SMR.1 **Security roles**

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles **CA Administrator, Administrator, Auditor and Operator**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.7.3 FMT_MOF (Management of functions in TSF)

FMT_MOF.1 **Management of security functions behaviour**

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to *modify the behaviour of* the functions **see 'Security function component being managed' column of Table 20** to **see 'Authorised role' column of Table 20**.

Management functions	Security function component being managed	Authorised role
Management of user security attributes username, roles, user-role association and user certificates of Officer, Auditor and Operator.	FMT_MSA.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FDP_ACF.1	Administrator
Management of user security attributes username, roles, user-role association, authentication matrix and user certificates of Administrator.	FMT_MSA.1, FIA_UAU.2, FIA_UID.2, FIA_USB.1, FDP_ACF.1	CA Administrator

Table 20: Management of security function behaviour

5.1.7.4 FMT_MSA (Management of security attributes)

FMT_MSA.1 **Management of security attributes**

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the **User Data Access Control Policy** to restrict the ability to *query, modify, delete* the security attributes **username, roles, username-role association information, authentication matrix and user certificates** to **CA Administrator and Administrator**.

Application note: CA Administrator can manage user security attributes associated with Administrator role. Only the CA Administrator manage authentication matrix. Administrator can manage user security attributes associated with Officer, Auditor and Operator roles. Administrator can only view authentication matrix. There can only be one user associated to the CA Administrator role; CA Administrator cannot be configured as part of the authentication matrix. Table 21 illustrates the security attribute management in table form.

		Security roles	
Roles being managed	**Security Attributes**	**CA Administrator**	**Administrator**
Administrator, Officer, Auditor and Operator	authentication matrix	**X**	
Administrator	username, roles, username-role association information and user certificates	**X**	
Officer, Auditor and Operator	username, roles, username-role association information and user certificates		**X**

Table 21: Management of security attributes

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the **User Data Access Control Policy** to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall not allow the **CA Administrator and Administrator** to specify alternative initial values to override the default values when an object or information is created.

Application notes: The default role that can be managed by CA Administrator is Administrator. The default set of roles that can be managed by Administrator are Officer, Auditor and Operator. However, the default value of role is not configurable. For the rest of the security attributes i.e. username, username-role association information, authentication matrix and user certificates, there are no default values and the default values are not configurable.

5.1.7.5 FMT_MTD (Management of TSF data)

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to see **'Action' column of Table 22** the **see 'TSF data' column of Table 22** to **see 'Roles' column of Table 22**.

Action	TSF data	Roles
Create and import	User certificates of Administrator	CA Administrator
Create and import	User certificates of Officer, Auditor and Operator	Administrator
Export	Audit log	Auditor
Create, query, modify and delete	Username-role association information of Administrator	CA Administrator
Create, query, modify and delete	Username-role association information of Officer, Auditor and Operator	Administrator
Modify	Authentication matrix	CA Administrator
Export	TOE configuration	Operator
Import	TOE configuration	CA Administrator

Table 22: Management of TSF data

5.1.7.6 FPT_ITI (Integrity of exported TSF data)

FPT_ITI.1 **Inter-TSF detection of modification**

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and another trusted IT product within the following metric: **HMAC-SHA256 digest**.

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform **halt restoration of TOE's configuration** if modifications are detected.

Application notes: The TOE generates HMAC-SHA256 digest for backup archives when it is exported out of the TOE. The backup archives consist of all TOE configuration. The TOE validates the HMAC-SHA256 digest when a backup archive is used to restore the TOE's configuration. If the HMAC-SHA256 digest verification fails, the TOE shall halt restoration of TOE's configuration.

5.2 Security Assurance Requirements

The assurance level for this TOE is EAL4+ ALC_FLR.2

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design

AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

Table 23: Assurance requirements for EAL4+ ALC_FLR.2

5.3 Security Requirement Rationale

5.3.1 Tracing between SFR and security objectives of TOE

SFR/Security Objectives	O.ID_n_Auth	O.Reauth	O.Access_Control	O.Integrity	O.Password_Policy	Duty_Separation	O.Audit
FDP_ACC.1			**X**			**X**	
FDP_ACF.1			**X**			**X**	
FDP_SDI.2				**X**			
FIA_ATD.1	**X**						
FIA_UAU.2	**X**						

FIA_UAU.6		X					
FIA_UID.2	X						
FIA_USB.1	X						
FAU_GEN.1							X
FAU_GEN.2							X
FAU_SAR.1			X			X	
FAU_SAR.2			X			X	
FAU_SAR.3							X
FAU_STG.4							X
FDP_ETC.1			X			X	
FDP_ITC.1			X			X	
FIA_SOS.1					X		
FCS_COP.1				X			
FCS_CKM.4				X			
FMT_SMF.1			X			X	
FMT_SMR.1			X			X	
FMT_MOF.1			X			X	
FMT_MSA.1			X			X	
FMT_MSA.3			X			X	
FMT_MTD.1			X			X	
FPT_ITI.1				X			

Table 24: Tracing between SFR and security objectives of TOE

5.3.2 Justification for tracing

The following section provides justification for the tracing in Table 14.

O.ID_n_Auth	The TOE shall identify and authenticate TOE users to ensure they are authorised to access the TSF and assets.
FIA_ATD.1	defines the user security attributes required for user identification and authentication.
FIA_UAU.2 and **FIA_UID.2**	provide user identification and authentication security function based on the user security attributes defined in **FIA_ATD.1**.
FIA_USB.1	provides user-subject binding after user authentication is successful.

O.Reauth	The TOE shall enforce re-authentication for every user-initiated TSF operation.
FIA_UAU.6	provides user re-authentication whenever user-initiate TSF-mediated action is required.

O.Access_Control	The TOE shall ensure each TOE user has access to authorised TOE operations and assets only, based on their associated subject (role).
FDP_ACC.1 and FDP_ACF.1	provides the user data access control policy.
FDP_ETC.1 and FDP_ITC.1	applies the user data access control policy defined in **FDP_ACC.1** and **FDP_ACF.1** for export and import of user data.
FMT_SMF.1	defines the security management functions offered by the TOE
FMT_SMR.1	defines security roles that can access the management functions defined in **FMT_SMF.1**.
FMT_MOF.1	defines the access control policy that governs access to management functions defined in **FMT_SMF.1** by security roles defined in **FMT_SMR.1**.
FMT_MSA.1	defines the access control policy to manage user security attributes related to user data access control policy defined in **FDP_ACC.1** and **FDP_ACF.1**.
FMT_MTD.1	defines the access control policy to manage TSF data.
FAU_SAR.1 and **FAU_SAR.2**	allows only the Auditor role to review audit logs.

O.Integrity	The TOE shall protect the integrity of certificate owner's and CA certificates and CRL. The TOE shall also protect the integrity of exported backup archives which contains the TOE configuration.
FDP_SDI.2	provides the integrity protection for certificate owner's and CA certificates and CRL.
FPT_ITI.1	provides the integrity protection for exported backup archives.
FCS_COP.1 and **FCS_CKM.4**	provides the HMAC-SHA256 implementation to protect the integrity of CA and certificate owner's certificates, CRL and backup archives.

O.Password_Policy	The TOE shall enforce password complexity policy on the user token PIN and Zip password of backup archive.
FIA_SOS.1	provides the quality metric for user token PIN, emCA crypto device PIN, HSM password, PDF password, Zip password, LDAP password and Remote System password

O.Duty_Separation	The TOE shall enforce separation of duties for critical operations.
FDP_ACC.1, FDP_ACF.1, FAU_SAR.1, FAU_SAR.2, FDP_ETC.1, FDP_ITC.1, FMT_SMF.1, FMT_SMR.1,	collectively ensures separation duties between the different roles i.e. CA Administrator, Administrator, Officer, Auditor and Operator.

FMT_MOF.1, FMT_MSA.1, FMT_MSA.3 and FMT_MTD.1	

O.Audit	The TOE shall generate audit logs for security relevant events.
FAU_GEN.1	generates audit logs for security relevant events.
FAU_GEN.2	associates each auditable event with the user identity that caused the event.
FAU_SAR.3	allows users to search audit logs based on a defined set of criteria.
FAU_STG.4	prevents the operation of audit, except those taken by the Auditor if the audit trail is full. In turn, this protected the audit logs from loss.

5.3.3 SFR Dependency Fulfilment

SFR	Dependencies	Fulfilment
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1
	FMT_MSA.3	FMT_MSA.3
FDP_SDI.2	No dependencies.	Not applicable
FIA_ATD.1	No dependencies.	Not applicable
FIA_UAU.2	FIA_UID.1	FIA_UID.2 is hierarchical to FIA_UID.1
FIA_UAU.6	No dependencies.	Not applicable
FIA_UID.2	No dependencies.	Not applicable
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FAU_GEN.1	FPT_STM.1	Fulfilled by **OE.Reliable_Time.**
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.2 is hierarchical to FIA_UID.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.4	FAU_STG.1	The protection of audit trails is enforced by OE.Approved_HSM such that the external HSM signs the audit logs during audit generation.
FDP_ETC.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1
FIA_SOS.1	No dependencies.	Not applicable

FCS_COP.1	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1]	The HMAC-SHA256 key is stored in the emCA Configuration file in encrypted form. **OE.Trusted_IT_Products** ensures that the local storage is trusted and secure, hence, FDP_ITC.1 or FDP_ITC.2 is not required.
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1, FDP_ITC.2 or FCS_CKM.1]	The HMAC-SHA256 key is stored in the emCA Configuration file in encrypted form. **OE.Trusted_IT_Products** ensures that the local storage is trusted and secure, hence, FDP_ITC.1 or FDP_ITC.2 is not required.
FMT_SMF.1	No dependencies.	Not applicable
FMT_SMR.1	FIA_UID.1	FIA_UID.2 is hierarchical to FIA_UID.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FPT_ITI.1	No dependencies.	Not applicable

Table 25: SFR dependency fulfilment

5.3.4 Rationale for EAL4 augmented

The assurance level for this protection profile is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. The TOE described in this protection profile is just such a product. Augmentation results from the selection of **ALC_FLR.2 Flaw reporting procedures**. This dependence exceeds in the EAL4 assurance package.

6 TOE Summary Specification (ASE_TSS)

6.1 User data protection

The TOE controls access to user data based on roles and authentication matrix. The associated role and authentication matrix of a user determines the user data and operations a user can access and perform, respectively.

FDP_ACC.1 Subset access control	Access control lists can be used to specify the acceptable subsets of security functions applicable to specified user data.
FDP_ACF.1 Security attribute based access control	TOE users are assigned roles that are granted a set of access control rules on a set of user data.

Table 26: SFR related to Access Control on user data

The TOE also protects the integrity of certificate owner's and CA certificates and CRL using HMAC-SHA256 digest. These certificate owner's and CA certificates and CRL are stored in an external database.

FDP_SDI.2 Stored data integrity monitoring and action	The TOE protects the integrity of certificate owner's and CA certificates and CRL are using HMAC-SHA256 digest. The TOE verifies certificate and CRL's digest whenever the TOE fetches this information from the external database.

Table 27: SFR related to user data integrity protection

6.2 Identification and Authentication

All security operations and access to assets requires user identification and authentication. Subsequently, each user-initiated TSF-mediated requires re-authentication of user as well.

FIA_ATD.1 User attribute definition	The TOE maintains user security attributes i.e. username, roles, username-role association information, authentication matrix and user certificates in the external database. The TOE uses these user security attributes to determine the user-role association. This user-role association is contained in a token. The token is held by the process or thread that calls the TOE.
FIA_UAU.2 User authentication before any action	The TOE authenticates the user via a challenge-response protocol. The TOE performs the challenge-response protocol using the user crypto token. The TOE issues a challenge to the user crypto token with a generated secure random number. The TOE then combines the secure random number with the username and associate role to form To Be Signed (TBS) data. Thereafter, the TOE sends the TBS data to the user crypto token where it is signed. Finally, the TOE then verifies the digital signature of the TBS data as part of the user authentication process. No TSF-mediated action can be performed on behalf of the user prior to successful user authentication.
FIA_UAU.6 Re-authenticating	The TOE ensures m out n authentication, is configured by CA administrator during TOE (emCA application) initial set up where in CA administrator has rights to configure "Authentication Matrix" to specify number of users (Max & Min). The configured users must re-authenticate themselves post login to perform specified actions. Authentication and access control both are inter-linked based on role,

	authorization and access privileges are pre-defined for individual users.
FIA_UID.2 User identification before any action	The TOE identifies the user using the user certificate that is contained within the user crypto token. The user crypto token first authenticates the user using the user token PIN. If the authentication is successful, the user crypto token shall present user certificate to the TOE. Subsequently, the TOE shall check the presented user certificate
FIA_USB.1 User-subject binding	The TOE uses the user security attributes to determine the associated role after successful user authentication. Each process and thread have a token that identifies the user and associated roles held by that process or thread. For each service request to the TOE, the TOE obtains the token from the calling process or thread (the SID). The TOE then uses the token to determine the user's privileges and access rights.

Table 28: SFR related to Identification and Authentication

6.3 Security Audit

The emCA application generates audit logs for internal actions and user actions and works with an external SQL database to store this information.

An emCA application generates the following log types:

Application logs	Problem tracking or maintenance purposes. Since these logs are solely for monitoring and maintenance purposes, they are not cryptographically protected.
Audit logs	Security relevant events. Each log entry contains audit relevant data and is cryptographically protected by the external HSM.

Table 29: Audit log types

Each audit log contains the following types of information:

Date	The date the event occurred.
Time	The time the event occurred.
User	Username i.e. user identity that originated the event.
Status	Success or failure of event.
Event	Description of the event.
Event ID	A unique number identifying the event.

Table 30: Audit log information

emCA application provides an interface to query, view and check the audit logs stored in the external database.

If an event prevents the recording of audit logs occurs, emCA application shall prevent audited security operations from being carried out except those being carried out by the Auditor. This avoids the execution of operations without properly recording related audit logs.

Date and time accuracy of audit logs is guaranteed an external time server.

FAU_GEN.1 Audit data generation	Audit logs are generated along the occurrence of the events and

	immediately committed and stored in the external database that is part of the IT environment.
FAU_GEN.2 User identity association	Audit logs include information about the user identity, either by username for an authenticated user or by a value for an unauthenticated user.
FAU_STG.4 Prevention of audit data loss	Only events triggered by Auditors can be executed when the external database cannot store any more audit logs.

Table 31: SFRs related to Security Audit

6.4 Export and import user data

FDP_ETC.1 Export of user data without security attributes	CRL contains the list of revoked and suspended certificate owners' certificates, CRL's are periodically exported by TOE to repositories such as LDAP/File Server, to communicate the end users the real time status of affected digital certificates. CA Certificates are periodically exported by TOE to repositories such as LDAP/File Server, to communicate the end users to validate the public key. The Officer can export certificate owner's certificate, CA CSR and CRL. The CA administrator can set the schedule to publish CRL.
FDP_ITC.1 Import of user data without security attributes	To identify and authenticate the user by role and grant access to the emCA application Username and user Token pin is required to enter in login page, User need to select role and based on the role selected usernames will be populated and enter the user token PIN after plugging the token to the system. The Officer imports certificate owner's CSR for purpose of issuing of certificate.

Table 32: SFR related to Export and Import of user data

6.5 Password Policy

FIA_SOS.1 Verification of secrets	Password Policy followed in TOE (emCA application): Password must contain atleast 1 Uppercase, 1 Lowercase, 1Digit, 1 Special Character (@, #, %, $) and must be 8 Character long.

Table 33: SFR related to Password Policy

6.6 Cryptographic Operations

FCS_COP.1 Cryptographic operation	The TOE generates and verifies HMAC-SHA256 digest on audit logs, CA/certificate owner's certificates, CRL and backup archives.
FCS_CKM.4 Cryptographic key destruction	

Table 34: SFR related to Cryptographic Operation

6.7 Security Management

FMT_SMF.1 Specification of Management Functions	The TOE ensures m out n authentication; during emCA application initial set up CA administrator has rights to configure "Authentication Matrix" to specify number of users (Max & Min) & can manage the administrator roles by making each user account active or inactive and its related security attributes. TOE has predefined roles and access rights and doesn't have any interface to create roles and map access rights to roles. The following users have access to perform set of
FMT_SMR.1 Security roles	
FMT_MOF.1 Management of security functions behaviour	
FMT_MSA.1 Management of	

security attributes **FMT_MSA.3 Static attribute initialisation** **FMT_MTD.1 Management of TSF data**	actions & functions with respect to their roles: **CA Administrator** has access to: • Initial set up & Registration (Generate ID, Registration Authentication Matrix, Key Generation [8]and Create Admins) • Configurations • Home • CA Hierarchy • User Certificate Management (Search) • CA Certificate Management (Search) • Reports (Except Logs) • Roles & Users Management [Create/Manage (create, edit, delete, enable, disable) Admins] • Application [Setup & Registration (License Renewal (Generated ID, Registration) and Authentication Matrix), emCA Application Keys] • System restore. **Administrator** has access to • Home • CA Hierarchy(Delete key from HSM) • Profile Management • User Certificate Management (Search, CERT/CRL Management (manage CRL->Download CRL)) • CA Certificate Management (Search) • Reports(Except Logs) • Roles & Users Management [Create/Manage(create, edit, delete, enable, disable) Officers/Auditors/Operators] • Application [Setup & Registration (License Renewal (Generated ID, Registration), emCA Application Keys and Scheduler Configuration.] **Officer** has access to : • Home • CA Hierarchy • User Certificate Management (Enrolment, Signing CSR, Search, Revocation/Suspension, Reinstate, CERT/CRL Management • CA Certificate Management (Enrolment, CA Certificates, Signing CSR, Search, and Revocation) • Key Management and Reports (Except Logs) **Auditor** has access to: • Home • CA Hierarchy • Reports (logs only) **Operator** has access to: • Home

[8] Key store generation resides on the external HSM; thus, this function is out of TOE scope, however, the TOE controls access to this function

	• CA Hierarchy • Backup
FPT_ITI.1 Inter-TSF detection of modification	The TOE generates HMAC-SHA256 digest for backup archives when it is exported out of the TOE. The backup archives consist of all TOE configuration. The TOE validates the HMAC-SHA256 digest when a backup archive is used to restore the TOE's configuration.

Table 35: SFR related to security management

7 References

[CC1] Common Criteria Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Version 3.1, Revision 5

[CC2] Common Criteria Information Technology Security Evaluation, Part 2: Security Functional Components, April 2017, Version 3.1, Revision 5

[CC3] Common Criteria Information Technology Security Evaluation, Part 3: assurance components, April 2017, Version 3.1, Revision 5

8 Glossary

Certificate Authority	The IT entity that receives CSR from and issues certificates to certificate owners. It is comprised of a combination of TOE + HSM.
Compromise	The unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other CSPs).
Confidentiality	The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.
Digital signature	A non-forgeable transformation of data that allows proof of the source (with non-repudiation) and verification of the integrity of that data.
Firmware	The programs and data stored in hardware (e.g., ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution. Hardware: the physical equipment used to process programs and data in a CIMC.
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Personal Identification Number (PIN)	A 6 or more character alphanumeric code or password used to authenticate an identity, commonly used in banking applications.
Plaintext key	An unencrypted cryptographic key.
Private key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public.
Protection Profile	An implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs.
Public key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public. (Public keys are not considered CSPs.)
Public key certificate	A set of data that unambiguously identifies an entity, contains the entity's public key, is digitally signed by a trusted party, and binds the public key to the entity.
Security policy	A precise specification of the security rules under which a CIMC shall operate, including the rules derived from the requirements of this document and additional rules imposed by the vendor.
Software	The programs and associated data that can be dynamically written and modified.

Split knowledge	A condition under which two or more entities separately have key components that individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module.
Target of Evaluation (TOE)	An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

9 Acronyms

CA	Certificate Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
COM	Component Object Model
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
CRMF	Certificate Request Message Format
DLL	Dynamic Link Library
DN	Domain Name
DoS	Denial of Service
EAL	Evaluation Assurance Level
EAC	Extended Access Control
EJB	Enterprise Java Bean
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HSM	Hardware Cryptographic Security Module
HTTP	Hypertext Transfer Protocol
ID	Identification
IEC	International Electro-technical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector

JDBC	Java Database Connectivity
JEE	Jakarta Enterprise Edition
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKCS#10	Certification Request Syntax Standard
PKCS#11	Cryptographic Token Interface Standard
PP	Protection Profile
POP	Proof of Possession
RFC	Request for Comment
SAM	Security Assurance Measure
SAR	Security Assurance Requirement
SD	Security Descriptor
SID	Security Identifier
SF	Security Functions
SFP	Security Functions Policy
SFR	Security Functional Requirement
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
VR	Validation Report
VAN	Vulnerability Analysis
VM	Virtual Machine

10 Annex

10.1 Role-based Access Control Matrix

Module	Sub Module	CA Administrator	Administrator	Officer	Auditor	Operator
Initial Setup	ID Generation	x				
	Authentication Matrix Configuration	x				
	Key Generation	x				
	Create Administrators	x				
Dashboard	Dashboard	x	x	x	x	x
CA Hierarchy	CA Hierarchy	x	x	x	x	x
User Certificate Management	Search User Certificate	x	x	x		
	Enrol User Certificate			x		
	Sign User CSR			x		
	Revoke or Suspend User Certificate			x		
	Reinstate User Certificate			x		
CA Certificate Management	Search CA Certificate	x	x	x		
	Enrol CA Certificate			x		
	Sign CA CSR			x		
	Revoke CA Certificate			x		
Profile Management	CRL Profile		x			
	Certificate Profile		x			
	Key Profile		x			
Keystore Management	Manage Keystores		x			
CRL/CERT Management	Manage CRL		Only download	x		
Roles and User Management[9]	Create Officer, Auditor and Operator		x			

[9] User profile creation using soft token is out of TOE scope.

Application	License Renewal	x	x			
	Update Authentication Matrix	x	Only View			
	Scheduler Configuration		x			
Restore	Restore	x				
Reports	Log Reports				x	
	CRL Reports	x	x	x	x	
	Certificate Statistics Reports	x	x	x	x	
	All Certificates Reports	x	x	x	x	
	Active Certificates Reports	x	x	x	x	
	Revoked Certificates Reports	x	x	x	x	
	Suspended Certificates Reports	x	x	x	x	
	Expired Certificates Reports	x	x	x	x	
Backup	Backup					x

Table 36: Role-based access control matrix

10.2 Non-TOE Components

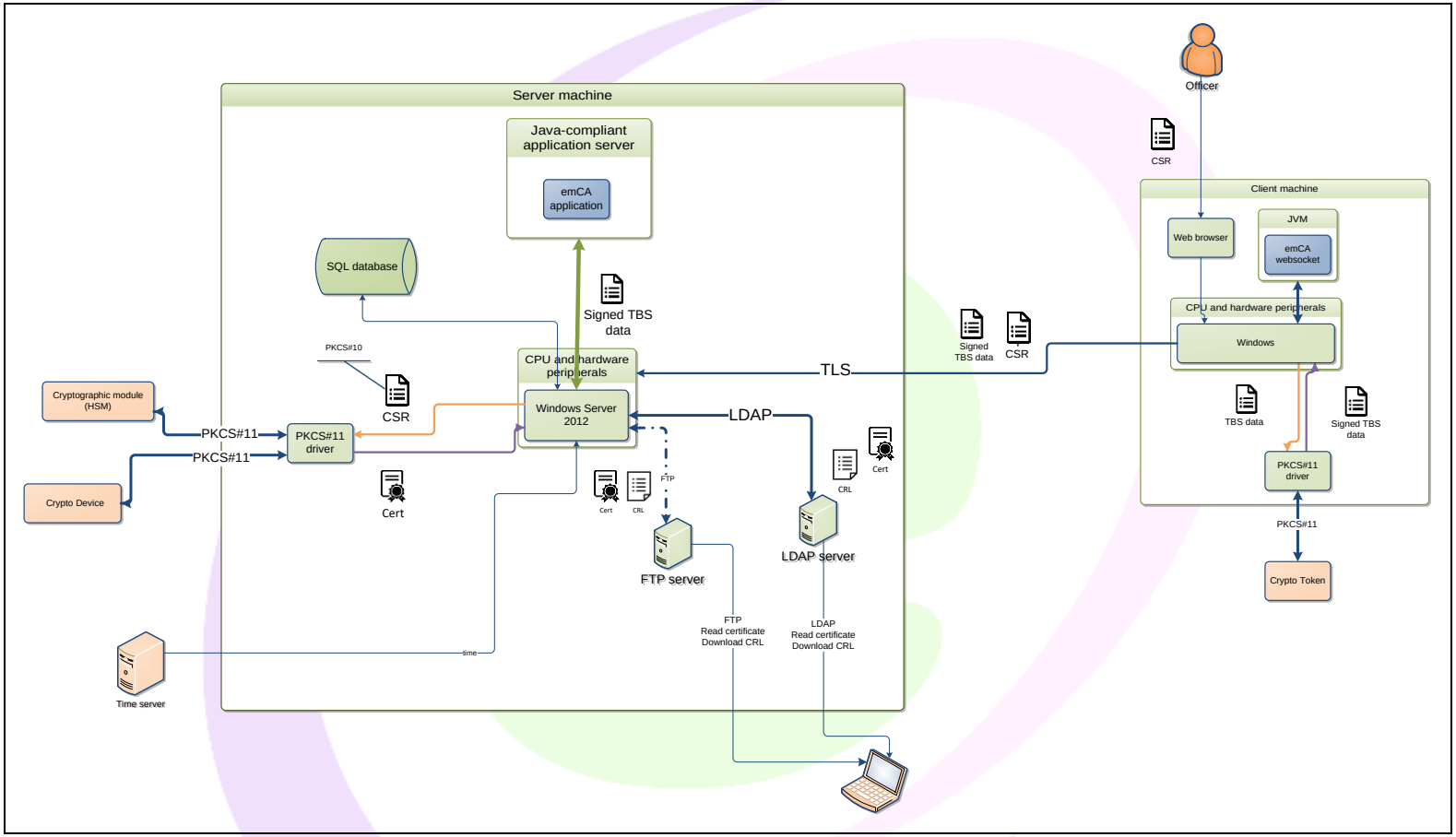

Figure 5: Non-TOE component (enlarged)