Enabling trusted identities

Nexus Certificate Manager

Nexus CM 8 Security Target

Requirements Specification

Technology Nexus Secured Business Solutions AB
Telefonvägen 26
SE-126 26 Hägersten
Phone: +46 8 685 45 60
contact.se@nexusgroup.com

Document ID: Nexus CM 8 Security Target

Version: 1.0, 2020-03-02

Contents

1 Security Target Introduction

This document is the Security Target for Nexus Certificate Manager 8.0.0 and Nexus OCSP Responder 6.0.2. The document was produced to enable this product to be evaluated against the Common Criteria. For information about the Common Criteria requirements, and the required content of the Security Target, please refer to references [CC].

This Security Target (ST) has been structured in accordance with [CC] Part 1. The main sections of the ST are the introduction, security problem definition, security objectives, security requirements, TOE summary description and annexes.

The introduction provides general information about the TOE, serves as an aid to understand the nature of the TOE and its security functionality and provide context for the evaluation. In the introduction is also a list of abbreviations, a glossary of terms for this ST and the list of references.

The security problem definition describes the security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. The TOE security environment includes:

- assumptions regarding the TOE's intended usage and environment of use
- threats relevant to secure TOE operation
- organisational security policies with which the TOE must comply

The security objectives reflect the stated intent of the ST. They pertain to how the TOE will counter identified threats and how it will cover identified organisational security policies and assumptions. The security objectives are divided into security objectives for the TOE and for the environment. The security objectives rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security problem definition and that they are suitable to cover them.

The extended components section identifies any extended security requirements, i.e. security requirements not defined in CC Part 2 and 3 that are used within this ST.

The security requirements section provides detailed requirements, in separate subsections, for the TOE and its environment. The security requirements are further divided into the TOE security functional requirements and the TOE security assurance requirements.

The TOE summary specification addresses the security functions that are represented by the TOE to answer the security requirements.

1.1 Security Target Reference

Title	Nexus CM 8 Security Target
ST Version	1.0
Date	2020-03-02

1.2 Target of Evaluation (TOE) Reference

Developer	Technology Nexus Secured Business Solutions AB
Name, version	Nexus Certificate Manager version 8.0.0.
Name, version	Nexus OCSP Responder version 6.0.2.

1.3 TOE Overview

1.3.1 TOE Type and TOE Usage

Nexus Certificate Manager consists of server and client software components that enables operation of a Certification Authority (CA) and OCSP Responder within a Public Key Infrastructure (PKI). It provides Certificate Issuing and Management Components (CIMC).

The configuration options of the CIMC software enables establishment of a wide range of PKI functionality, for establishment of Certification Authority and OCSP Responder services. Based on the software license obtained by the customer can the software be used for customized operations on-premises or in a hosted environment, etc.

1.3.2 TOE Major Security Features

All interactions between the Certificate Manager Client and Server components take place over secured channels. All requests that involve changing of status are required to be digitally signed by authorized users and all requests are logged to an Audit Log.

As a result of the above interactions all significant CA policy changes and CA outputs (e.g. user certificates and certificate status information) are digitally signed and all actions are logged.

The TOE OCSP Responder interface is provided with the Nexus OCSP Responder, which enables clients to obtain up-to-date certificate status information using the standardized OCSP protocol. The OCSP responder can optionally be used with a front-end Proxy OCSP Responder, which can be realized by configuring the Nexus OCSP Responder to act as proxy.

The main security features of the TOE are:

- Security Audit
- Roles
- Access Control
- Identification and Authentication
- Remote Data Entry and Export
- Key Management: Key Storage, Key Destruction and Key Export
- Certificate Profile Management
- Certificate Revocation List Profile Management
- OCSP Profile Management
- Certificate Registration
- Certificate Revocation (CRL and OCSP Validation)

1.3.3 Required non-TOE Hardware, Software and Firmware

Additional hardware and software components are required in order to operate the CIMC and to have it accredited. These components are considered to be part of the TOE environment and not part of the TOE.

The TOE Server software components are installed in a supported operating system that executes directly on hardware or on virtualized machine. Database software is also required. The TOE software itself runs within a Java Run Time Environment (JRE). The TLS library used by the TOE is also provided by the JRE. Both the JRE and the TLS library provided by the JRE are part of the operational environment. The TLS library has been tested by the developer, based on which the developer has verified that the TLS protocol and the associated cryptographic functionality work as expected in the context of the TOE testing.

A further hardware/firmware requirement is for one or more Secure Signature Creation Devices (SSCDs) for use in signing data on behalf of the CA. These devices are validated/evaluated/accredited Hardware Security Modules (HSMs) and are also referred to as "FIPS 140-2 validated cryptographic module" in this Security Target. A device driver software is required to communicate with an HSM in accordance with the PKCS#11 cryptographic interface. The PKCS#11 driver is part of the TOE environment. Any FIPS 140-2 or CC EAL 4+ evaluated HSM with support for PKCS#11 can be used with the TOE.

Furthermore, the digital signatures created by SSCDs are verified by the TOE using the standard Java or Bouncy Castle crypto library. In cases where the standard Java crypto library does not support the signature algorithm/scheme used by the SSCD (such as Brainpool elliptic curves and RSA-PSS), the Bouncy Castle library is used to verify the signature. The standard Java crypto library is provided by the JRE and therefore part of the TOE environment. The Bouncy Castle crypto library is also part of the TOE environment.

Finally, whilst Client software is supplied as part of Certificate Manager and customised client components can be written using a Java API (CM SDK) or other API’s, these components are not part of the TOE.

Non-TOE components used in evaluation:

- CentOS Linux 7 (Core)
- OpenJDK Runtime Environment AdoptOpenJDK (build 11.0.4+11)
- PostgreSQL 11.5
- nCipher nShield F2 500+, v11.72.02.
- Utimaco SecurityServer HSM simulator V4.30.0, corresponding to CryptoServer Se-Series Gen2.

Additional Non-TOE components used during TOE development and test:

- Windows 2012, Oracle Java 11.0.2, MS SQL Server 2012.
- Windows 2016, AdoptOpenJDK 11.0.2, MS SQL Server 2017.
- CentOS 7, AdoptOpenJDK 11.0.3 with Oracle 18.3, PostgreSQL 11 and MySQL 8.0.
- OpenSUSE LEAP 15.0, Oracle Java 11.0.3 with Oracle 18.3, PostgreSQL 11 and MySQL 8.0.

1.4 TOE Description

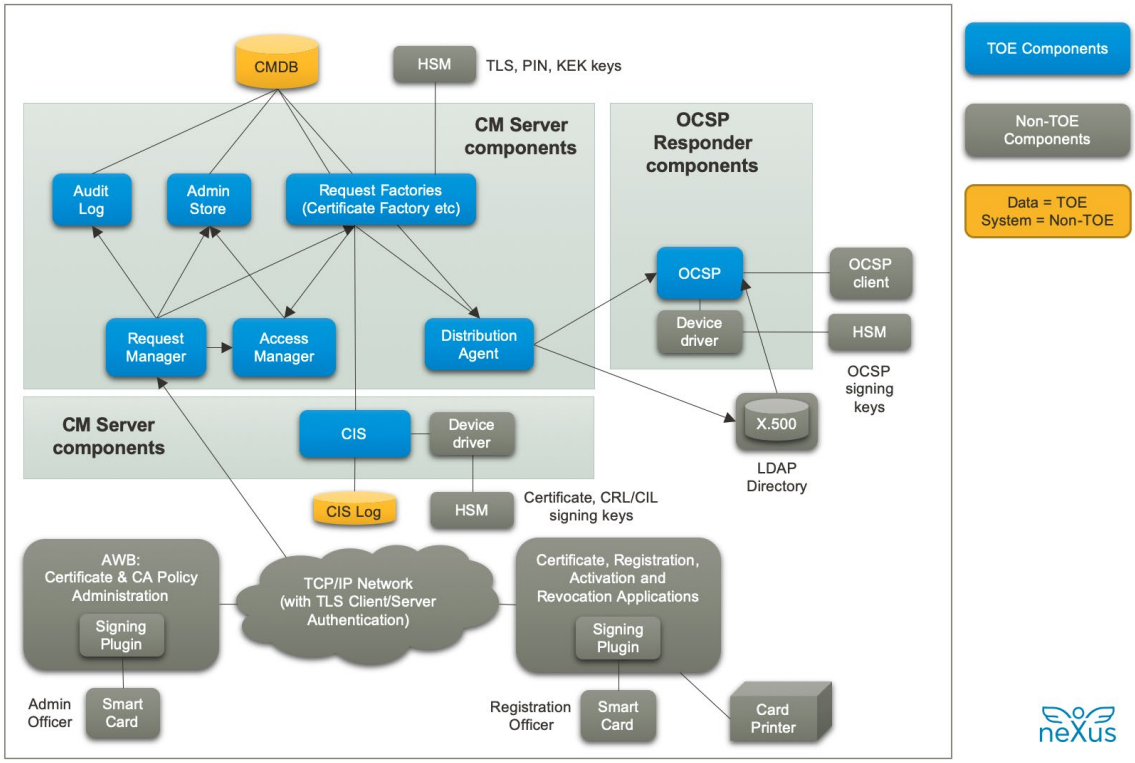

Figure 1: Nexus Certificate Manager, overview of TOE components.

Figure 1 shows that more than one HSM can be used for generation, protection, and operational use of cryptographic keys with the TOE's cryptographic functions. The choice of using a single or several HSM's in a deployment depends on

different factors, such as a security policy that stipulates HSM-separation of different keys, performance requirements, or network separation of components, etc. Digital signatures created by HSM's are verified by the TOE using either the standard Java or Bouncy Castle crypto library depending on used algorithm.

Together the TOE components support the following CIMC functions:

- Logical Access Control and Authorization
- CA Policy Administration
- Certificate and Subject Data Registration
- Certificate Preparation
- Certificate Signing
- Certificate Activation
- Certificate Status Information Provision – OCSP
- Certificate Status Information Provision – CRL/CIL
- Certificate Publication
- Certificate Revocation
- Key Archiving and Recovery
- PIN Management
- Audit and CIS Log Review
- Batch Processing
- Initial Boot Process

1.4.1 TSF Summary

The security services that are provided by the TOE, including the CIMC functions listed above, are described in this section. Each of the main security functions is further defined and mapped to requirements in Section 7 TOE Summary Specification.

1.4.1.1 Roles

The TOE users are known collectively as Officers. The TOE enables configuration of officer roles on a fine-grained level for restricting officers to perform specific tasks only, e.g. as prescribed by the CA operational policies. The role configuration is done in officer profiles, which are applied to the officer objects. A unique officer is created by associating a profile either to a certificate issued by the TOE, to a system unique subject, or to a token serial number. Even though many role combinations can be defined in a profile, there are three general types of Officers used to separate administrative from operational duties and for establishing a secure connection from client to server:

- Administration Officers
- Registration Officers
- Authentication Officers

Administration Officers are responsible for administering the security policies of the TOE (i.e. setting up CA Policies, auditing etc.), whereas Registration Officers are responsible for registering users, issuing certificates etc. The Certificate Manager has well defined interfaces for Administration Officers to administer the CA and for Registration Officers to perform certificate registration, certificate activation and

revocation. These interfaces are invoked via client tools which are part of the TOE environment. The administrative tool for Administration Officers is the Administrator's Workbench (AWB) whereas there exist a number of client tools for the Registration Officers.

Authentication Officers have restricted rights, not permitting an unattended service to do other tasks than establishing the TLS connection between the core server and the client, listing of certificates, and the forwarding of certification requests signed by a Registration Officer. Note that the TLS library is provided by the JRE and is therefore part of the TOE environment.

Another role is Administrator with the rights to generate component keys other than CA keys, perform OCSP profile management, and Secret Key Storage.

CA Policy Administration
In order to fulfil its primary intended function (i.e. to issue and manage CA certificates and end user PKI certificates), the TOE operates in accordance with a CA Policy. This policy is established by the action of Administration Officers in accordance with various guidance documents. CA Policy means the creation of Officers with appropriate authorization levels and the creation of CA keys, CA certificates, various Certificate Procedures (e.g. defining the content and format of end-user certificates), CRL and CIL Procedures, Distribution Rules, Publication Procedures, and Key Procedures.

To create or change a CA Policy, Administration Officers make use of AWB. Two Administration Officers sign CA Policy changes and all changes are written via the Admin Store component to the 'AdminStore' table in the Certificate Manager Database (CMDB). They are also written as signed Audit Records to the 'AuditLog' table in the same database.

CA Policies must be appropriately signed for use in the TOE and the signature validation protects against unauthorized change. Accordingly, the CA Policy is established in a controlled and traceable manner. For a further discussion of CA Policy please refer to the guidance documents.

Initiation Boot Process
As described previously, the CA Policy is established and maintained by the action of Administration Officers. When the system is first installed however, no true Administration Officers are known to the system. Instead the initial installed system is pre-configured to run with two default Officers known as the Boot Officers. These Officers are responsible for creating the first true users of the system, two real Administration Officers. These Administration Officers then become responsible for creating further Officers and setting up the CA Policies.

1.4.1.2 Identification and Authentication

The TOE requires identification and authentication before performing any security-relevant functions. Identification and authentication of users is accomplished by use of certificates, i.e. PKI based signed challenges and requests. During the TLS negotiation, the TOE user authenticates to the server and while the TLS session is still open, the TOE maintains the identity of the user.

The TOE User identification is a TLS Client Authentication Process, whereby a mutual authentication is achieved between server and client. Thus, it is not

possible for authentication data to be forged or reused (as a new challenge is issued each time). The TLS library used by the TOE is part of the TOE environment.

Administration Officers and Registration Officers
All requests received by the Certificate Manager servers are first handled by the Request Manager component. Request Manager authenticates the connecting Officer, and during this process a client/server authenticated TLS session is established between the Certificate Manager Server and the Certificate Manager Client. Administration Officers and Registration Officers are issued with cryptographic smart cards on which are stored their private authentication and signature (non-repudiation) keys. These keys are used by the Officers to authenticate themselves in a TLS connection to the Certificate Manager, as well as to sign policy changes, certificate requests, etc. After authentication, all data transfers are protected with regard to confidentiality and integrity.

OCSP Clients
The TOE configuration for authentication of OCSP users defines whether users must be authenticated or not to accept and reply to OCSP requests. OCSP clients can be identified and authenticated by the OCSP Responder when TLS is enabled, or by enforcing use of signed OCSP client requests.

1.4.1.3 Access Control

Administration Officers and Registration Officers
For each request received by Certificate Manager, the Access Manager component ensures that the authorization level of the Officer is adequate. The Access Manager component ensures that the authorization level of Officers, once authenticated, are suitable for all given requests (i.e. registration requests, revocation requests, etc.). All other components rely upon the Access Manager to perform these checks.

Hence, authentication is performed by the Request Manager component, whereas authorization is carried out by the Access Manager. The Request Manager and Access Manager therefore ensure together that the TOE does not accept certificate request data through channels that are not secure and it does not accept data that is not signed by an authorized user.

OCSP Clients
Authorization of subject is made either by matching the subject name to a table of authorized users or by matching the certificate to the content of a trust store. OCSP client identification and authentication is optional, but enforcement is decided upon by the CIMC policies.

1.4.1.4 Certificate Registration

Certificate and Subject Data Registration
Signed certificate requests (and/or certificate orders) are received via the Request Manager component over a secure channel (as previously discussed). The Request Manager is responsible for distributing the incoming request to the other factory components. For each request, the Access Manager verifies that it is issued by an authorized user, and the received certificate request data is stored and logged in the CMDB.

Subject data pre-registration is done by a Registration Officer as preparation to receiving certificate requests in a scenario where CA operation requires automated validation of certificate request content from end-entities, or to prepare for smart card batch production. The Registration Officer signs the subject data and the request is authorized in the same way as with certificate requests.

Certificate Preparation
The data content of a certificate is prepared by the Certificate Factory[1] component using the signed certificate request data plus possibly other data (determined by the CA Policy – see Section 1.4.1.1) and the public key read from the user's smart card.

The user's public key is either included as part of the signed certificate request data (in the case of single issuance of a smart card at a Registration Authority workstation) or as part of batch card production (at a Batch Explorer, Card Production Workstation).

Batch Processing
The Certificate Manager issues smart cards with key pairs and certificates that bind the name of the owner of the smart card to the corresponding public key. Batch processing for volume production of smart cards involves steps of card order registration, registration of data for certificates, visual personalization, logistical handling, PIN letter distribution and chip personalization.

Certificate Signing
Once the certificate data has been prepared (including the user's public key) it is sent to the 'Certificate Issuing System' (CIS) for signing by a CA key. The CIS is responsible for signing the certificate by sending the data via the HSM driver for signature by the HSM.

CIS signature requests are logged to the CIS log file, and the CIS Log entries are signed for integrity protection.

Certificate Activation
Certificate activation requests are received over a secure channel, and the Access Manager ensures the request is authorized. Upon activation, the certificate will be added to the Certificate Issuance List (CIL) and distributed to the OCSP responder to enable provision of certificate status information to OCSP clients.

The Certificate Factory initiates the publication of certificates if they are to be published as soon as they are created. Otherwise the Publication Factory is responsible for initiating the publication of certificates as a result of a delayed publication request from a Registration Officer.

[1] Certificate Factory is one of several Factory components that handle requests from Request Manager. The generic term for these components is Request Factories. The other Request Factory components are the following: Publication Factory, Revocation Factory, CRL factory and Key Archiving and Recovery (KAR) Factory.

1.4.1.5 Certificate Revocation (CRL and OCSP validation)

In addition to activation of a certificate (and consequently making this status available via the OCSP Responder interface) the certificate may (or may not) be published to an LDAP directory. Hence, the certificate status export regards distribution of certificates and CILs/CRLs to the various LDAP directories, HTTP servers, OCSP responders, as specified in the CA Policy Distribution rules.

Certificate Status Information Provision – OCSP

Certificate Activation and Certificate Revocation status provision over OCSP with the OCSP Responder is realized by publishing CILs and CRLs. A CIL contains all certificates issued by the signing CA, whereas a CRL lists all revoked certificates.

Expired certificates are not removed and therefore the CIL contains a definite statement whether a specific certificate serial number has ever been issued. The content of the CIL can be configured to contain only activated certificates.

It is allowable for the OCSP Responder not to reply. However, if it does reply then the information must be guaranteed to be correct.

Certificate Status Information Provision – CRL

Certificate Status Information Provision with CRL is handled in accordance with RFC 5280 and RFC 5755.

The CIS is responsible for the signing of CRLs and CILs.

1.4.1.6 Certificate Profile Management

The TOE configuration of certificate profiles is performed by Administrator Officers, who specify the acceptable values of the certificate’s fields and extensions.

1.4.1.7 OCSP Profile Management

The TOE configuration of OCSP profiles is performed by Administrators. OCSP responder profiles enables configuring acceptable values, fields and types in OCSP responses and is in accordance with RFC 6960.

1.4.1.8 Certificate Revocation List Profile Management

The TOE certificate revocation list profile management, using CRL formats and CRL procedures, is performed by Administration Officers, and is in accordance with ISO/ITU X.509, RFC 5280, RFC 5755.

1.4.1.9 Key Management: Key Storage, Key Destruction and Key Export

Key Storage

The CIMC server enables clients to submit asymmetric Key Archiving and Recovery, KAR, requests. The KAR Factory module processes the archiving and recovery request. An HSM must be used for key generation and for protection of archived keys. Private keys are first encrypted and then stored in the CMDB.

Key Destruction

Cryptographic keys are destroyed by FIPS 140-2 validated cryptographic module in accordance with the FIPS 140-2 cryptographic key destruction method to ensure that an untrusted entity cannot use a trusted entity's key to sign malicious code. Note: The cryptographic module is not part of the TOE, but the TOE environment.

Key Export
The TOE ensures that private and secret keys are protected when they are transmitted to and from the TOE: the keys shall only be exported from the TOE in encrypted form or using split knowledge procedures.

PIN Management
Smart card PINs and PUKs are stored encrypted in CMDB. An HSM must be used for highest level of protection. Storing PIN/PUK is an optional choice of providing service for PIN/PUK retrieval after authorization of a PIN/PUK retrieval request.

1.4.1.10 Remote Data Entry and Export

Remote data entry and export are achieved through an HTTPS mutually authenticated connection, which is validated and auditable at all times.

The TOE enables secure data entry for certificate creation, registration, revocation, keys, PIN/PUK and other data, and supports secure export of certificates CRLs, CILs, keys, PIN/PUK and OCSP responses.

1.4.1.11 Security Audit

Audit Log
The Audit Log in the database contains signed requests from the TOE users that can change the configuration or state of any policy object or certificate. Policy Objects are a type of objects used by the Nexus Certificate Manager to hold the certificate policy (CP) and certification practice statement (CPS).

CIS Log
CIS signature requests are logged to the CIS log file. This file consists of digitally signed, chained log records. All CIS Log entries are signed by the CIS. The chaining is achieved by including the previous record's hash in the next record's signature. Modification to the log can thus be detected during the following read operation.

Audit and CIS Log Review
Review of the Audit and CIS Logs is performed by an Administration Officer that has the role of 'Audit tasks'. The Officer uses the AWB workstation to request and search for the log records to be displayed.

1.4.2 Physical Scope of the TOE

The scope of the TOE is the Certificate Manager's Server and the OCSP Responder, and the Certificate Manager and the OCSP Responder documentation. Both the software and the documentation can be downloaded from Nexus Support Portal, along with other software components and documentation that are not within the TOE scope. The downloaded software can be installed by the customers themselves. The software components documentation is listed below.

Certificate Manager Server Components

The servers that the Certificate Manager Server Components have been installed on are considered an abstract machine from the TOE installation view. Any hardware, firmware and software needed to implement this abstract machine are outside the physical boundaries of the TOE. The TOE software itself runs within a Java Run Time Environment (JRE), which is part of the operational environment.

The TLS library used by the TOE is also provided by the JRE. Both the JRE and the TLS library provided by the JRE are part of the operational environment. Nevertheless, it is essential that these servers are placed within a physically secured facility.

Hardware and firmware used in Hardware Security Modules and software used for interfacing these devices are outside the physical boundaries of the TOE.

The main server components included in the TOE are Certificate Factory, Certificate Issuing System, and the OCSP Responder. Certificate Issuing System can operate stand-alone or as part of Certificate Factory.

The certificate request data, certificate status data, and the ProductionOrders, AdminStore and AuditLog tables are considered to be part of the TOE but not the entire CMDB database or the database software. These are considered to be part of the TOE environment. Database table definitions can be found in the guidance document Nexus Certificate Manager Technical Description. The CIS log file is considered to be part of the TOE but not the disk subsystem.

Intermediate Server Components

A few intermediate server components operate as clients to the core CA under the collective name of Protocol Gateway for enabling certificate enrolment using the standards-based protocols CMC, CMP, SCEP, and EST. Protocol Gateway also provides a restful API (RestAPI), a PKCS#12 issuing service (AST), PKCS#10 uploading (EUI), Windows certificate Enrolment Proxy (WinEP), and a health check tool for monitoring of the core server (Ping). New server components for supporting additional protocols or services are added with new versions of Certificate Manager. The Protocol Gateway services connects to the core server using the CM SDK programmer's API and authenticate the TLS connection using an Authentication Officer.

The Protocol Gateway components are not part of the TOE.

Certificate Manager Client Components

The Certificate Manager clients are not part of the TOE.

The clients will create digital signatures on policy objects as required by the TOE, with private key belonging to an authorized officer. Hardware and software used to access the key, e.g. in smart card, are outside the physical boundaries of the TOE.

Guidance Documents

The following guidance documents contains the TOE specific information for the customer to read and are delivered with the complete product distribution and are part of the standard product documentation:

- Nexus Certificate Manager Technical Description. This document provides technical information of all Nexus components delivered.
- Nexus Certificate Manager Installation Guide. This provides installation instructions for the installation of a typical system and an evaluated configuration.

- Nexus Certificate Manager CA Administrator’s Guide.
- Nexus Certificate Manager Registration Officer’s Guide.
- Nexus Certificate Manager System Administrator’s Guide.
- Nexus Certificate Manager CC Configuration Guide.
- Nexus OCSP Responder Reference Guide.

2 Conformance Claims

This ST is CC Part 2 extended and CC Part 3 conformant. This ST claims conformance to CC version 3.1 Revision 5.

This ST claims demonstrable conformance to Certificate Issuing and Management Components Protection Profile [CERT-PP]. This ST claims conformance to the EAL4 package of security assurance requirements, augmented with ALC_FLR.2.

The [CERT-PP] requires demonstrable compliance. The PP was evaluated and certified under the Canadian scheme and the certification report is available here [CERT-CR].

3 Security Problem Definition

With exception of the additional clarification of the assets in the threat description the security problem definition was taken directly from the [CERT-PP].

3.1 Assumptions

This section specifies the assumptions on the TOE environment that are necessary for the TOE to meet its security objectives.

The assumptions are organized in three categories: personnel (assumptions about administrators and users of the system), physical (assumptions about the physical location of the TOE or any attached peripheral devices), and connectivity (assumptions about other IT systems that are necessary for the secure operation of the TOE).

Personnel assumptions	
A.Auditors Review Audit Logs	Audit logs are required for security-relevant events and must be reviewed by the Auditors.
A.Authentication Data Management	An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.)
A.Competent Administrators, Operators, Officers and Auditor	Competent Administrators, Operators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.
A.Cooperative Users	Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner.
A.CPS	All Administrators, Operators, Officers, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.

A.Disposal of Authentication Data	Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).
A. Malicious Code Not Signed	Malicious code destined for the TOE is not signed by a trusted entity.
A.Notify Authorities of Security Issues	Administrators, Operators, Officers, Auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
A.Social Engineering Training	General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks.
Connectivity assumptions	
A.Operating System	The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats identified in this PP.
Physical assumptions	
A.Communications Protection	The system is adequately physically protected against loss of communications i.e., availability of communications.
A.Physical Protection	The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.

3.2 Threats

The following threats are addressed by the TOE and the TOE environment.

The threats are organized in four categories: authorized users, system, cryptography, and external attacks depending on the threat agent and the type of functionality affected.

Authorized Users

Threat agent for the following threats is an authorized user. Asset that can be compromised are the CIMC and/or the systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses. The latter systems are termed relying party systems.

Authorized users' related threats	
T.Administrative errors of omission	Administrators, Operators, Officers or Auditors fail to perform some function essential to security.

	Clarification: Functions essential to security are the management functions that are described in Table 2 under FMT_MOF.1 (iteration 2).
T.Administrators, Operators, Officers and Auditors commit errors or hostile actions	An Administrator, Operator, Officer or Auditor commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur. Clarification: Changes to the security policy are changes in security management functions behaviour as described in Table 2 under FMT_MOF.1 (iteration 2).
T.User abuses authorization to collect and/or send data	User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data. Clarification: Sensitive or security-critical data is any information that authorized users will be given access to that may not be disclosed to other parties. While it cannot be prevented for authorized users, access to any information as part of the operation of the TOE will be audited. This is described in Table 1 under FAU_GEN.1 Audit data generation (iteration 2) in rows "Local Data Entry", "Remote Data Entry", "Data Export and Output".
T.User error makes data inaccessible	User accidentally deletes user data rendering user data inaccessible.
System related threats	
T.Critical system component fails	Failure of one or more system components results in the loss of system critical functionality. Threat agent in this case is the CIMC hardware. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.
T.Flawed code	A system or applications developer delivers code that does not perform according to specifications or contains security flaws. Threat agent in this case is the TOE developer. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.
T.Malicious code exploitation	An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets. Threat agent could be an authorized user, TOE itself, or an unauthorized user. Adverse action can be compromise of the

	security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.
T.Message content modification	A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient. Threat agent is an unauthorized user. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.
Cryptography related threats	
T.Disclosure of private and secret keys	A private or secret key is improperly disclosed. Threat agent is the authorized user or erroneous protocol. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.
T.Modification of private/secret keys	A secret/private key is modified. Threat agent is the authorized user or erroneous protocol. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.
T.Sender denies sending information	The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction. Threat agent is a subscriber to CIMC. Adverse action can be reduced trust in CIMC.
External attacks	
T.Hacker gains access	A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability. Threat agent is the unauthorized user. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.
T.Hacker physical access	A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises. Threat agent is the unauthorized user. Adverse action can be compromise of the security of the CIMC and/or relying party

	systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.
T.Social engineering	A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation. Threat agent is the unauthorized user. Adverse action can be compromise of the security of the CIMC and/or relying party systems that rely on the PKI objects such as certificates, CRLs, or OCSP Responses.

3.3 Organisational Security Policies

The following organisational security policies are enforced by the TOE and the TOE environment.

P.Authorized use of information	Information shall be used only for its authorized purpose(s).
P.Cryptography	FIPS-approved or NIST-recommended cryptographic functions shall be used to perform all cryptographic operations.

4 Security Objectives

The security objectives provide a concise and abstract statement of the intended solution to the problem as defined in the Security Problem Definition (see section 3). It will describe which security needs will be addressed by the TOE and which will be addressed by the TOE environment, in the form of a statement of security objectives.

All the security objectives for the TOE, TOE environment, and both TOE and TOE environment, have been directly replicated from the [CERT-PP].

4.1 Security Objectives for the TOE

The following security objectives are to be met by the TOE.

O.Certificates	The TSF must ensure that certificates, certificate revocation lists, and certificate status information are valid.
O.Preservation/trusted recovery of secure state	Preserve the secure state of the system in the event of a secure component failure and/or recover to a secure state.
O.Non-repudiation	Prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message.
O.Control unknown source communication traffic	Control (e.g., reroute or discard) communication traffic from an unknown source to prevent potential damage.
O.Security roles	Maintain security-relevant roles and the association of users with those roles.
O.Data import/export	Protect data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.
O.Detect modifications of software, and backup data	Provide integrity protection to detect modifications to software, and backup data.
O.Individual accountability and audit records	Provide individual accountability for audited events. Record in audit records: date and time

	of action and the entity responsible for the action.
O.Integrity protection of user data and software	Provide appropriate integrity protection for user data and software.
O.Limitation of administrative access	Design administrative functions so that Administrators, Operators, Officers and Auditors do not automatically have access to user objects, except for necessary exceptions. Control access to the system by Operators and Administrators who troubleshoot the system and perform system updates.
O.Maintain user attributes	Maintain a set of security attributes (which may include role membership. access privileges, etc.) associated with individual users. This is in addition to user identity.
O.Manage behavior of security functions	Provide management functions to configure, operate, and maintain the security mechanisms.
O.Procedures for preventing malicious code	Incorporate malicious code prevention procedures and mechanisms.
O.Protect stored audit records	Protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.
O.Protect user and TSF data during internal transfer	Ensure the integrity of user and TSF data transferred internally within the system.
O.React to detected attacks	Implement automated notification (or other responses) to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent.
O.Respond to possible loss of stored audit records	Respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.
O.Restrict actions before authentication	Restrict the actions a user may perform before the TOE authenticates the identity of the user.
O.Security-relevant configuration management	Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.
O.Time stamps	Provide time stamps to ensure that the sequencing of events can be verified.
O.User authorization management	Manage and update user authorization and privilege data to ensure they are consistent with organizational security and personnel policies.

4.2 Security Objectives for the TOE Environment

The following security objectives are to be met by the TOE environment.

OE.Administrators, Operators, Officers and Auditors guidance documentation	Deter Administrator, Operator, Officer or Auditor errors by providing adequate documentation on securely configuring and operating the CIMC.
OE.Configuration Management	Implement a configuration management plan. Implement configuration management to assure identification of system connectivity (software, hardware, and firmware), and components (software, hardware, and firmware), auditing of configuration data, and controlling changes to configuration items.
OE.Auditors Review Audit Logs	Identify and monitor security-relevant events by requiring auditors to review audit logs on a frequency sufficient to address level of risk.
OE.Authentication Data Management	Ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) through enforced authentication data management (Note: this objective is not applicable to biometric authentication data.)
OE.Communications Protection	Protect the system against a physical attack on the communications capability by providing adequate physical security.
OE.Competent Administrators, Operators, Officers and Auditors	Provide capable management of the TOE by assigning competent Administrators, Operators, Officers and Auditors to manage the TOE and the security of the information it contains.
OE.Cooperative Users	Ensure that users are cooperative so that they can accomplish some task or group of tasks that require a secure IT environment and information managed by the TOE.
OE.CPS	All Administrators, Operators, Officers and Auditors shall be familiar with the certificate policy (CP) and the certification practices statement (CPS) under which the TOE is operated.
OE.Cryptographic functions	The TOE must implement approved cryptographic algorithms for encryption/ decryption, authentication, and signature generation/verification; approved key generation techniques and use validated cryptographic modules. (Validated is defined as FIPS 140-2 validated)
OE.Disposal of Authentication Data	Provide proper disposal of authentication data and associated privileges after access has been removed (e.g., job termination, change in responsibility).

OE.Installation	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner, which maintains IT security.
OE.Lifecycle security	Provide tools and techniques used during the development phase to ensure security is designed into the CIMC. Detect and resolve flaws during the operational phase.
OE.Malicious Code Not Signed	Protect the TOE from malicious code by ensuring all code is signed by a trusted entity prior to loading it into the system.
OE.Notify Authorities of Security Issues	Notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
OE.Operating System	The operating system used is validated to provide adequate security, including domain separation and non-bypassability, in accordance with security requirements recommended by the National Institute of Standards and Technology.
OE.Periodically check integrity	Provide periodic integrity checks on both system and software.
OE.Physical Protection	Those responsible for the TOE must ensure that the security-relevant components of the TOE are protected from physical attack that might compromise IT security.
OE.Repair identified security flaws	The vendor repairs security flaws that have been identified by a user.
OE.Security roles	Maintain security-relevant roles and the association of users with those roles.
OE.Social Engineering Training	Provide training for general users, Administrators, Operators, Officers and Auditors in techniques to thwart social engineering attacks.
OE.Sufficient backup storage and effective restoration	Provide sufficient backup storage and effective restoration to ensure that the system can be recreated.
OE.Trusted Path	Provide a trusted path between the user and the system. Provide a trusted path to security-relevant (TSF) data in which both end points have assured identities.
OE.Validation of security function	Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.
OE.Data import/export	Protect data assets when they are being transmitted to and from the TOE, either through

	intervening untrusted components or directly to/from human users.
OE.Detect modifications of firmware	Provide integrity protection to detect modifications to firmware.
OE.Individual accountability and audit records	Provide individual accountability for audited events. Record in audit records: date and time of action and the entity responsible for the action.
OE.Integrity protection of user data and software	Provide appropriate integrity protection for user data and software.
OE.Limitation of administrative access	Design administrative functions so that Administrators, Operators, Officers and Auditors do not automatically have access to user objects, except for necessary exceptions. Control access to the system by Operators and Administrators who troubleshoot the system and perform system updates.
OE.Manage behavior of security functions	Provide management functions to configure, operate, and maintain the security mechanisms.
OE.Object and data recovery free from malicious code	Recover to a viable state after malicious code is introduced and damage occurs. That state must be free from the original malicious code.
OE.Procedures for preventing malicious code	Incorporate malicious code prevention procedures and mechanisms.
OE.Protect user and TSF data during internal transfer	Ensure the integrity of user and TSF data transferred internally within the system.
OE.React to detected attacks	Implement automated notification (or other responses) to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent.
OE.Require inspection for downloads	Require inspection of downloads/transfers.
OE.Restrict actions before authentication	Restrict the actions a user may perform before the TOE authenticates the identity of the user.
OE.Security-relevant configuration management	Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.

4.3 Security Objectives Rationale

The security objectives rationale consists of a tracing back from the security objectives to the security problem definition and a set of justifications that show that all threats, organisational security policies and assumptions are effectively addressed by the security objectives.

Both the security problem definition and the security objectives are taken directly and unchanged from the [CERT-PP]. The security objectives rationale of [CERT-PP] is applicable and has therefore not been reproduced here.

5 Extended Components Definition

This Security Target does not define its own extended components. The extended components have been taken directly from the extended components defined in [CERT-PP].

The extended components from the [CERT-PP] can be identified by the use of the keyword “CIMC” in the requirement component and element identifiers.

6 Security Requirements

6.1 Security Functional Requirements for the TOE

The following convention is used for operations applied to the Security Functional Requirements: Assignments, selections and refinements that have been performed by the Protection Profile are indicated by underscore. For operations performed within the Security Target the following conventions are used: Assignment and selection are indicated by **bold**. Refinements are indicated by **bold underscore** for additions and by ~~**bold strike through**~~ for deletions. Iterations are identified by adding a letter or explicitly marked as such, e.g. FAU_GEN.1 Audit data generation (iteration 2). This is following the conventions used in the [CERT-PP].

Note: References in the SFRs to chapters and sections made in the [CERT-PP] that have been updated in the ST have not been marked as refinements, since their meaning is unchanged. Also, all tables used in the SFRs that comes from the PP have not been marked. This is also consistent with markings done in the PP. Since several SFRs intended for the TOE environment into the [CERT-PP] now are part as SFRs for the TOE, we have changed the refinement made by the PP from "IT environment" into "TSF". None of these refinements are marked as refinements as long as this corresponds to the original CC Part 2 SFR.

Furthermore, Section 6.2 has been added to include the Security Functional Requirements for the TOE environment that are part of the [CERT-PP].

6.1.1 CIMC TOE Access Control Policy

The TOE shall support the administration and enforcement of a CIMC TOE access control policy that provides the capabilities described below.

Subjects (human users) will be granted access to objects (data/files) based upon the:

- Identity of the subject requesting access,
- Role (or roles) the subject is authorized to assume,
- Type of access requested,
- Content of the access request, and,
- Possession of a secret or private key, if required.

Subject identification includes:

- Individuals with different access authorizations

- Roles with different access authorizations
- Individuals assigned to one or more roles with different access authorizations

Access type, with explicit allow or deny:

- Read
- Write
- Execute

6.1.2 Security Audit

6.1.2.1 FAU_GEN.1 Audit data generation (iteration 2)

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 minimum level of audit; and

c) The events listed in Table 1 below.

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, the information specified in the Additional Details column in Table 1 below. Additionally, the audit shall not include plaintext private or secret keys or other critical security parameters.

Table 1, Auditable Events and Audit Data

The following part originates from [CERT-PP] in iteration 2			
Function	**Component**	**Event**	**Additional Details**
Security Audit	FAU_GEN.1 Audit data generation (iteration 2)	Any changes to the audit parameters, e.g., audit frequency, type of event audited Any attempt to delete the audit log	**Audit parameters cannot be modified by anyone, nor can the audit log be deleted.** **This means there is no such audit event.**
	FPT_CIMC_TSP.1 Audit log signing event	Audit log signing event	Digital signature, keyed hash, or authentication code shall be included in the audit log. **The Audit Log consists of signed records in the AuditLog Table of the CMDB. The CIS log file consists of**

			digitally signed, chained log records.
Local Data Entry		All security-relevant data that is entered in the system	**The Audit Log contains the date and time of events, user identity based on the Officer certificate, subject identity, event type, request id, and whether operation was allowed or disallowed.**
Remote Data Entry		All security-relevant messages that are received by the system	**The Audit Log contains the date and time of events, user identity based on the Officer certificate, subject identity, event type, request id, and whether operation was allowed or disallowed.**
Data Export and Output		All successful and unsuccessful requests for confidential and security- relevant information	**The Audit Log contains the date and time of events, user identity based on the Officer certificate, subject identity, event type, request id, and whether operation was allowed or disallowed.** **Success or failure of event is logged in the Audit Log table in the CMDB.**
Key Generation	FCS_CKM.1 Cryptographic Key Generation	Whenever the TSF requests generation of a cryptographic key. (Not mandatory for single session or one-time use symmetric keys.)	The public component of any asymmetric key pair generated
Private Key Load		The loading of Component private keys	
Private Key Storage		All access to certificate subject private keys	

		retained within the TOE for key recovery purposes	
Trusted Public Key Entry, Deletion and Storage		All changes to the trusted public keys, including additions and deletions	The public key and all information associated with the key
Secret Key Storage		The manual entry of secret keys used for authentication	
Private and Secret Key Export	FDP_ETC_CIMC.5 Extended user private and secret key export; FMT_MTD_CIMC.7 Extended TSF private and secret key export	The export of private and secret keys (keys used for a single session or message are excluded)	
Certificate Registration	FDP_CIMC_CER.1 Certificate Generation	All certificate requests	If accepted, a copy of the certificate. If rejected, the reason for rejection (e.g., invalid data, request rejected by ~~**Officer**~~ **Registration Officer**, etc.). **All certificate requests are stored as signed requests in the Audit Log table in the CMDB**.
Certificate Status Change Approval		All requests to change the status of a certificate	Whether the request was Accepted or rejected. **Requests to change the status of a certificate are stored as signed requests in the Audit Log table in the CMDB.**
CIMC Configuration		Any security-relevant changes to the configuration of the TSF.	**Changes to the CA policy are written as signed Audit Records to the 'AuditLog' table in the CMDB.**
Certificate Profile Management	FMT_MOF_CIMC.3 Extended certificate profile management	All changes to the certificate Profile	The changes made to the Profile
Revocation Profile Management		All changes to the revocation profile	The changes made to the Profile

Certificate Revocation List Profile Management	FMT_MOF_CIMC.5 Extended certificate revocation list profile management	All changes to the certificate revocation list profile	The changes made to the profile
Online Certificate Status Protocol (OCSP) Profile Management	FMT_MOF_CIMC.6 OCSP Profile Management	All changes to the OCSP profile	The changes made to the profile
The following part originates from [CERT-PP] in iteration 1			
Function	**Component**	**Event**	**Additional Details**
Security Audit	FAU_GEN.1 Audit data generation (iteration 1)	Any changes to the audit parameters, e.g., audit frequency, type of event audited	**Audit parameters cannot be configured.** **This means there is no such audit event.**
		Any attempt to delete the audit log	**The audit log cannot be deleted.** **This means there is no such audit event.**
Identification and Authentication	FIA_ATD.1 User attribute definition	Successful and unsuccessful attempts to assume a role	**Unsuccessful attempts to login with certificates that have no officer role, will be logged as failure in the AuditLog table in the CMDB.**
	FIA_AFL.1 Authentication failure handling	The value of maximum authentication attempts is changed	**It is not possible to change the behaviour of the authentication function, not even for Administration Officers. Note: Authentication is PKI based and not password based.** **This means there is no such audit event.**
	FIA_AFL.1 Authentication failure handling	*Maximum authentication attempts* unsuccessful authentication attempts occur during user login	**It is not possible to change the behaviour of the authentication function, not even for Administration Officers.** **This means there is no such audit event.**

	FIA_AFL.1 Authentication failure handling	An ~~**Administrator**~~ **Administration Officer** unlocks an account that has been locked as a result of unsuccessful authentication attempts	**It is not possible to change the behaviour of the authentication function, not even for Administration Officers.** **This means there is no such audit event.**
		An ~~**Administrator**~~ **Administration Officer** changes the type of authenticator, e.g., from password to biometrics	**It is not possible to change the behaviour of the authentication function, not even for Administration Officers.** **This means there is no such audit event.**
Roles		Roles and users are added or deleted	**Adding or deleting roles and users are written as signed audit records to the AuditLog table in the CMDB.**
		The access control privileges of a user account or a role are modified	**Modifications to roles and users are written as signed audit records to the AuditLog table in the CMDB.**

Application note: Several auditable events listed in the table above are not supported or applicable to the TOE (i.e. parameters for audit data generation cannot be configured). These events are therefore not audited, but accountability can still be maintained as needed by “O.Individual accountability and audit records” since the configuration is not possible.

6.1.2.2 FAU_GEN.2 User identity association (iteration 2)

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.

6.1.2.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide ~~**Auditors**~~ **Administration Officers with audit tasks** with the capability to read all information from the audit records.

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

Application note: This SFR was taken from the [CERT-PP] were the SFR was to be addressed by the TOE environment. In the ST, it is addressed by the TOE

instead. Therefore, the refinement made to the SFR in the [CERT-PP] has been removed so that it no longer refers to the IT environment, but rather to the TSF.

6.1.2.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply searches of audit data based on the type of event, the user responsible for causing the event, and as specified in Table 2 below.

Table 2 Audit Search Criteria

Function	Search Criteria
Certificate Request Remote and Local Data Entry	Identity of the subject of the certificate being requested
Certificate Revocation Request Remote and Local Data Entry	Identity of the subject of the certificate to be revoked

Application note: This SFR was taken from the [CERT-PP] were the SFR was to be addressed by the TOE environment. In the ST it is addressed by the TOE instead. Therefore, the refinement made to the SFR in the [CERT-PP] has been removed so that it no longer refers to the IT environment, but rather to the TSF.

6.1.2.5 FAU_SEL.1 Selective audit (iteration 2)

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) Object identity, user identity, subject identity, event type

b) Date, request id, failed only

Application note: This SFR is addressing both SFRs taken from the [CERT-PP], i.e. both FAU_SEL.1 (iteration 1) and FAU_SEL.1 (iteration 2). In the [CERT-PP] the iteration 1 was for the environment and iteration 2 for the TOE. But now, both of them are addressed by the TOE in iteration 2.

6.1.2.6 FAU_STG.1 Protected audit trail storage (iteration 2)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to detect unauthorized modifications to the stored audit records in the audit trail.

Application note: This SFR is addressing both SFRs taken from the [CERT-PP], i.e. both FAU_STG.1 (iteration 1) and FAU_STG.1 (iteration 2). In the [CERT-PP] the iteration 1 was for the environment and iteration 2 for the TOE. But now, both of them are addressed by the TOE in iteration 2.

6.1.2.7 FAU_STG.4 Prevention of audit data loss (iteration 2)

FAU_STG.4.1 The TSF shall prevent auditable events, except those taken by the ~~**Auditor**~~ **Administration Officer with audit tasks** if the audit trail is full.

Application note: This SFR is addressing both SFRs taken from the [CERT-PP], i.e. both FAU_STG.4 (iteration 1) and FAU_STG.4 (iteration 2). In the [CERT-PP] the iteration 1 was for the environment and iteration 2 for the TOE. But now both of them are addressed by the TOE in iteration 2.

6.1.2.8 FPT_STM.1 Reliable time stamps (iteration 2)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application note: This SFR is addressing both SFRs taken from the [CERT-PP], i.e. both FPT_STM.1 (iteration 1) and FPT_STM.1 (iteration 2). In the [CERT-PP] the iteration 1 was for the environment and iteration 2 for the TOE. But now both of them are addressed by the TOE in iteration 2.

6.1.2.9 FPT_CIMC_TSP.1 Audit log signing event

FPT_CIMC_TSP.1.1 The TSF shall periodically create an audit log signing event in which it computes a digital signature, keyed hash, or authentication code over the entries in the audit log.

FPT_CIMC_TSP.1.2 The digital signature, keyed hash, or authentication code shall be computed over, at least, every entry that has been added to the audit log since the previous audit log signing event and the digital signature, keyed hash, or authentication code from the previous audit log signed event.

FPT_CIMC_TSP.1.3 The specified frequency at which the audit log signing event occurs shall be configurable.

FPT_CIMC_TSP.1.4 The digital signature, keyed hash, or authentication code from the audit log signing event shall be included in the audit log.

Application Note: The Request Audit log and the CIS Audit log differs in the way that the CIS log uses chained signature scheme while the Request Audit log has a signature per log entry.

6.1.3 Roles

6.1.3.1 FMT_MOF.1 Management of security functions behavior (iteration 2)

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behavior of the functions listed in Table 3 to the authorized roles as specified in Table 3.

Table 3 Authorized Roles for Management of Security Functions Behavior

The following part originates from [CERT-PP] in iteration 2		
Function	**Component Function**	**Authorized Role**
Security Audit		~~**The capability to configure the audit parameters shall be restricted to Administrators.**~~ ~~**The capability to change the frequency of the audit log signing event shall be restricted to Administrators.**~~ **It is not possible to configure the audit parameters. Accordingly, events cannot be prevented from being audited by any role.**

Certificate Registration		The capability to approve fields or extensions to be included in a certificate shall be restricted to ~~Officers~~ **Registration Officers.** If an automated process is used to approve fields or extensions to be included in a certificate, the capability to configure that process shall be restricted to ~~Officers~~ **Registration Officers.**
Data Export and Output		~~The export of CIMC private keys shall require the authorization of at least two Administrators or one Administrator and one Officer, Auditor or Operator.~~ **Not applicable: the TOE does not allow exporting of CIMC private keys.**
Certificate Status Change Approval		~~Only Officers shall configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate.~~ **Revocation of certificate status requests can only made by Registration Officers, which are approved by the Access Manager based on the Officers Role and identity.** ~~Only Officers shall configure the automated process used to approve the placing of a certificate on hold or information about the on hold status of a certificate.~~ **The publishing of certificates can only be put on hold by Registration Officers.**
CIMC Configuration		The capability to configure any TSF functionality shall be restricted to ~~Administrators~~ **Administration Officers** in Certificate Manager and Administrators in OCSP Responder TOE environment. (This requirement applies to all configuration parameters unless the ability to configure that aspect of the TSF functionality has been assigned to a different role elsewhere in this document.)
Certificate Profile Management	FMT_MOF_CIMC.3 Extended certificate profile management	The capability to modify the certificate profile shall be restricted to ~~Administrators~~ **Administration Officers.**
Revocation Profile Management		The capability to modify the revocation profile shall be restricted to ~~Administrators~~ **Administration Officers.**

Certificate Revocation List Profile Management	FMT_MOF_CIMC.5 Extended certificate revocation list profile management	The capability to modify the certificate revocation list profile shall be restricted to ~~**Administrators**~~ **Administration Officers.**
Online Certificate Status Protocol (OCSP) Profile Management	FMT_MOF_CIMC.6 OCSP profile management	The capability to modify the OCSP profile shall be restricted to Administrators.

The following part originates from [CERT-PP] in iteration 1	
Function	**Function/Authorized Role**
Security Audit	~~**The capability to configure the audit parameters shall be restricted to Administrators.**~~ **This function is covered by iteration 2: It is not possible to configure the audit parameters. Accordingly, events cannot be prevented from being audited by any role.**
Backup and Recovery	~~**The capability to configure the backup parameters shall be restricted to [ST assignment: *authorized user*]1.**~~ **The capability to configure the backup parameters is not supported by the TOE, as it is a security function of the TOE environment.** ~~**The capability to initiate the backup or recovery function shall be restricted to [ST assignment: *authorized user*]2.**~~ **The capability to initiate the backup or recovery function is not supported by the TOE, as it is part of the TOE environment.** **Backup and Recovery functionality is part of the TOE environment, and is therefore covered in Section 6.2.4 FDP_CIMC_BKP.1 CIMC and FDP_CIMC_BKP.2 Extended CIMC**
Identification and Authentication	~~**The capability to specify or change *maximum authentication attempts* shall be restricted to Administrators.**~~ ~~**The capability to change authentication mechanisms shall be restricted to Administrators**~~ **It is not possible to change the behaviour of the authentication function, not even for Administration Officers. Note: Authentication is PKI based and not password based.**
Roles	The capability to create user accounts and roles shall be restricted to ~~**Administrators**~~ **Administration Officers**. The capability to assign privileges to those accounts and roles shall be restricted to ~~**Administrators**~~ **Administration Officers**.

Application note: This SFR addresses both FMT_MOF.1 (iteration 1) and

FMT_MOF.1 (iteration 2) as provided by the [CERT-PP], where iteration 1 is meant to be addressed by the TOE environment and iteration 2 by the TOE.

6.1.3.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 6.1.1 to restrict the ability to modify **none** of the security attributes to ~~**Administrators**~~ **Administration Officers.**

Application Note: Security attributes of the access control policy cannot be configured by any role.
In the [CERT-PP] this SFR was included as a requirement for the TOE environment. However, it has been included as an SFR for the TOE, since the TOE is meeting the requirement.

6.1.3.3 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for **certificate-based authentication and access control.**

Application Note: Access control is employed according to the role as assigned to the user's certificate. The role configuration is done in officer profiles, which are applied to the officer objects. A unique officer is created by associating a profile to a certificate issued by the TOE.
In the [CERT-PP] this SFR was included as a requirement for the TOE environment. However, it has been included as an SFR for the TOE, since the TOE is meeting the requirement.

6.1.3.4 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 6.1.1 to provide **permissive** default values for security attributes that are used to enforce the SFP.

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

Application Note: In the [CERT-PP] this SFR was included as a requirement for the TOE environment. However, it has been included as an SFR for the TOE, since the TOE is meeting the requirement.

6.1.3.5 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: **Administration Officer, Registration Officer, Authentication Officer** and **Administrator**.

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

6.1.3.6 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to view (read) ~~**or delete**~~ the audit logs to ~~**Auditors**~~ **Administration Officer with audit tasks**.

Application note: In the [CERT-PP] this SFR was for the TOE environment, but this has been turned into an SFR for the TOE since the TOE is meeting the requirement.

6.1.4 Access Control

6.1.4.1 FDP_ACC.1 Subset access control (iteration 2)

FDP_ACC.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 6.1.1 on **Officers, Policy Objects Requests**.

Application note: Policy Objects are a type of objects used by the Nexus Certificate Manager to hold the certificate policy (CP) and certification practice statement (CPS).

6.1.4.2 FDP_ACF.1 Security attribute based access control (iteration 2)

FDP_ACF.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 6.1.1 to objects based on the following: the identity of the subject and the set of roles that the subject is authorized to assume.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: specified in Table 4.

FDP_ACF.1.3 The TSF shall explicitly authorize 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**.

Table 4 Access Controls

Function	Event
Certificate Request Remote and Local Data Entry	The entry of certificate request data shall be restricted to Registration Officers and the subject of the requested certificate.
Certificate Revocation Request Remote and Local Data Entry	The entry of certificate revocation request data shall be restricted to Registration Officers and the subject of the certificate to be revoked.
Data Export and Output	The export or output of confidential and security-relevant data shall only be at the request of authorized users.
Key Generation	The capability to request the generation of Component keys (used to protect data in more than a single session or message) shall be restricted to Administrators
Private Key Load	The capability to request the loading of Component private keys into cryptographic modules shall be restricted to Administration Officers.
Private Key Storage	The capability to request the decryption of certificate subject private keys shall be restricted to Registration Officers. The TSF shall not provide a capability to decrypt certificate subject private keys that may be used to generate digital signatures. A Registration Officer with a Recover key role shall be required to request the decryption of a certificate subject private key.
Trusted Public Key Entry, Deletion, and Storage	The capability to change (add, revise, delete) the trusted public keys shall be restricted to Administration Officers.

Secret Key Storage	The capability to request the loading of CIMC secret keys into cryptographic modules shall be restricted to Administrators.
Private and Secret Key Destruction	The capability to zeroize CIMC plaintext private and secret keys shall be restricted to Administration Officers.
Private Key Export	The export of a certificate subject private key shall require the authorization of a Registration Officer with a Recover key role.
Certificate Status Change Approval	Only Registration Officers and the subject of the certificate shall be capable of requesting that a certificate be placed on hold. Only Registration Officers shall be capable of removing a certificate from on hold status. Only Registration Officers shall be capable of approving the placing of a certificate on hold. Only Registration Officers and the subject of the certificate shall be capable of requesting the revocation of a certificate. Only Registration Officers shall be capable of approving the revocation of a certificate and all information about the revocation of a certificate.

Application note: The table above is changed from the original SFR taken from the [CERT-PP] since the roles and privilege mechanism of the TOE is different to the one foreseen by the PP author. This also means that the private and secret key export is restricted to a Registration officer with a Recover key role only, and not limited to any two administrator roles.

6.1.5 Identification and authentication

6.1.5.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 If authentication is not performed in a cryptographic module that has been FIPS 140-2 validated to an overall Level of 2 or higher with Level 3 or higher for Roles and Services , the TSF shall detect when an Administrator configurable maximum limit for unsuccessful authentication attempts has occurred since the last successful authentication for the indicated user identity.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **do nothing since for the certificate-based authentication there is no such limit**.

Application note: Since the TOE only supports certificate-based authentication there is no need for authentication failure handling as described above. This SFR is only here only to identify that it is covered by a cryptographic module.
In the [CERT-PP], this SFR was for the TOE environment. However, it has been included as an SFR for the TOE, since the TOE is meeting the requirement.

6.1.5.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: the set of roles that the user is authorized to assume **and the digital certificate of that user**.

Application note: Attributes required by the TOE to enforce the CIMC TOE Access Control Policy (section 6.1.1), the generation of audit records, and proper identification and authentication of users are the following: the digital certificate and the user role bounded to the certificate, as well as verification of signature of the signed request. Every subject is associated with the user identity and user role.

6.1.5.3 FIA_SOS.1 Verification of secrets (iteration 2)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet:

1) For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods.) and
2) For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur

Application note: The TOE relies on certificate-based authentication, and therefore does not use passwords for authentication. The certificate-based authentication mechanism verifies validity of the Officer's authentication certificate based on authentication keys stored on cryptographic smart cards and through PKI based signed challenges and requests. Authentication data cannot be forged or reused as a new challenge is issued each time. Upon unsuccessful authentication, the smart card is blocked or a PIN code is required to invoke the key for authentication. The unlocking mechanism with the PIN code is part of the TOE environment / The security requirements for the PIN code ensure that the probability shall be less than one in 1,000,000 that a random attempt will succeed.

6.1.5.4 FIA_UAU.1 Timing of authentication (iteration 2)

FIA_UAU.1.1 The TSF shall allow **responding to OCSP requests** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF- mediated actions on behalf of that user.

6.1.5.5 FIA_UID.1 Timing of identification (iteration 2)

FIA_UID.1.1 The TSF shall allow **responding to OCSP requests** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF- mediated actions on behalf of that user.

Application note: It is configurable whether OCSP requests will be accepted or not without any authentication.

6.1.5.6 FIA_USB.1 User-subject binding (iteration 2)

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

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:

1. **The TSF determines the user identity and user role from the digital certificate presented by the user for authentication.**

2. **Every subject (user session) is associated with the user identity and user role of the user on whose behalf the subject will act.** SEP

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: **Changes to the user security attributes must be acknowledged by two Administration Officers.**

6.1.6 Remote Data Entry and Export

6.1.6.1 FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin

FCO_NRO_CIMC.3.1 The TSF shall enforce the generation of evidence of origin for certificate status information and all other security-relevant information at all times.

FCO_NRO_CIMC.3.2 The TSF shall be able to relate the identity, **role of the user and signature of each transaction** of the originator of the information, and the security-relevant portions of the information to which the evidence applies.

FCO_NRO_CIMC.3.3 The TSF shall verify the evidence of origin of information for all security-relevant information.

Application note: Any information obtained is provided using an HTTPS mutually authenticated connection. Each transaction arriving through such a connection is validated according to the criteria described above.

6.1.6.2 FDP_ITT.1 Basic internal transfer protection (iteration 3)

FDP_ITT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 6.1.1 to prevent the modification of security-relevant user data when it is transmitted between physically-separated parts of the TOE.

6.1.6.3 FDP_ITT.1 Basic internal transfer protection (iteration 4)

FDP_ITT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 6.1.1 to prevent the disclosure of confidential user data when it is transmitted between physically separated parts of the TOE.

6.1.6.4 FDP_UCT.1 Basic data exchange confidentiality (iteration 2)

FDP_UCT.1.1 The TSF shall enforce the CIMC TOE Access Control Policy specified in Section 6.1.1 to transmit confidential objects in a manner protected from unauthorized disclosure.

6.1.6.5 FPT_ITC.1 Inter-TSF confidentiality during transmission (iteration 2)

FPT_ITC.1.1 The TSF shall protect all confidential TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

6.1.6.6 FPT_ITT.1 Basic internal TSF data transfer protection (iteration 3)

FPT_ITT.1.1 The TSF shall protect all security-relevant TSF data from modification when it is transmitted between separate parts of the TOE.

6.1.6.7 FPT_ITT.1 Basic internal TSF data transfer protection (iteration 4)

FPT_ITT.1.1 The TSF shall protect all confidential TSF data from disclosure when it is transmitted between separate parts of the TOE.

6.1.6.8 FCO_NRO_CIMC.4 Advanced verification of origin

FCO_NRO_CIMC.4.1 The TSF shall, for initial certificate registration messages sent by the certificate subject, only accept messages protected using an authentication code, keyed hash, or digital signature algorithm.

FCO_NRO_CIMC.4.2 The TSF shall, for all other security-relevant information, only accept the information if it was signed using a digital signature algorithm.

6.1.6.9 FDP_CIMC_CSE.1 Certificate status export

FDP_CIMC_CSE.1.1 Certificate status information shall be exported from the TOE in messages whose format complies with **the X.509 standard for CRLs, and CIL, the Nexus defined format for listing of issued certificates**.

ST Application note: The CIL contains a list of certificate serial number of certificates issued by the CA. The format of the CIL is described in the TOE overview and in the product documentation provided to the customer.

6.1.7 Key Management

6.1.7.1 FDP_ACF_CIMC.2 User private key confidentiality protection

FDP_ACF_CIMC.2.1 CIMS personnel private keys shall be stored in a FIPS 140-2 validated cryptographic module or stored in encrypted form. If CIMS personnel private keys are stored in encrypted form, the encryption shall be performed by the FIPS 140-2 validated cryptographic module.

FDP_ACF_CIMC.2.2 If certificate subject private keys are stored in the TOE, they shall be encrypted using a Long Term Private Key Protection Key. The encryption shall be performed by the FIPS 140-2 validated cryptographic module.

6.1.7.2 FMT_MTD_CIMC.4 TSF private key confidentiality protection

FMT_MTD_CIMC.4.1 CIMC private keys shall be stored in a FIPS 140-2 validated cryptographic module or stored in encrypted form. If CIMC private keys are stored in encrypted form, the encryption shall be performed by the FIPS 140-2 validated cryptographic module.

6.1.7.3 FDP_SDI_CIMC.3 Stored public key integrity monitoring and action

FDP_SDI_CIMC.3.1 Public keys stored within the CIMC, but not within a FIPS 140-2 validated cryptographic module, shall be protected against undetected modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_SDI_CIMC.3.2 The digital signature, keyed hash, or authentication code used to protect a public key shall be verified upon each access to the key. If verification fails, the TSF shall **record audit events of failed verifications and prevent operations that involves use of the affected key**.

6.1.7.4 FDP_ACF_CIMC.3 User secret key confidentiality protection

FDP_ACF_CIMC.3.1 User secret keys stored within the CIMC, but not within a FIPS 140-2 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the FIPS 140-2 validated cryptographic module.

6.1.7.5 FMT_MTD_CIMC.5 TSF secret key confidentiality protection

FMT_MTD_CIMC.5.1 TSF secret keys stored within the TOE, but not within a FIPS 140-2 validated cryptographic module, shall be stored in encrypted form. The encryption shall be performed by the FIPS 140-2 validated cryptographic module.

6.1.7.6 FCS_CKM_CIMC.5 CIMC private and secret key zeroization

FCS_CKM_CIMC.5.1 The TSF shall provide the capability to zeroize plaintext secret and private keys within the FIPS 140-2 validated cryptographic module.

6.1.7.7 FDP_ETC_CIMC.5 Extended user private and secret key export

FDP_ETC_CIMC.5.1 Private and secret keys shall only be exported from the TOE in encrypted form or using split knowledge procedures. Electronically distributed secret and private keys shall only be exported from the TOE in encrypted form.

ST Application note: Both Smart card and PKCS#12 certificates are supported. The smart card is protected by a PIN and the PKCS#12 file is encrypted and password protected. There is no split knowledge mechanism for either of them.

6.1.7.8 FMT_MTD_CIMC.7 Extended TSF private and secret key export

FMT_MTD_CIMC.7.1 Private and secret keys shall only be exported from the TOE in encrypted form or using split knowledge procedures. Electronically distributed secret and private keys shall only be exported from the TOE in encrypted form.

6.1.8 Certificate Profile Management

6.1.8.1 FMT_MOF_CIMC.3 Extended certificate profile management

FMT_MOF_CIMC.3.1 The TSF shall implement a certificate profile and shall ensure that issued certificates are consistent with that profile.

FMT_MOF_CIMC.3.2 The TSF shall require the ~~**Administrator**~~ **Administration Officer** to specify the set of acceptable values for the following fields and extensions:

- the key owner's identifier;
- the algorithm identifier for the subject’s public/private key pair;
- the identifier of the certificate issuer;
- the length of time for which the certificate is valid;

FMT_MOF_CIMC.3.3 If the certificates generated are X.509 public key certificates, the TSF shall require the ~~**Administrator**~~ **Administration Officer** to specify the set of acceptable values for the following fields and extensions:

- keyUsage;

- basicConstraints;
- certificatePolicies

FMT_MOF_CIMC.3.4 The ~~**Administrator**~~ **Administration Officer** shall specify the acceptable set of certificate extensions.

6.1.9 Certificate Revocation List Profile Management

6.1.9.1 FMT_MOF_CIMC.5 Extended certificate revocation list profile management

FMT_MOF_CIMC.5.1 If the TSF issues CRLs, the TSF must implement a certificate revocation list profile and ensure that issued CRLs are consistent with the certificate revocation list profile.

FMT_MOF_CIMC.5.2 If the TSF issues CRLs, the TSF shall require the ~~**Administrator**~~ **Administration Officer** to specify the set of acceptable values for the following fields and extensions:

- Issuer;
- issuerAltName (NOTE: If a CIMC does not issue CRLs with this extension, then it is not required within the certificate revocation list profile.)
- nextUpdate (i.e., a promise of next CRL in specified time).

FMT_MOF_CIMC.5.3 If the TSF issues CRLs, the ~~**Administrator**~~ **Administration Officer** shall specify the acceptable set of CRL and CRL entry extensions.

6.1.10 Online Certificate Status Protocol (OCSP) Profile Management

An online certificate status protocol profile is used to define the set of acceptable values for the fields in an OCSP response. The OCSP profile may specify the type(s) of responses that the CIMC may generate (i.e., acceptable values for responseType) as well as the set of acceptable values for the fields within the acceptable response types. An example of a value that may be covered by an OCSP profile for the basic response type is ResponderID, the identifier of the OCSP responder.

6.1.10.1 FMT_MOF_CIMC.6 OCSP profile management

FMT_MOF_CIMC.6.1 If the TSF issues OCSP responses, the TSF shall implement an OCSP profile and ensure that issued OCSP responses are consistent with the OCSP profile.

FMT_MOF_CIMC.6.2 If the TSF issues OCSP responses, the TSF shall require the Administrator to specify the set of acceptable values for the responseType field (unless the CIMC can only issue responses of the basic response type).

FMT_MOF_CIMC.6.3 If the TSF is configured to allow OCSP responses of the basic response type, the TSF shall require the Administrator to specify the set of acceptable values for the ResponderID field within the basic response type.

6.1.11 Certificate Registration

6.1.11.1 FDP_CIMC_CER.1 Certificate Generation

FDP_CIMC_CER.1.1 The TSF shall only generate certificates whose format complies with:

- **X.509 standard for public key certificates [RFC5280],**
- **X.509/RFC 5755 attribute certificates,**
- **Card Verifiable Certificates (CVC) according to Gematik specification Electronic Health Card,**
- **Card Verifiable Certificates (CVC) according to BSI Technical Guideline TR-03110,**
- **IEEE 1609.2 certificates,**
- **ISO 9796-2 Tachograph Certificates,**
- **RFC 6962 Certificate Transparency Precertificates,**
- **PGP certificates [RFC4880].**

FDP_CIMC_CER.1.2 The TSF shall only generate certificates that are consistent with the currently defined certificate profile.

FDP_CIMC_CER.1.3 The TSF shall verify that the prospective certificate subject possesses the private key that corresponds to the public key in the certificate request before issuing a certificate, unless the public/private key pair was generated by the TSF, whenever the private key may be used to generate digital signatures.

FDP_CIMC_CER.1.4 If the TSF generates X.509 public key certificates, it shall only generate certificates that comply with requirements for certificates as specified in ITU-T Recommendation X.509. At a minimum, the TSF shall ensure that:

a) The version field shall contain the integer 0, 1, or 2.
b) If the certificate contains an issuerUniqueID or subjectUniqueID then the version field shall contain the integer 1 or 2.
c) If the certificate contains extensions then the version field shall contain the integer 2.
d) The serialNumber shall be unique with respect to the issuing Certification Authority.
e) The validity field shall specify a notBefore value that does not precede the current time and a notAfter value that does not precede the value specified in notBefore.
f) If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical issuerAltName extension.
g) If the subject field contains a null Name (e.g., a sequence of zero relative distinguished names), then the certificate shall contain a critical subjectAltName extension.
h) The signature field and the algorithm in the subjectPublicKeyInfo field shall contain the OID for a FIPS- approved or recommended algorithm.

6.1.12 Certificate Revocation

The functions in this section address the validation and approval of certificate revocation information.

6.1.12.1 FDP_CIMC_CRL.1 Certificate revocation list validation

FDP_CIMC_CRL.1.1 A TSF that issues CRLs shall verify that all mandatory fields in any CRL issued contain values in accordance with ITU-T Recommendation X.509. At a minimum, the following items shall be validated:

1. If the version field is present, then it shall contain a 1.
2. If the CRL contains any critical extensions, then the version field shall be present and contain the integer 1.
3. If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the CRL shall contain a critical issuerAltName extension.
4. The signature and signatureAlgorithm fields shall contain the OID for a FIPS-approved digital signature algorithm.
5. The thisUpdate field shall indicate the issue date of the CRL.
6. The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.

6.1.12.2 FDP_CIMC_OCSP.1 OCSP basic response validation

FDP_CIMC_OCSP.1.1 If a TSF is configured to allow OCSP responses of the basic response type, the TSF shall verify that all mandatory fields in the OCSP basic response contain values in accordance with **RFC 6960** ~~**IETF RFC 2560**~~**.** At a minimum, the following items shall be validated:

1. The version field shall contain a 0.
2. If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the response shall contain a critical issuerAltName extension.
3. The signatureAlgorithm field shall contain the OID for a FIPS-approved digital signature algorithm.
4. The thisUpdate field shall indicate the time at which the status being indicated is known to be correct.
5. The producedAt field shall indicate the time at which the OCSP responder signed the response.
6. The time specified in the nextUpdate field (if populated) shall not precede the time specified in the thisUpdate field.

Application note: The RFC 6960 obsoletes RFCs 2560 and 6277.

6.1.13 Strength of Function Requirements

6.1.13.1 FCS_SOF_CIMC.1 CIMC Strength of Functions

FCS_SOF_CIMC.1.1 The TSF shall provide cryptographic mechanisms that fulfill the specific Strength of Function requirements of Section 6.1.13.2.

6.1.13.2 Cryptographic Modules

FIPS 140-2 validated validated cryptographic modules must perform all cryptographic functions performed by CIMCs. FIPS 140-2 validated cryptographic modules, are also required to generate cryptographic keys and to store plaintext private and secret keys.

6.1.13.2.1 Encryption Algorithms

The encryption specified for:

- FAU_STG.1 Protected audit trail storage
- FCO_NRO_CIMC.4 Advanced verification of origin
- FDP_ACF_CIMC.2 User private key confidentiality protection
- FDP_ACF_CIMC.3 User secret key confidentiality protection
- FDP_ETC_CIMC.5 Extended user private and secret key export
- FDP_SDI_CIMC.3 Stored public key integrity monitoring and action
- FMT_MTD_CIMC.4 TSF private key confidentiality protection
- FMT_MTD_CIMC.5 TSF secret key confidentiality protection
- FMT_MTD_CIMC.7 Extended TSF private and secret key export
- FPT_CIMC_TSP.1 Audit log signing event

shall be performed using a FIPS-approved recommended algorithm.

The SFRs listed above are using the following cryptographic functions provided by the TOE environment, which is the HSM, standard Java library or Bouncy Castle.

SFR	Supported by the following SFR and algorithm
FAU_STG.1 Protected audit trail storage	FCS_COP.1(3) Cryptographic operation (digital signature) signed using the HSM. Algorithm: RSA-PSS and SHA2, or RSA and SHA2
FCO_NRO_CIMC.4 Advanced verification of origin	FCS_COP.1(5) Cryptographic operation (digital signature) verified using standard Java or Bouncy Castle signature providers. The TOE verifies the origin only, since signatures are produced outside of the TOE. Algorithms: RSA-PSS and SHA2, or RSA and SHA2
FDP_ACF_CIMC.2 User private key confidentiality protection	FCS_COP.1(1) Cryptographic operation (symmetric) Algorithm: AES128CBC, AES192CBC, or AES256CBC.
FDP_ACF_CIMC.3 User secret key confidentiality protection	FCS_COP.1(1) Cryptographic operation (asymmetric) Algorithm: RSA-OAEP
FDP_ETC_CIMC.5 Extended user private and secret key export	FCS_COP.1(1) Cryptographic operation (symmetric) using the HSM. Algorithms used: AES or 3DES 3DES only if AES is not supported by the end user.
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	FCS_COP.1(3) Cryptographic operation (digital signature) signed using the HSM and verified using the standard Java or Bouncy Castle signature providers in FCS_COP.1(5).

	Algorithm: RSA-PSS and SHA-2, RSA-PSS and SHA-3, RSA and SHA-2, DSA and SHA-2, ECDSA and SHA-2
FMT_MTD_CIMC.4 TSF private key confidentiality protection	There are private keys that are stored in the FIPS 140-2 HSM. The private keys that are exported or stored outside of the HMS the FCS_COP.1(1) Cryptographic operation (symmetric) is used, using the HSM. Algorithm: AES128CBC, AES192CBC, or AES256CBC.
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	FCS_COP.1(2) Cryptographic operation (asymmetric) using the HSM Algorithm used: RSA-OAEP or RSA
FMT_MTD_CIMC.7 Extended TSF private and secret key export	FCS_COP.1(1) Cryptographic operation (symmetric) using the HSM Algorithms used: AES or 3DES 3DES only if AES is not supported by the end user.
FPT_CIMC_TSP.1 Audit log signing event	FCS_COP.1(3) Cryptographic operation (digital signature) using the HSM

6.1.13.2.3 FIPS 140-2 Validated Cryptographic Modules

Cryptographic modules specified for:

- FDP_ACF_CIMC.2 User private key confidentiality protection
- FDP_ACF_CIMC.3 User secret key confidentiality protection
- FDP_ETC_CIMC.5 Extended user private and secret key export
- FDP_SDI_CIMC.3 Stored public key integrity monitoring and action
- FMT_MTD_CIMC.4 TSF private key confidentiality protection
- FMT_MTD_CIMC.5 TSF secret key confidentiality protection
- FMT_MTD_CIMC.7 Extended TSF private and secret key export
- FPT_CIMC_TSP.1 Audit log signing event

shall be validated against FIPS 140-2.

The SFRs and algorithms provided by the FIPS 140-2 approved HSM are listed in Section 6.1.13.2.1.

6.1.13.2.4 Split Knowledge Procedures

Split-knowledge procedures specified in:

- FDP_ETC_CIMC.5 Extended user private and secret key export
- FMT_MTD_CIMC.7 Extended TSF private and secret key export

shall be implemented and validated as specified in FIPS 140-2.

The SFRs and algorithms provided by the FIPS 140-2 approved HSM are listed in Section 6.1.13.2.1.

6.1.13.2.5 Authentication Codes

The authentication code specified in:

- FAU_STG.1 Protected audit trail storage
- FCO_NRO_CIMC.4 Advanced verification of origin
- FPT_CIMC_TSP.1 Audit log signing event
- FDP_SDI_CIMC.3 Stored public key integrity monitoring and action

shall be a FIPS-approved or recommended authentication code.

The SFRs listed above are using the cryptographic algorithms listed in the table in Section 6.1.13.2.1.

6.2 Security Functional Requirements for the TOE Environment

Some of the SFRs into the [CERT-PP] for the TOE environment are addressed by the TOE and not by the TOE environment. These SFRs they are still listed here with a headline, but clearly marked with an application note as being addressed by a corresponding SFR for the TOE.

6.2.1 CIMC IT Environment Access Control Policy

The IT environment shall support the administration and enforcement of a CIMC IT Environment access control policy that provides the capabilities described below.

Subjects (human users) will be granted access to objects (data/files) based upon the:

- Identity of the subject requesting access,
- Role (or roles) the subject is authorized to assume,
- Type of access requested,
- Content of the access request, and,
- Possession of a secret or private key, if required.

Subject identification includes:

- Individuals with different access authorizations
- Roles with different access authorizations
- Individuals assigned to one or more roles with different access authorizations

Access type, with explicit allow or deny:

- Read
- Write
- Execute

6.2.2 Security Audit

6.2.2.1 FAU_GEN.1 Audit data generation (iteration 1)

Application note: FAU_GEN.1 (iteration 1) is fully addressed by the TOE as described in Section 6.1.2.1 FAU_GEN.1 (iteration 2).

6.2.2.2 FAU_GEN.2 User identity association (iteration 1)

Application note: FAU_GEN.2 (iteration 1) is fully addressed by the TOE as described Section 6.1.2.2 in FAU_GEN.2 (iteration 2).

6.2.2.3 FAU_SAR.1 Audit review

Application note: FAU_SAR.1 is fully addressed by the TOE as described in Section 6.1.2.3 FAU_SAR.1.

6.2.2.4 FAU_SAR.3 Selectable audit review

Application note: FAU_SAR.3 is fully addressed by the TOE as described in Section 6.1.2.4 FAU_SAR.3.

6.2.2.5 FAU_SEL.1 Selective audit (iteration 1)

Application note: FAU_SEL.1 (iteration 1) is fully addressed by the TOE as described in Section 6.1.2.5 FAU_SEL.1 (iteration 2).

6.2.2.6 FAU_STG.1 Protected audit trail storage (iteration 1)

Application note: FAU_STG.1 (iteration 1) is fully addressed by the TOE as described in Section 6.1.2.6 FAU_STG.1 (iteration 2).

6.2.2.7 FAU_STG.4 Prevention of audit data loss (iteration 1)

Application note: FAU_STG.4 (iteration 1) is fully addressed by the TOE as described in Section 6.1.2.7 FAU_STG.4 (iteration 2).

6.2.2.8 FPT_STM.1 Reliable time stamps (iteration 1)

Application note: FPT_STM.1 (iteration 1) is fully addressed by the TOE as described in Section 6.1.2.8 FPT_STM.1 (iteration 2).

6.2.3 Roles

6.2.3.1 FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The IT environment shall maintain the roles: **Administrator, ~~Auditor, and Officer~~. Administration Officer, Registration Officer and Authentication Officer**

FMT_SMR.2.2 The IT environment shall be able to associate users with roles.

FMT_SMR.2.3 The IT environment shall ensure that the conditions **no identity should be assigned more than one role**.

~~(a) no identity is authorized to assume both an Administrator and an Officer role;~~

~~(b) no identity is authorized to assume both an Auditor and an Officer role; and~~

(c) ~~no identity is authorized to assume both an Administrator and an Auditor role are satisfied.~~

Application Note: Although the TOE maintains the roles and thereby addresses FMT_SMR.1, the IT environment also has to be aware of these roles. This SFR can be enforced by the TOE environment, either by technical or administrative means into the operational environment of the TOE.

6.2.3.2 FMT_MOF.1 Management of security functions behavior (iteration 1)

Application Note: FMT_MOF.1 (iteration 1) is fully addressed by the TOE as described in Section 6.1.3.1 FMT_MOF.1 (iteration 2).

6.2.3.3 FMT_MSA.1 Management of security attributes

Application note: FMT_MSA.1 is fully addressed by the TOE as described in Section 6.1.3.2 FMT_MSA.1. This section is only here as a reference for the reader and for consistency with the [CERT-PP].

6.2.3.4 FMT_MSA.2 Secure security attributes

Application note: FMT_MSA.2 is fully addressed by the TOE as described in Section 6.1.3.3 FMT_MSA.2. This section is only here as a reference for the reader and for consistency with the [CERT-PP]**.**

6.2.3.5 FMT_MSA.3 Static attribute initialization

Application note: FMT_MSA.3 is fully addressed by the TOE as described in Section 6.1.3.4 FMT_MSA.3. This section is only here as a reference for the reader and for consistency with the [CERT-PP]**.**

6.2.3.6 FMT_MTD.1 Management of TSF data

Application note: FMT_MTD.1 is fully addressed by the TOE as described in Section 6.1.3.6 FMT_MTD.1. This section is only here as a reference for the reader and for consistency with the [CERT-PP].

6.2.4 Backup and Recovery

6.2.4.1 FDP_CIMC_BKP.1 CIMC backup and recovery

FDP_CIMC_BKP.1.1 The IT environment shall include a backup function.

FDP_CIMC_BKP.1.2 The IT environment shall provide the capability to invoke the backup function on demand.

FDP_CIMC_BKP.1.3 The data stored in the system backup shall be sufficient to recreate the state of the system at the time the backup was created using only:

a) copy of the same version of the CIMC as was used to create the backup data;

b) a stored copy of the backup data;

c) the cryptographic key(s), if any, needed to verify the digital signature, keyed hash, or authentication code protecting the backup; and

d) the cryptographic key(s), if any, needed to decrypt any encrypted critical security parameters.

FDP_CIMC_BKP.1.4 The IT environment shall include a recovery function that is able to restore the state of the system from a backup. In restoring the state of the system, the recovery function is only required to create an “equivalent” system state in which information about all relevant CIMC transactions has been maintained.

6.2.4.2 FDP_CIMC_BKP.2 Extended CIMC backup and recovery

FDP_CIMC_BKP.2.1 The backup data shall be protected against modification through the use of digital signatures, keyed hashes, or authentication codes.

FDP_CIMC_BKP.2.2 Critical security parameters and other confidential information shall be stored in encrypted form only.

6.2.5 Access Control

6.2.5.1 FDP_ACC.1 Subset access control (iteration 1)

FDP_ACC.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in Section 6.2.1 on

- **Subjects: Processes with user ID and group**
- **Objects: Files and directories with access rights**
- **Operations: Read, write and execute**

Application note: The access control mechanism is the one for the file system of the underlying operating systems, which in the case of the TOE is either Windows or Linux.

6.2.5.2 FDP_ACF.1 Security attribute based access control (iteration 1)

FDP_ACF.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in Section 6.2.1 to objects based on the following: the identity of the subject and the set of roles that the subject is authorized to assume.

FDP_ACF.1.2 The IT environment shall enforce the following rule to determine if an operation among controlled subjects and controlled objects is allowed: the capability to zeroize plaintext private and secret keys shall be restricted to **~~Auditors, Officers, and Operators~~. IT-Administrators of the IT environment~~,~~**

FDP_ACF.1.3 The IT environment shall explicitly authorize access of subjects to objects based on the following additional rules: **no additional rules**.

FDP_ACF.1.4 The IT environment shall explicitly deny access of subjects to objects based on the following additional rules: **no additional rules**.

Application Note: The access control mechanism is the one for the file system of the underlying operating systems, which in the case of the TOE is either Windows or Linux.

6.2.6 Identification and Authentication

6.2.6.1 FIA_AFL.1 Authentication failure handling

Application note: All identification and authentication of users with user roles into the TOE are identified and authenticated by the TOE, which is described in Section 6.1.5.1 FIA_AFL.1. This section is only here as a reference for the reader and for consistency with the [CERT-PP].

6.2.6.2 FIA_ATD.1 User attribute definition

Application note: This SFR is fully addressed by the TOE, described in Section 6.1.5.2 FIA_ATD.1. This section is only here as a reference for the reader and for consistency with the [CERT-PP]. The reason is that no users with user roles in the

TOE are identified and authenticated and therefore have no user attributes maintained by the TOE environment.

6.2.6.3 FIA_SOS.1 Verification of secrets (iteration 1)

Application note: This SFR is fully addressed by the TOE, described in Section 6.1.5.3 FIA_SOS.1 Verification of secrets (iteration 2). This section is only here as a reference for the reader and for consistency with the [CERT-PP].

6.2.6.4 FIA_UAU.1 Timing of authentication (iteration 1)

Application note: This SFR is fully addressed by the TOE, described in Section 6.1.5.4 FIA_UAU.1 Timing of authentication (iteration 2). This section is only here as a reference for the reader and for consistency with the [CERT-PP].

6.2.6.5 FIA_UID.1 Timing of identification (iteration 1)

Application note: This SFR is fully addressed by the TOE, described in Section 6.1.5.5 FIA_UID.1 Timing of identification (iteration 2). This section is only here as a reference for the reader and for consistency with the [CERT-PP].

6.2.6.6 FIA_USB.1 User-subject binding (iteration 1)

Application note: This SFR is fully addressed by the TOE, described in Section 6.1.5.6 FIA_USB.1 User-subject binding (iteration 2). This section is only here as a reference for the reader and for consistency with the [CERT-PP].

6.2.6.7 FTP_TRP.1 – Trusted path

FTP_TRP.1.1 The IT environment shall provide a communication path between itself and **remote or local** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The IT environment shall permit **local users or remote users** to initiate communication via the trusted path.

FTP_TRP.1.3 The IT environment shall require the use of the trusted path for **initial user authentication as well as all other communication with the TOE**.

Application note: The remote or local user is using the client that is connecting to the server component of Nexus Certificate Manager and connections between server components of Nexus Certificate Manager. Note that the TLS library used by the TOE is part of the TOE environment.

6.2.7 Remote Data Entry and Export

6.2.7.1 FDP_ITT.1 Basic internal transfer protection (iteration 1)

FDP_ITT.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in Section 6.2.1 to prevent the modification of security-relevant user data when it is transmitted between physically-separated parts of the IT environment.

6.2.7.2 FDP_ITT.1 Basic internal transfer protection (iteration 2)

FDP_ITT.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in Section 6.2.1 to prevent the disclosure of

confidential user data when it is transmitted between physically-separated parts of the IT environment.

6.2.7.3 FDP_UCT.1 Basic data exchange confidentiality (iteration 1)

FDP_UCT.1.1 The IT environment shall enforce the CIMC IT Environment Access Control Policy specified in Section 6.2.1 to transmit confidential user data in a manner protected from unauthorized disclosure.

6.2.7.4 FPT_ITC.1 Inter-TSF confidentiality during transmission (iteration 1)

FPT_ITC.1.1 The IT environment shall protect confidential IT environment data transmitted from the IT environment to a remote trusted IT product from unauthorized disclosure during transmission.

6.2.7.5 FPT_ITT.1 Basic internal TSF data transfer protection (iteration 1)

FPT_ITT.1.1 The IT environment shall protect security-relevant IT environment data from modification when it is transmitted between separate parts of the IT environment.

6.2.7.6 FPT_ITT.1 Basic internal TSF data transfer protection (iteration 2)

FPT_ITT.1.1 The IT environment shall protect confidential IT environment data from disclosure when it is transmitted between separate parts of the IT environment.

6.2.8 Key Management

6.2.8.1 FCS_CKM.1 Cryptographic key generation (iteration 1)

FCS_CKM.1.1 The **cryptographic module in the operational environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **RSA** and specified cryptographic key sizes **2048, 3072, 4096, 8192, 16384 bit** that meet the following: **[PKCS1]**.

Application note: The FIPS 140-2 validated cryptographic module generates RSA keys used as CA-keys, CIS log signing keys, PIN decryption keys, TLS server keys, OCSP Responder keys, TLS client keys and user keys when created with function KAR generate.

6.2.8.2 FCS_CKM.1 Cryptographic key generation (iteration 2)

FCS_CKM.1.1 The **cryptographic module in the operational environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **Elliptic Curve Digital Signature Algorithm** and cryptographic key sizes **[256 bits or greater]** that meet the following: **[FIPS186, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" P-256, P-384, P-521; RFC5639, "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation" brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1.**

Application note: The FIPS 140-2 validated cryptographic module generates EC keys used for CA-keys, TLS server keys, OCSP Responder keys, TLS client keys and user keys when created with function KAR generate.

6.2.8.3 FCS_CKM.1 Cryptographic key generation (iteration 3)

FCS_CKM.1.1 The **cryptographic module in the operational environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **AES, 3DES** and specified cryptographic key sizes **128, 192, 256 (AES) and 168 (3DES)** that meet the following: [**FIPS197] for AES and [ISO 18033-3] for 3DES.**

Application note: The FIPS 140-2 validated cryptographic module generates AES, 3DES keys for use as KEK (Key Encryption Key).

6.2.8.4 FCS_CKM.1 Cryptographic key generation (iteration 4)

FCS_CKM.1.1 The **cryptographic module in the operational environment** shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **DSA** and specified cryptographic key sizes **L=1024, N=160; L=2048, N=224; L=2048, N=256; L=3072, N=256** that meet the following: **[FIPS186].**

Application note: The FIPS 140-2 validated cryptographic module generates DSA keys used as CA-keys.

6.2.8.5 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The **cryptographic module in the operational environment** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **implemented in the FIPS validated module** that meets the following: **FIPS 140-2**.

6.2.9 Self-tests

6.2.9.1 FPT_TST_CIMC.1 Abstract Machine Testing

FPT_TST_CIMC.1.1 The IT environment shall run a suite of tests **during initial start-up** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the IT environment.

FPT_TST_CIMC.1.2 The IT environment shall provide authorized users with the capability to verify the integrity of the security assumptions provided by the abstract machine that underlies the IT environment.

FPT_TST_CIMC.1.2 The IT environment shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

Application note: The operating system performs a self-test as part of the startup process. Moreover, the FIPS module does a self-test as required by FIPS 140-2.

6.2.9.2 FPT_TST_CIMC.2 Software/firmware integrity test

FPT_TST_CIMC.2.1 An error detection code (EDC) or FIPS-approved or recommended authentication technique (e.g., the computation and verification of an authentication code, keyed hash, or digital signature algorithm) shall be applied to all security-relevant software and firmware residing within the CIMC (e.g., within EEPROM and RAM). The EDC shall be at least 16 bits in length.

FPT_TST_CIMC.2.2 The error detection code, authentication code, keyed hash, or digital signature shall be verified at power-up and on-demand. If verification fails, the IT environment shall **enter an error state and not start operation**.

6.2.9.3 FPT_TST_CIMC.3 Software/firmware load test

FPT_TST_CIMC.3.1 A cryptographic mechanism using a FIPS-approved or recommended authentication technique (e.g., an authentication code, keyed hash, or digital signature algorithm) shall be applied to all security relevant software and firmware that can be externally loaded into the CIMC.

FPT_TST_CIMC.3.2 The IT environment shall verify the authentication code, keyed hash, or digital signature whenever the software or firmware is externally loaded into the CIMC. If verification fails, the IT environment shall **enter an error state and not start operation**.

6.2.10 Cryptographic Modules

FCS_COP.1(1) Cryptographic operation (symmetric)

FCS_COP.1.1 The **cryptographic module in the operational environment** shall perform **symmetric encryption and decryption** in accordance with a specified cryptographic algorithm

a) AES in CBC mode

b) 3DES in CBC mode

and cryptographic key sizes

a) 128, 192, 256 (AES)

b) 168 (3DES)

that meet the following:

a) [FIPS197] for AES

b) [ISO 18033-3] for 3DES

c) [SP 800-38A] for CBC

Application note: The FIPS 140-2 validated cryptographic module performs symmetric encryption and decryption of archived asymmetric keys.

FCS_COP.1(2) Cryptographic operation (asymmetric)

FCS_COP.1.1 The **cryptographic module in the operational environment** shall perform **asymmetric encryption and decryption** in accordance with a specified cryptographic algorithm

a) RSA-OAEP

b) RSA

and cryptographic key sizes

a) 3072, 4096, 8192, 16384 (RSA-OAEP)

b) 2048, 3072, 4096, 8192, 16384 (RSA)

that meet the following:

a) [PKCS1] for RSA-OAEP

b) [PKCS1] for RSA

Application note: The FIPS 140-2 validated cryptographic module performs asymmetric encryption and decryption of archived symmetric keys and of archived PIN codes.

FCS_COP.1(3) Cryptographic operation (digital signature)

FCS_COP.1.1 The **cryptographic module in the operational environment** shall perform **digital signature creation** in accordance with a specified cryptographic algorithm

a) **RSA-PSS and SHA-2**
b) **RSA-PSS and SHA-3**
c) **RSA and SHA-2**
d) **DSA and SHA-2**
e) **ECDSA and SHA-2**

and cryptographic key sizes

a) **RSA-PSS using 3072, 4096, 8192, 16384 bit; SHA2 using 256, 384, 512 bit, SHA3 using 256, 384 bit**
b) **RSA using 2048, 3072, 4096, 8192, 16384 bit; SHA2 using 256, 384, 512 bit**
c) **DSA using L=1024, N=160; L=2048, N=224; L=2048, N=256; L=3072, N=256; SHA2 using 256, 384, 512 bit**
d) **ECDSA using curves P-256, P-384, P-521, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1; SHA2 using 256, 384, 512 bit**

that meet the following:

a) **[PKCS1] for RSA-PSS**
b) **[PKCS1] for RSA**
c) **[FIPS186] for DSA**
d) **[FIPS186] for ECDSA "NIST" curves; [RFC5639] for ECDSA Brainpool curves**

Application note: The FIPS 140-2 validated cryptographic module performs digital signature creation for certificates, CRL's, CIL's, OCSP responses, and CIS log.

FCS_COP.1(4) Cryptographic operation (hash)

FCS_COP.1.1 The **cryptographic module in the operational environment** shall perform **secure hash** in accordance with a specified cryptographic algorithm

a) **SHA-2**
b) **SHA-3**

and cryptographic key sizes

a) **SHA-2 using 256, 384, 512 bit**
b) **SHA-3 using 256, 384 bit**

that meet the following:

a) **[FIPS180] for SHA-2**
b) **[FIPS202] for SHA-3**

Application note: The FIPS 140-2 validated cryptographic module performs secure hash operations in creation of certificates, CRL's and CIL's.

FCS_COP.1(5) Cryptographic operation (digital signature verification)

FCS_COP.1.1 The **cryptographic modules in the operational environment** shall perform **message authentication** in accordance with a specified cryptographic algorithm

a) **RSA-PSS and SHA-2**
b) **RSA-PSS and SHA-3**
c) **RSA and SHA-2**
d) **DSA and SHA-2**
e) **ECDSA and SHA-2**

and cryptographic key sizes

a) **RSA-PSS using 3072, 4096, 8192, 16384 bit; SHA2 using 256, 384, 512 bit, SHA3 using 256, 384 bit**
b) **RSA using 2048, 3072, 4096, 8192, 16384 bit; SHA2 using 256, 384, 512 bit**
c) **DSA using L=1024, N=160; L=2048, N=224; L=2048, N=256; L=3072, N=256; SHA2 using 256, 384, 512 bit**
d) **ECDSA using curves P-256, P-384, P-521, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1; SHA2 using 256, 384, 512 bit**

that meet the following:

a) **[PKCS1] for RSA-PSS**
b) **[PKCS1] for RSA**
c) **[FIPS186] for DSA**
d) **[FIPS186] for ECDSA "NIST" curves; [RFC5639] for ECDSA Brainpool curves**

Application note: The cryptographic modules used for digital signature verification in the operational environment comprises the Java standard library and Bouncy Castle. Digital signatures created by TOE connected HSM's are verified by the TOE using either the standard Java or Bouncy Castle crypto library depending on the algorithm used.

6.3 Security Functional Requirements Rationale

6.3.1 Coverage of the SFRs

With the exception of additional SFR FMT_SMR.1, all SFRs have been directly taken from the [CERT-PP]. FMT_SMR.1 is hierarchical to FMT_SMR.2, which was included for the TOE environment, and they both meet the security objective O.Security roles.

On the SFRs taken from the [CERT-PP], no operations have been made in a way that has changed the meaning of the SFRs, so the rationale remain unchanged. This means that the coverage rationale for the SFRs taken from the [CERT-PP] remains valid, however it is replicated here for convenience.

SFR	Objective
FAU_GEN.1 Audit data generation (iterations 1 and 2)	O.Individual accountability and audit records

FAU_GEN.2 User identity association (iterations 1 and 2)	O.Individual accountability and audit records
FAU_SAR.1 Audit review	O.Individual accountability and audit records
FAU_SAR.3 Selectable audit review	O.Individual accountability and audit records
FAU_SEL.1 Selective audit (iterations 1 and 2)	O.Individual accountability and audit records
FAU_STG.1 Protected audit trail storage (iterations 1 and 2)	O.Protect stored audit records
FAU_STG.4 Prevention of audit data loss (iterations 1 and 2)	O.Respond to possible loss of stored audit records
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	O.Non-repudiation, O.Control unknown source communication traffic
FCO_NRO_CIMC.4 Advanced verification of origin	O.Non-repudiation
FCS_CKM.1 Cryptographic key generation (iterations 1, 2, 3 and 4)	OE.Cryptographic functions
FCS_CKM.4 Cryptographic key destruction	OE.Procedures for preventing malicious code, OE.React to detected attacks
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	O.Procedures for preventing malicious code, O.React to detected attacks
FCS_COP.1 Cryptographic operation (symmetric)	OE.Cryptographic functions
FCS_COP.1 Cryptographic operation (asymmetric)	OE.Cryptographic functions
FCS_COP.1 Cryptographic operation (digital signature)	OE.Cryptographic functions
FCS_COP.1 Cryptographic operation (hash)	OE.Cryptographic functions
FCS_COP.1 Cryptographic operation (signature verification)	OE.Cryptographic functions
FCS_SOF_CIMC.1 CIMC Strength of Functions	OE.Cryptographic functions
FDP_ACC.1 Subset access control (iterations 2)	O.Limitation of administrative access
FDP_ACF.1 Security attribute based access control (iterations 2)	O.Limitation of administrative access
FDP_ACF_CIMC.2 User private key confidentiality protection	O.Certificates, O.Procedures for preventing malicious code
FDP_ACF_CIMC.3 User secret key confidentiality protection	O.Certificates, O.Procedures for preventing malicious code
FDP_CIMC_CER.1 Certificate Generation	O.Certificates
FDP_CIMC_CRL.1 Certificate revocation list validation	O.Certificates

FDP_CIMC_CSE.1 Certificate status export	O.Certificates
FDP_CIMC_OCSP.1 OCSP basic response validation	O.Certificates
FDP_ETC_CIMC.5 Extended user private and secret key export	O.Data import/export
FDP_ITT.1 Basic internal transfer protection (iterations 1 and 3)	O.Integrity protection of user data and software, O.Protect user and TSF data during internal transfer
FDP_ITT.1 Basic internal transfer protection (iterations 2 and 4)	O.Protect user and TSF data during internal transfer
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	O.Integrity protection of user data and software
FDP_UCT.1 Basic data exchange confidentiality (iterations 2)	O.Data import/export
FIA_AFL.1 Authentication failure handling	O.React to detected attacks
FIA_ATD.1 User attribute definition	O.Maintain user attributes
FIA_SOS.1 Verification of secrets (iterations 1 and 2)	O.Limitation of administrative access
FIA_UAU.1 Timing of authentication (iterations 2)	O.Limitation of administrative access, O.Restrict actions before authentication
FIA_UID.1 Timing of identification (iterations 2)	O.Individual accountability and audit records, O.Limitation of administrative access
FIA_USB.1 User-subject binding (iterations 1 and 2)	O.Maintain user attributes
FMT_MOF.1 Management of security functions behavior (iterations 1 and 2)	O.Configuration management, O.Manage behavior of security functions, O.Security-relevant configuration management
FMT_MOF_CIMC.3 Extended certificate profile management	O.Configuration management
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	O.Configuration management
FMT_MOF_CIMC.6 OCSP Profile Management	O.Configuration management
FMT_MSA.1 Management of security attributes	O.Maintain user attributes, O.User authorization management
FMT_MSA.2 Secure security attributes	O.Security-relevant configuration management
FMT_MSA.3 Static attribute initialization	O.Security-relevant configuration management
FMT_MTD.1 Management of TSF data	O.Individual accountability and audit records, O.Protect stored audit records
FMT_MTD_CIMC.4 TSF private key confidentiality protection	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software

FMT_MTD_CIMC.5 TSF secret key confidentiality protection	O.Detect modifications of firmware, software, and backup data, O.Integrity protection of user data and software
FMT_MTD_CIMC.7 Extended TSF private and secret key export	O.Data import/export
FMT_SMR.1 Security Roles	O.Security roles
FPT_CIMC_TSP.1 Audit log signing event	O.Protect stored audit records
FPT_ITC.1 Inter-TSF confidentiality during transmission (iterations 2)	O.Data import/export
FPT_ITT.1 Basic internal TSF data transfer protection (iterations 3-4)	O.Protect user and TSF data during internal transfer
FPT_STM.1 Reliable time stamps (iterations 1 and 2)	O.Individual accountability and audit records, O.Time stamps

6.3.2 Sufficiency of the SFRs

All security objectives and SFRs defined by [CERT-PP] have been included in this ST, and all operations performed to the SFRs have been made in a way that the meaning of the SFRs remain unchanged. This means that the sufficiency rationale of the [CERT-PP] remains valid.

6.3.2.1 Security Objectives for the TOE

Authorized Users

O.Certificates is provided by FDP_CIMC_CER.1 (Certificate Generation), which ensures that certificates are valid, and FDP_CIMC_CRL.1 (Certificate revocation list validation), FDP_CIMC_CSE.1 (Certificate status export), and FDP_CIMC_OCSP.1 (OCSP basic response validation), which ensure that certificate revocation lists and certificate status information are valid. In the case that the TOE maintains a copy of the certificate subject's private key, FDP_ACF_CIMC.2 (User private key confidentiality protection) ensures that the certificate is not invalidated by the disclosure of the private key by the TOE. In the case that a secret key is used by the certificate subject as an authenticator in requesting a certificate, FDP_ACF_CIMC.3 (User secret key confidentiality protection) ensures that an attacker cannot obtain a bad certificate by obtaining a user's authenticator from the TOE and then using that authenticator to obtain a bad certificate.

System

O.Preservation/trusted recovery of secure state is provided by FDP_CIMC_BKP.1 (CIMC backup and recovery), which covers the requirement that the state of the system be preserved so that it can be recovered in the event of a secure component failure.

O.Sufficient backup storage and effective restoration is provided by FDP_CIMC_BKP.1 (CIMC backup and recovery) which covers the requirement that sufficient backup data is created and stored and that an effective restoration procedure is provided.

External Attacks

O.Control unknown source communication traffic is provided by FCO_NRO_CIMC.3 (Enforced proof of origin and verification of origin), which covers the requirement that the TOE discard messages from an unknown source that contain security-relevant information.

Cryptography

O.Non-repudiation is provided by FCO_NRO_CIMC.3 (Enforced proof of origin and verification of origin) which covers the requirement that messages containing security-relevant data are not accepted by the TOE unless they contain evidence of origin and FCO_NRO_CIMC.4 (Advanced verification of origin) which covers the requirement that digital signatures be used so that the evidence of origin for a message may be verified by a third-party.

O.Security roles is provided by FMT_SMR.1 (Security Roles) and and FMT_SMR.2 (Restrictions on security roles) which covers the requirement that a set of security roles be maintained and that users be associated with those roles.
Note: the roles of the TOE are maintained by the TOE itself and not by the TOE environment, but the restrictions on the roles are maintained by the environment.

O.Data import/export is provided by FDP_UCT.1 (Basic data exchange confidentiality) (iterations 1 and 2) and FPT_ITC.1 (Inter-TSF confidentiality during transmission) (iterations 1 and 2), which cover the requirement that data other than private and secret keys be protected when they are transmitted and from the CIMC. FDP_ETC_CIMC.5 (Extended user private and secret key export) and FMT_MTD_CIMC.7 (Extended TSF private and secret key export) cover the requirement that private and secret keys be protected when they are transmitted to and from the TOE.

O.Detect modifications of firmware, software, and backup data is provided by FPT_TST_CIMC.2 (Software/firmware integrity test) which covers the requirement that modifications to software or firmware be detected and FDP_CIMC_BKP.2 (Extended CIMC backup and recovery) which covers the requirement that modifications to backup data be detected. Since FPT_TST_CIMC.2 and FDP_CIMC_BKP.2 make use of digital signatures, keyed hashes, or authentication codes to detect modifications, FMT_MTD_CIMC.4 (TSF private key confidentiality protection) and FMT_MTD_CIMC.5 (TSF secret key confidentiality protection) are necessary to ensure that an attacker who has modified firmware, software, or backup data cannot prevent detection of the modification by computing a new digital signature, keyed hash, or authentication code.

O.Individual accountability and audit records is provided by a combination of requirements. FIA_UID.1 (Timing of identification) (iterations 1 and 2) covers the requirement that users be identified before performing any security-relevant operations. FAU_GEN.1 (Audit data generation) (iterations 1 and 2) and FAU_SEL.1 (Selective audit) (iterations 1 and 2) cover the requirement that security-relevant events be audited while FAU_GEN.2 (User identity association) (iterations 1 and 2) and FPT_STM.1 (Reliable time stamps) (iterations 1 and 2) cover the requirement that the date and time of audited events are recorded in the audit records along with the identities of the entities responsible for the actions. FMT_MTD.1 (Management of TSF data) covers the requirement that audit data be available for review by ensuring that users, other than Auditors, cannot delete audit

logs. Finally, FAU_SAR.1 (Audit review) and FAU_SAR.3 (Selectable audit review) cover the requirement that the audit records are made available for review so that individuals can be held accountable for their actions.

O.Integrity protection of user data and software is provided by FDP_ITT.1 (Basic internal transfer protection) (iterations 1 and 3) and FDP_SDI_CIMC.3 (Stored public key integrity monitoring and action) which cover the requirement that user data be protected and FPT_TST_CIMC.2 (Software/firmware integrity test) and FPT_TST_CIMC.3 (Software/firmware load test) which cover the requirement that software and firmware be protected. Since data and software are protected using cryptography, FMT_MTD_CIMC.4 (TSF private key confidentiality protection) and FMT_MTD_CIMC.5 (TSF secret key confidentiality protection) are required to protect the confidentiality of the private and secret keys used to protect the data and software.

O.Limitation of administrative access is provided by FDP_ACC.1 (Subset access control) (iterations 1 and 2), FDP_ACF.1 (Security attribute based access control) (iterations 1 and 2), FIA_SOS.1 (Verification of secrets) (iterations 1 and 2), FIA_UAU.1 (Timing of authentication) (iterations 1 and 2), and FIA_UID.1 (Timing of identification) (iterations 1 and 2). FIA_UAU.1 (Timing of authentication) (iterations 1 and 2), FIA_SOS.1 (Verification of secrets) (iterations 1 and 2), and FIA_UID.1 (Timing of identification) (iterations 1 and 2) ensure that Administrators, Operators, Officers, and Auditors cannot perform any security-relevant operations until they have been identified and authenticated and FDP_ACC.1 (Subset access control) (iterations 1 and 2) and FDP_ACF.1 (Security attribute based access control) (iterations 1 and 2) ensure that Administrators, Operators, Officers, and Auditors can only perform those operations necessary to perform their jobs.

O.Maintain user attributes is provided by FIA_ATD.1 (User attribute definition) and FIA_USB.1 (User- subject binding) (iterations 1 and 2) which cover the requirement to maintain a set of security attributes associated with individual users and/or subjects acting on users' behalves. FMT_MSA.1 (Management of security attributes) ensures that only authorized users can modify security attributes.

O.Manage behavior of security functions is provided by FMT_MOF.1 (Management of security functions behavior) (iterations 1 and 2) which covers the requirement that authorized users be able to configure, operate, and maintain the security mechanisms.

O.Procedures for preventing malicious code is provided by FPT_TST_CIMC.2 (Software/firmware integrity test) which ensures that only signed code can be executed and AGD_OPE.1 (Operational user guidance) and A.Malicious Code Not Signed which ensure that those who are capable of signing code do not to sign malicious code. It is also supported by FDP_ACF_CIMC.2 (User private key confidentiality protection), FDP_ACF_CIMC.3 (User secret key confidentiality protection), FCS_CKM.4 (Cryptographic key destruction) and FCS_CKM_CIMC.5 (CIMC private and secret key zeroization), which ensure that an untrusted entity cannot use a trusted entity's key to sign malicious code.

O.Protect stored audit records is provided by FAU_STG.1 (Protected audit trail storage) (iterations 1 and 2) which covers the requirement that audit records be protected against modification or unauthorized deletion and FMT_MTD.1 (Management of TSF data) which covers the requirement that audit records be protected from unauthorized access. Where the threat of malicious activity is

greater, FPT_CIMC_TSP.1 (Audit log signing event) is required so that modifications to the audit logs can be detected.

O.Protect user and TSF data during internal transfer is provided by FDP_ITT.1 (Basic internal transfer protection) (iterations 1-4) which covers the requirement that user data be protected during internal transfer and FPT_ITT.1 (Basic internal TSF data transfer protection) (iterations 1-4) which covers the requirement that TSF data be protected during internal transfer.

O.Respond to possible loss of stored audit records is provided by FAU_STG.4 (Prevention of audit data loss) (iterations 1 and 2), which covers the requirement that no auditable events, except those taken by the Auditor, can be performed when audit trail storage is full.

O.Restrict actions before authentication is provided by FIA_UAU.1 (Timing of authentication) (iterations 1 and 2) which covers the requirement that no security-relevant actions are performed on behalf of a user until that user has been authenticated.

O.Security-relevant configuration management is provided by FMT_MSA.3 (Static attribute initialization) and FMT_MSA.2 (Secure security attributes), which cover the requirement that security attributes have secure values. FMT_MOF.1 (Management of security functions behavior) (iterations 1 and 2) ensures that security-relevant configuration data can only be modified by those who are authorized to do so. O.Security-relevant configuration management is also supported by AGD_OPE.1 (Operational user guidance) which covers the requirement that Administrators be provided with documentation describing the configuration management features of the TOE and by A.Competent Administrators, Operators, Officers and Auditors and A.CPS which ensure that Administrators are competent and are familiar with the CPS under which the TOE is to be operated.

O.Time stamps is provided by FPT_STM.1 (Reliable time stamps) (iterations 1 and 2) which covers the requirement that the time stamps be reliable.

O.User authorization management is provided by FMT_MSA.1 (Management of security attributes), which covers the requirement that Administrators manage and update user’s security attributes. O.User authorization management is also supported by AGD_OPE.1 (Operational user guidance) which covers the requirement that Administrators be provided with documentation describing the user authorization management features of the TOE and by A.Competent Administrators, Operators, Officers and Auditors and A.CPS which ensure that Administrators are competent and are familiar with the CPS under which the TOE is to be operated.

O.React to detected attacks is provided by FCS_CKM.4 (Cryptographic key destruction) and FCS_CKM_CIMC.5 (CIMC private and secret key zeroization) which cover the requirement that the user who detected the attack be able to destroy any plaintext keys within the TOE in order to prevent the attacker from obtaining copies of these keys. FIA_AFL.1 (Authentication failure handling) covers the requirement that the TSF respond to detected attacks (in the form of repeated authentication attempts) by taking actions to prevent the attacker from successfully authenticating him/herself. In the case that an attack is detected by an Administrator, Auditor, Officer, or Operator.

6.3.3 Dependency Analysis Between SFRs

The stated security requirements together must form a mutually supportive and internally consistent whole. Internal consistency is demonstrated in an analysis of dependencies. Mutual support is shown through consideration of the interactions between and among the SFRs.

All the SFRs in Chapter 6 have been taken from the [CERT-PP], with the exception of FMT_SMR.1. FMT_SMR.1 is hierarchical to FMT_SMR.2, which was included for the TOE environment, and they both meet the security objective O.Security roles. Moreover, all operations have been performed to the SFRs in such a way that the meaning of the dependencies between the SFRs remain unchanged. This means that the dependency analysis done in the [CERT-PP] is valid.

Table 5 Dependency Analysis for the SFRs

SFR	Dependencies	Resolution
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation	Included
	FIA_UID.1 Timing of identification	Included
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	Included
FAU_SAR.3 Selectable audit review	FAU_SAR.1 Audit review	Included
FAU_SEL.1 Selective audit	FAU_GEN.1 Audit data generation	Included
	FMT_MTD.1 Management of TSF data	Included
FAU_STG.1 Protected audit trail storage	FAU_GEN.1 Audit data generation	Included
FAU_STG.4 Prevention of audit data loss	FAU_STG.1 Protected audit trail storage	Included
FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin	FIA_UID.1 Timing of identification	Included
FCO_NRO_CIMC.4 Advanced verification of origin	FCO_NRO_CIMC.3	Included
FCS_CKM.1 Cryptographic key generation	FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation	FCS_COP.1 Included

	FCS_CKM.4 Cryptographic key destruction	Included
FCS_CKM.4 Cryptographic key destruction	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.1 Included
FCS_CKM_CIMC.5 CIMC private and secret key zeroization	FCS_CKM.4 Cryptographic key destruction	Included
	FDP_ACF.1 Security attribute based access control	Included
FCS_COP.1 Cryptographic operation	FCS_CKM.4 Cryptographic key destruction	Included
	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.1 Included
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control	Included
	FMT_MSA.3 Static attribute initialization	Included
FDP_ACF_CIMC.2 User private key confidentiality protection	None	
FDP_ACF_CIMC.3 User secret key confidentiality protection	None	
FDP_CIMC_BKP.1 CIMC backup and recovery	FMT_MOF.1 Management of security functions behavior	Included
FDP_CIMC_BKP.2 Extended CIMC backup and recovery	FDP_CIMC_BKP.1 CIMC backup and recovery	Included
FDP_CIMC_CER.1 Certificate Generation	None	
FDP_CIMC_CRL.1 Certificate revocation list validation	None	
FDP_CIMC_CSE.1 Certificate status export	None	

FDP_CIMC_OCSP.1 OCSP basic response validation	None	
FDP_ETC_CIMC.5 Extended user private and secret key export	None	
FDP_ITT.1 Basic internal transfer protection	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	None	
FDP_UCT.1 Basic data exchange confidentiality	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
	FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path	FTP_TRP.1 Provided by the TOE environment.
FIA_AFL.1 Authentication failure handling	FIA_UAU.1 Timing of authentication	Included
FIA_ATD.1 User attribute definition	None	
FIA_SOS.1 Verification of secrets	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FIA_USB.1 User-subject binding	FIA_ATD.1 User attribute definition	Included
FMT_MOF.1 Management of security functions behavior	FMT_SMR.1 Security roles	Included
	FMT_SMF.1 Specification of Management Functions	Not Included
FMT_MOF_CIMC.3 Extended certificate profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Included
FMT_MOF_CIMC.5 Extended certificate revocation list profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Included
FMT_MOF_CIMC.6 OCSP profile management	FMT_MOF.1 Management of security functions behavior	Included
	FMT_SMR.1 Security roles	Included

FMT_MSA.1 Management of security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	Included
	FMT_SMR.1 Security roles	Included
	FMT_SMF.1 Specification of Management Functions	Not Included
FMT_MSA.2 Secure security attributes	FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control	FDP_ACC.1 Included
	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security Roles	Included
FMT_MSA.3 Static attribute initialization	FMT_MSA.1 Management of security attributes	Included
	FMT_SMR.1 Security roles	Included
FMT_MTD.1 Management of TSF data	FMT_SMR.1 Security roles	Included
	FMT_SMF.1 Specification of Management Functions	Not Included
FMT_MTD_CIMC.4 TSF private key confidentiality protection	None	
FMT_MTD_CIMC.5 TSF secret key confidentiality protection	None	
FMT_MTD_CIMC.6 TSF private and secret key export	None	
FMT_MTD_CIMC.7 Extended TSF private and secret key export	FMT_MTD_CIMC.6	Included
FMT_SMR.1 Security roles	FIA_UID.1 Timing of identification	Included
FMT_SMR.2 Restrictions on security roles	FIA_UID.1 Timing of identification	Included
FPT_TST_CIMC.1 Abstract Machine testing	None	
FPT_CIMC_TSP.1 Audit log signing event	FAU_GEN.1 Audit data generation	Included
	FMT_MOF.1 Management of security functions behavior	Included
FPT_ITC.1 Inter-TSF confidentiality during transmission	None	

FPT_ITT.1 Basic internal TSF data transfer protection	None	
FPT_STM.1 Reliable time stamps	None	
FPT_TST_CIMC.2 Software/firmware integrity test	FPT_TST_CIMC.1 Abstract Machine testing	Included
FPT_TST_CIMC.3 Software/firmware load test	FPT_TST_CIMC.1 Abstract Machine Testing	Included

6.3.3.2 Justification of Unsupported Dependencies FMT_SMF.1

The following components depend on FMT_SMF.1 Specification of Management Functions:

- FMT_MOF.1 Management of security functions behavior
- FMT_MSA.1 Management of security attributes
- FMT_MTD.1 Management of TSF data

This requirement need not be explicitly covered by the product since requirements in Table 3 meet or exceed the requirement for FMT_SMF.1 Specification of Management Functions.

6.4 Security Assurance Requirements

The security assurance requirements of this Security Target are those defined for the assurance level EAL4 augmented with ALC_FLR.2

Table 6: Summary of Security Assurance Requirements

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_FLR.2 Flaw reporting procedures (augmentation)

	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 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

6.5 Security Assurance Requirements Rationale

Dependencies within the EAL package selected (EAL4) for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again. The augmentation by flaw remediation, ALC_FLR.2, has no dependencies on other requirements. The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Security Target introduce dependencies on any security functional requirement.

The assurance level EAL4 augmented with ALC_FLR.2 has been chosen since this is the one specified by the [CERT-PP], with which compliance is claimed.

7 TOE Summary Specification

This TOE Summary Specification describes how the TOE Security Functions (TSFs) are mapped onto the components of the TOE and how these components together satisfy the Security Functional Requirements (SFRs) presented in section 6.1.

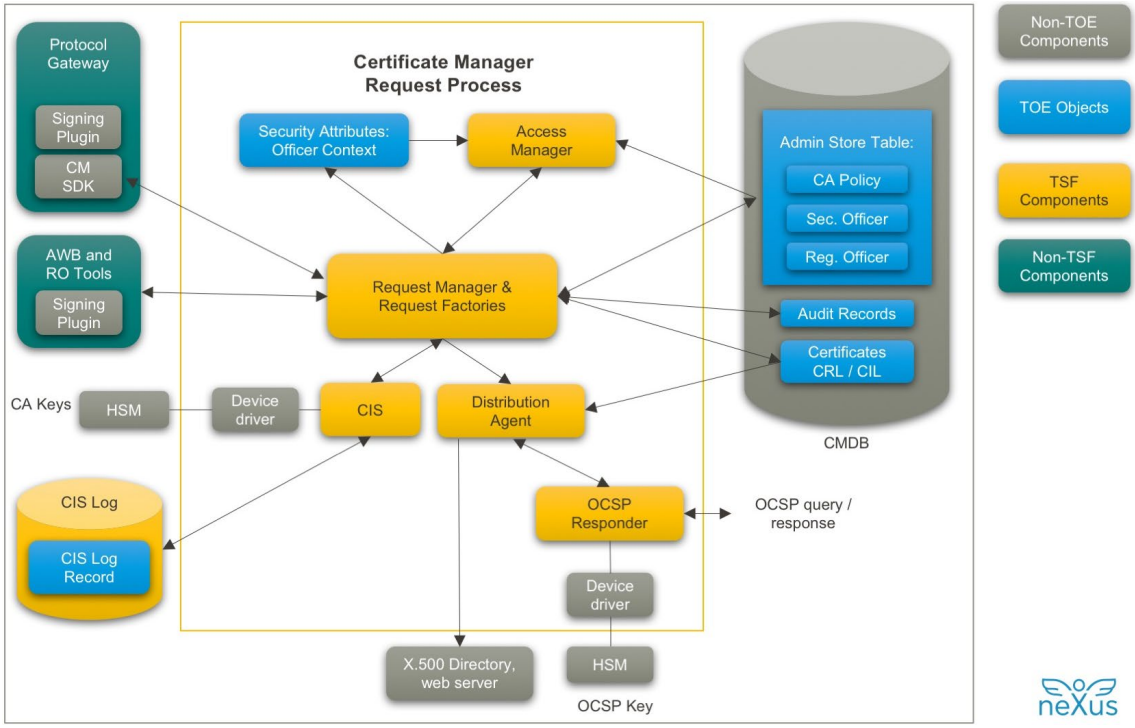

Figure 5, TSF, non-TSF and non-TOE components

7.1 TOE Security Functions

7.1.1 Security Audit

Audit Log
The Certificate Manager will record the start of the audit function in the Audit Log.

As the Request Manager receives and responds to requests from TOE users, the requests are also recorded in the Audit Log. The Audit Log consists of signed records in the AuditLog Table of the CMDB.

The request Audit Log in the database contains signed requests from the TOE users that can change the configuration or state of any policy object or certificate. TOE server generated events logged in the Audit Log originates from named processes. Auditable events include requests for the generation, loading and export of private keys. In addition, requests to change the status of a certificate, modifications made to Certificate Profiles, Revocation Profiles, Certificate Revocation List Profiles and OCSP Profiles, as well as security-relevant changes to the configuration of the TSF/CIMC configuration. A complete list of auditable events can be regarded in Table 1 in Section 6.1.2.1.

The Audit Log records startup time of log, the date and time of events, user identity based on the Officer certificate, subject identity, event type, request id. The log event status show if the action was allowed or disallowed. Success or failure of event is logged.

Audit log events generated by TOE server processes, e.g. generation of a CRL, are identified by the name of process that generated the event.

If the storage space for the Audit Log or the CIS Log would be exhausted the auditing will stop and no further certificate management request will be accepted until the storage space has been cleaned up or extended.

CIS Log
As certificates, CILs and CRLs are signed by the CIS component, log records are written to the CIS Log. Entries are signed by a system key and chained to the previous record. The chained signature of the CIS Log enables detection of a modification of the CIS Log and by that alerting Officers operating the Administrator Workbench. It is recommended that an external write once read only disk system (WORM drive) be used for this logging. This protects against the CIS log file from being replaced by an earlier version.

The CIS Log records startup and stop of the log, the data to be signed by a CA key, the date and time of the event, success or failure message. The CIS is responsible for signing the CIS Log entries.

Both the Audit Log and CIS Log components will generate audit records with a granularity of one second.

The Operational logs of TOE components are not signed since the logging purpose is to assist TOE operators with the daily maintenance, trouble-shooting, performance measurement, etc. The amount of logging details and choice of log type is configurable. The log types are text file based logs, Syslog, and SNMP.

Table 7, Security Audit Rationale

Security Functional Component	Rationale
FAU_GEN.1 (iteration 2)	Secure audit events are logged without delay in the database and cannot be disabled by configuration. TOE user requests are signed with Officer certificate. Log

	information details is not configurable. CIS Log events are stored and signed immediately by the CIS.
FAU_GEN.2 (iteration 2)	Audit events originating from TOE users are identifiable by the associated Officer certificate.
FAU_SAR.1	Audit records are made available for review so that individuals can be held accountable for their actions.
FAU_SAR.3	Audit records are made available for selectable audit review, by applying searches of audit data so that individuals can be held accountable for their actions.
FAU_SEL.1 (iteration 2)	Selective audit is possible by selection of attributes: object identity, user identity, subject identity, event type, date, request id, failed only.
FAU_STG.1 (iteration 2)	The TOE provides no function for removal of Log events. Manipulation of request in the Audit log cause the signature to become corrupt. CIS Logs manipulation is detected at read or write operations at which point the chained signature is verified.
FAU_STG.4 (iteration 2)	The TOE does not permit auditable events, except those taken by the Administration Officer with audit tasks if the AuditLog is full.
FPT_CIMC_TSP.1	Each request in the Audit Log has a signature, every new CIS log event is signed immediately.
FPT_STM.1 (iteration 2)	The TOE environment must use a trusted time source that the TOE can rely on for providing time stamps.

7.1.2 Roles

The TOE users are known collectively as Officers. The TOE enables configuration of officer roles on a fine-grained level for restricting officers to perform specific tasks only, e.g. as prescribed by the CA operational policies. The role configuration is done in officer profiles which are applied to the officer objects. A unique officer is created by associating a profile to a certificate issued by the TOE.

Three general Officer types; Administration Officer, Authentication Officer, and Registration Officer, are used to separate administrative from operational duties. Fine grained role definitions are constructed from a selection of the roles below together with additional name constraints, domain belonging, and filters:

Administration Officer roles

- Use AWB
- Audit tasks
- Domain tasks
- CA and Key tasks
- Policy tasks
- Officer tasks
- Profile tasks
- Configuration tasks

Authentication Officer role

- Use Clients

Registration Officer roles

- Use Clients
- Issue certificate
- Issue attribute certificate
- Recover key
- Manage OCSP Activation
- Manage user data retention
- Manage Revocation password
- Publish certificate
- Republish failed distribution
- Revoke certificate
- Revoke certificate with password
- Revoke attribute certificate
- Revoke attribute certificate with password
- Export search results
- Create batch
- Claim batch
- Manage PIN letters

Officers are created and managed by the Administrator's Workbench (AWB). In the AWB an Administration Officer retrieves the user information from the CMDB, updates the new Officer with its new role and signs the request together with a second Administration Officer. The Officer account data is stored in the Admin Store.

To create or modify the CA policy, administration Officers use the AWB to connect to the Central Certificate Manager (CCM) via the Request Manager and Access Manager components. Two administration officers sign CA policy changes and all changes are written via the Admin Store component to the 'AdminStore' table in the CMDB. They are also written as signed Audit Records to the 'AuditLog' table in the same database.

The Authentication Officer role is restricted to establishing secure connections between client and server components:

- Establish the TLS connection between the client and the core server
- List certificates
- Forward certification requests signed by a Registraion Officer
- Used with intermediate servers or applications

The private key of the Authentication Officer is protected in HSM or in PKCS#12 file.

Table 8, Roles Rationale

Security Functional Component	Rationale
FMT_MOF.1 (iteration 2)	The TOE access control enforces policies, based on the Officer role of the TOE user, for management of security functions behavior.
FMT_SMR.1	The TOE associates users with the role of either Administration Officer, Registration Officer, Authentication Officers or Administrator.
FMT_MSA.1	The TOE enforces the CIMC TOE Access Control Policy specified in Section 6.1.1 to restrict the ability to modify none of the security attributes to Administration officers, since security attributes of the access control policy cannot be configured by any role.
FMT_MSA.2	The TOE ensures that only secure values are accepted for certificate-based authentication and access control. Access control is employed according to the role as assigned to the user's certificate. The role configuration is done in officer profiles, which are applied to the officer objects. A unique officer is created by associating a profile to a certificate issued by the TOE.
FMT_MSA.3	The TOE enforces the CIMC TOE Access Control Policy specified in Section 6.1.1 to provide permissive default values for security attributes. The TOE does not allow any roles to specify alternative initial values to override the default values when an object or information is created.
FMT_MTD.1	The TOE allows Administration Officers with audit tasks to read the audit logs.

Table 9, Rationale - Authorized Roles for Management of Security Functions Behavior

Function	Authorized Role	TOE Officer Role
Security Audit	The capability to configure the audit parameters shall be restricted to Administration Officers. The capability to change the frequency of the audit log signing event shall be restricted to Administration Officers.	Not applicable: the TOE does not provide configuration of audit parameters. Not applicable: the TOE does not provide capability to change frequency of audit log signing.
Certificate Registration	The capability to approve fields or extensions to be included in a certificate shall be restricted to Registration Officers. If an automated process is used to approve fields or extensions to be included in a certificate, the capability to configure that process shall be restricted to Registration Officers.	Administration Officer: Policy Tasks.
Data Export and Output	The export of CIMC private keys shall require the authorization of at least two Administration Officers.	Not applicable: the TOE does not allow exporting of CIMC private keys.
Certificate Status Change Approval	Only Registration Officers shall configure the automated process used to approve the revocation of a certificate or information about the revocation of a certificate. Only Registration Officers shall configure the automated process used to approve the placing of a certificate on hold or information about the on hold status of a certificate.	Registration Officer: Revoke certificate or Revoke certificate with password
CIMC Configuration	The capability to configure any TSF functionality shall be restricted to Administration Officers. (This requirement applies to all configuration parameters unless the ability to configure that aspect of the TSF functionality has been assigned to a different role elsewhere in this document.)	Administration Officer: CA and key tasks, Policy tasks, Officer tasks, Profile tasks.

Certificate Profile Management / FMT_MOF_CIMC.3 Extended certificate profile management	The capability to modify the certificate profile shall be restricted to Administration Officers.	Administration Officer: Policy tasks.
Revocation Profile Management	The capability to modify the revocation profile shall be restricted to Administration Officers.	Administration Officer: Policy tasks.
Certificate Revocation List Profile Management / FMT_MOF_CIMC.5 Extended certificate revocation list profile management	The capability to modify the certificate revocation list profile shall be restricted to Administration Officers.	Administration Officer: Policy tasks.
Online Certificate Status Protocol (OCSP) Profile Management / FMT_MOF_CIMC.6 OCSP profile management	The capability to modify the OCSP profile shall be restricted to Administrators.	Administrator.

CA Policy Administration
In order to fulfil its primary intended function (i.e. to issue and manage CA certificates and end user PKI certificates), the TOE operates in accordance with a CA Policy. This policy is established by the action of Administration Officers in accordance with various guidance documents. CA Policy means the creation of Officers with appropriate authorization levels and the creation of CA keys, CA certificates, various Certificate Procedures (e.g. defining the content and format of end-user certificates), CRL and CIL Procedures, Distribution Rules, Publication Procedures, and Key Procedures.

To create or change a CA Policy, Administration Officers make use of AWB. Two Administration Officers sign CA Policy changes and all changes are written via the Admin Store component to the ’AdminStore’ table in the Certificate Manager Database (CMDB). They are also written as signed Audit Records to the ’AuditLog’ table in the same database.

Initiation Boot Process
As described previously, the CA Policy is established and maintained by the action of Administration Officers. When the system is first installed however, no true Administration Officers are known to the system. Instead the initial installed system is pre-configured to run with two default Officers known as the Boot Officers. These Officers are responsible for creating the first true users of the system, two real Administration Officers. These Administration Officers then become responsible for creating further Officers and setting up the CA Policies.

The ‘boot process’ follows guidelines contained in the Installation Guide and the CA Administrator’s Guide. As soon as the boot process is completed, the Boot Officers are removed from the system and can no longer be authenticated.

7.1.3 Access Control

The TOE User identification is a TLS Client Authentication Process, whereby a mutual authentication is achieved between server and client. Thus, it is not possible for authentication data to be forged or reused (as a new challenge is issued each time). While the TLS session is still open, the Request Manager maintains the identity of the TOE User by verifying the Officer role that has been defined for the TOE User certificate in the TOE. Before a TOE process (e.g. one of the Request Factories) accesses any of the TSF Data Objects, or performs any operation resulting in a change to those objects, the Access Manager is asked whether the requested access is permitted by validation of the Officer's role. The request will only be processed if Access Manager grants permission. Decisions are based on the context of the TOE User in the Request Manager. Note that the TLS library is provided by the JRE (TOE environment) and is not in scope of the TOE.

All write, update or delete operations must be signed, and the signature is checked by the Access Manager before the operation is allowed. Write, update or delete operations on Admin Store records (i.e. the TSF Administration Officer, Registration Officer or CA Policy data objects) require a second Administration Officer signature. Access Manager also checks the validity of this signature.

The entry of certificate request data and certificate revocation request data is restricted to Officers and is verified by the Access Manager. Only Officers are authorized to perform certificate status changes in the TOE (i.e. place a certificate on hold, revoking a certificate). Moreover, the Access Manager ensures that CA Policy requests, i.e. to generate and destruct CA keys, and other functions is restricted to TOE users with the role of Administration Officers.

Integrity of the TSF Data Objects is maintained as the system runs by verifying signatures on the signed data objects and checking the correctness of hash values.

OCSP Clients
OCSP clients can be identified and authenticated by the OCSP Responder when TLS is enabled or by enforcing the use of signed OCSP client requests. Authorization of subjects is made either by matching the subject name to a table of authorized users or by matching the certificate to the content of a trust store. OCSP client identification and authentication is optional, but enforcement is decided upon by the CIMC policies.

Table 10, Access Control Rationale

Security Functional Component	Rationale
FDP_ACC.1 (iteration 2)	The TOE enforces policies for subset access control on Officers, Policy objects, and Requests by matching the Officer role, Officer issuing constraints and Officer domain belonging of the TOE user.
FDP_ACF.1 (iteration 2)	The TOE enforces policies for attribute based access control on Officers, Policy objects, and Requests by matching the Officer role, Officer issuing constraints and Officer domain belonging of the TOE user.

7.1.4 Identification and Authentication

Identification and authentication of users is accomplished by use of certificates, i.e. PKI based signed challenges and requests. All requests received by the Certificate Manager servers are first handled by the Request Manager component. The Request Manager authenticates the connecting Officer and during this process a client/server authenticated TLS session is established between the Certificate Manager Server and the Certificate Manager Client. The Officer uses a private authentication key for this purpose.

During the TLS negotiation, the TOE user authenticates to the server and while the TLS session is open, the TOE maintains the identity of the user. The TOE User (client software) can terminate the TLS session at any time. For TLS it relies on the TLS library of the Java Runtime Environment.

To verify that the TOE User is a valid Officer, the Access Manager is called to check the Admin Store entries and the validity of the Officer's authentication certificate. The TOE associates the authenticated user with subjects acting on behalf of the user. Before a TOE process accesses any of the TSF subjects or objects, or performs any operation resulting in a change to those subject or objects, the user's role is verified by the TOE before associating the user with subjects acting on behalf of the user.

OCSP Clients
The TOE configuration for authentication of OCSP users, defines whether users must be authenticated or not to accept and reply to OCSP requests. OCSP clients can be identified and authenticated by the OCSP Responder when TLS is enabled, or by enforcing use of signed OCSP client requests. The TLS client authentication certificate is checked for validity and the signed response to the TLS challenge is verified. The OCSP client request signing certificate is checked for validity. Simultaneously, the TOE TLS certificate is made available to the OCSP client. The OCSP client checks that a trusted CA has signed the certificate and that the TOE has sent a signed response to the TLS challenge. While the TLS session is still open, the OCSP Responder maintains the identity of the TOE User and when the OCSP reply has been delivered the client will terminate the connection.

Table 11, Timing of Identification and Authentication Rationale

Security Functional Component	Rationale
FIA_AFL.1	If authentication is not performed in a cryptographic module that has been FIPS 140-2 validated to an overall Level of 2 or higher with Level 3 or higher for Roles and Services, the TOE detects when an Administrator configurable maximum limit for unsuccessful authentication attempts has occurred since the last successful authentication for the indicated user identity. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TOE does nothing since for the certificate-based authentication there is no such limit.
FIA_ATD.1	Attributes required by the TOE to enforce the Access Control Policy, the generation of audit records, and proper identification and authentication of users are the following: the digital certificate and the user role bounded to the certificate. Every subject is associated with the user identity and user role.
FIA_SOS.1 (iteration 2)	The TOE relies on certificate-based authentication, and therefore does not use passwords for authentication. The certificate-based authentication mechanism verifies validity of the Officer's authentication certificate based on authentication keys stored on cryptographic smart cards and through PKI based signed challenges and requests. Authentication data cannot be forged or reused as a new challenge is issued each time. Since the TOE performs authentication based on certificates, the requirement, which concerns a mechanism to verify password-based authentication, is not applicable.
FIA_UAU.1 (iteration 2)	The TOE allows OCSP user queries without authentication.
FIA_UID.1 (iteration 2)	The TOE allows OCSP user queries without identification.
FIA_USB.1 (iteration 2)	The TSF determines the user identity from the digital certificate presented by the user during authentication or signing, and matches the certificate with the associated digitally signed user role in the database.

7.1.5 Remote Data Entry and Export

The TSF enforce the generation of evidence of origin for all security related information and relates the identity, role of the user and signature of each transaction of the originator of the information.

Any information obtained is provided using an HTTPS mutually authenticated connection. Each transaction arriving through such a connection is validated and is

auditable at all times. TOE OCSP responder can be configured to accept unauthenticated OCSP users.

The TSF enforces secure data entry for certificate creation, revocation, registration, keys, PIN/PUK, and other data. The TOE enables secure export of certificates, CRLs, CILs, keys, PIN/PUK, and OCSP responses.

Data entry and export within the TOE environment to the TOE database can use a secure connection if enabled by the database server. The database server can be installed on the same host as the TOE to eliminate the need of remote connection, or a integrity protected network connection be used. Connection to HSM's in the TOE environment is established using the secure connection mechanism provided by the HSM.

Table 12, Remote Data Entry and Export Rationale

Security Functional Component	Rationale
FCO_NRO_CIMC.3	By use of identity, role of the user, signature and verification of each transaction of the originator of the information over TLS authenticated connection.
FDP_ITT.1 (iteration 3 and 4)	By use of mutually authenticated secure connections.
FDP_UCT.1 (iteration 2)	By use of secure connection to TOE database and HSM.
FPT_ITC.1 (iteration 2)	By use of secure communication method supported by remote IT product.
FPT_ITT.1 (iteration 3 and 4)	By use of mutually authenticated secure connections.
FCO_NRO_CIMC.4	By use of signature by Officer with authorized role.

7.1.5.1 Certificate Status Export

The TSF Certificate and Status Distribution Process is mapped onto the Distribution Agent component. This component is responsible for preparing the data content and distribution information for distribution of certificates and CRLs/CILs to the various LDAP directories, HTTP servers, OCSP Responders, as specified in the CA Policy Distribution Rules.

Certificate Activation and Certificate Revocation status provision over OCSP with the OCSP Responder is realized by publishing CILs and CRLs from the Certificate Manager to the responder by using an HTTP/HTTPS push mechanism. Certificate Activation with OCSP implies that the certificate activation status is made available to the responder by the use of CILs that have been signed by the Certificate Manager. Certificate Activation over OCSP is an optional configuration.

Certificate Status Information Provision – OCSP
Certificate Activation in the Certificate Manager and OCSP Responder is realized by adding certificate serial numbers of activated or issued certificates in a signed Certificate Issuance List (CIL). The CIL is a proprietary format designed by Nexus that is based on the CRL specification (see RFC 5280). In comparison to a CRL that lists all revoked certificates, a CIL contains all certificates issued by the signing CA. Expired certificates are not removed and therefore the list contains a definite statement whether a specific certificate serial number has ever been issued. The

content of the CIL can be configured to contain only activated certificates. This configuration is done in a policy configuration, using CIL procedures. More information about CIL can be found in the guidance document Nexus Certificate Manager Technical Description.

The OCSP Responder enables different CIL option: without CIL, with CIL that contains certificate serial numbers of all issued certificates, and with CIL that contains specifically activated certificates. Certificate revocation in Certificate Manager results in signing of CRL. The CRL is provided to the OCSP Responder to enable it to answer on certificate revocation status. The OCSP Responder component is part of the TOE.

The OCSP Responder component provides the following status information when used with CIL:

- Certificate unknown
- Certificate good (i.e. activated or issued certificate, but may have expired)
- Certificate revoked (i.e. revoked or not issued/activated)

The OCSP Responder component provides the following status information when used without CIL:

- Certificate unknown
- Certificate good (but certificate may not exist or may have expired)
- Certificate revoked

It is allowable for the OCSP Responder not to reply. However, if it does reply then the information must be guaranteed to be correct. OCSP responses are signed by an accredited HSM (not part of the TOE).

Together with CRLs, CILs are used to support the extended revoked definition in OCSP as defined in RFC 6960 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP).

Certificate Status Information Provision – CRL
Certificate Status Information Provision with CRL is handled in accordance with RFC 5280 and RFC 5755. CRL procedures define the type and issuance parameters for the chosen CRL type, i.e. complete CRL, CRL distribution point partitioned CRL, and indirect CRL. All CRL types can be created and distributed both as full CRLs and delta CRLs. A CRL procedure is used with Distribution Rules for configuring the LDAP and HTTP/HTTPS connection parameters to publish the CRL to LDAP servers, OCSP Responders, and http servers.

Table 14, Certificate Status Export Rationale

Security Functional Component	Rationale
FDP_CIMC_CSE.1	The TOE export certificate status according to the X.509 standard for CRLs, and CIL, the Nexus defined format for listing of issued certificates.

7.1.6 Key Management: Key Storage, Key Destruction and Key Export

Key Storage
The TOE relies on CIMC keys being protected by use of FIPS 140-2 validated HSM. The CIMC keys are generated and used within the HSM. Backup of CIMC keys cannot be done by the TOE and must be handled in accordance with the secure mechanisms provided by the HSM.

Certificate subject private keys can be archived in encrypted form in the TOE database. Secure encryption of the keys to be archived is achieved by using a FIPS 140-2 validated HSM and key encryption keys, KEK's. To support clients in archiving and recovery of keys, the CIMC server enables clients to submit asymmetric Key Archiving and Recovery, KAR, requests. The KAR factory module processes the archiving and recovery request. Prior to archiving a subject private key in the CMDB it is encrypted using a symmetric Key Encryption Key, KEK, in the HSM. Depending on the configuration, either a master KEK can be used for all archived keys, or individual KEKs be used to protect each archived key. The KEK will be encrypted and archived along with the archived key. Protection of KEKs is done with a master key that never leaves the HSM by other means than the backup facilities of the HSM. Keys with keyUsage NonRepudiation / Content Commitment cannot be archived for user privacy reasons. The archiving process has the following options:

- Archive - generates key pair and archive the private key.
- Generate - generates key pair without archiving the private key.
- ImportToArchive - archives private keys submitted by a CM SDK application.

The recovery process has the following options:

- Recover - recovers the latest issued key and certificate for the user.
- RecoverAllHistory - recovers all archived keys and certificates for the user.
- RecoverKeyHistory - recovers the latest issued key and all its certificates for the user.

Key Destruction
Cryptographic keys are destroyed by the cryptographic module in accordance with the FIPS 140-2 cryptographic key destruction method to ensure that an untrusted entity cannot use a trusted entity's key to sign malicious code. In addition, this security functionality requires that in case TOE users detect an attack, they are to be able to destroy any plaintext keys within the TOE in order to prevent the attacker from obtaining copies of these keys (Section 6.2.8.5).

Key Export
The TOE ensures that private and secret keys are protected when they are transmitted to and from the TOE: the keys shall only be exported from the TOE in encrypted form or using split knowledge procedures. Electronically distributed secret and private keys shall only be exported from the TOE in encrypted form. The keys are exported to either a smart card or to a PKCS#12 soft certificate. Both Smart card and PKCS#12 certificates are supported. The smart card is protected by a PIN and the PKCS#12 file is encrypted and password protected. AES and

3DES are used for the encryption of the private key stored in PKCS#12 files. The AES and 3DES encryption is performed by the FIPS 140-2 validated HSM (Section 6.1.4.2).

PIN Management
Smart card PINs and PUKs are stored encrypted in CMDB. An HSM must be used for highest level of protection. Storing PIN/PUK is an optional choice of providing service for PIN/PUK retrieval after authorization of a PIN/PUK retrieval request.

Table 13, Key Management Rationale

Security Functional Component	Rationale
FDP_ACF_CIMC.2	TOE User private keys are not stored in the TOE. Archived certificate subject private are protected by the TOE by use of FIPS 140-2 validated HSM.
FMT_MTD_CIMC.4	TSF private keys are generated and used within a FIPS 140-2 validated HSM.
FDP_SDI_CIMC.3	A public key used outside the FIPS 140-2 validated HSM by the CIMC is stored in a certificate. The certificate signature is verified when the public key is used by the CIMC. If the signature verification fails, an Audit event is recorded and the attempted use of the key is stopped.
FDP_ACF_CIMC.3	If user secret keys (PINs) are stored in the TOE database they are encrypted with a key in a FIPS 140-2 validated HSM.
FMT_MTD_CIMC.5	TSF secret keys used for protecting archived certificate subject keys are stored in the database only after being encrypted by a key protected within a FIPS 140-2 validated HSM.
FCS_CKM_CIMC.5	Zeroization of CIMC private key is managed by the FIPS 140-2 HSM that maintains the key by command from CIMC dual users. Zeroization of encrypted secret key stored in the TOE database is managed by a CIMC user.
FDP_ETC_CIMC.5	AES or 3DES is used for the encryption of the private key stored in PKCS#12 files. Default is to use AES, but 3DES is also available in case the client software does not support AES. The AES and 3DES encryption is performed by the FIPS 140-2 validated HSM.
FMT_MTD_CIMC.7	The secure procedures provided by the FIPS 140-2 validated HSM must be followed for backup of TSF private keys.

The FIPS 140-2 validated HSM is part of the TOE environment and is described in Section 6.1.13. SFRs concerning the cryptography for the HSM are described in Section 6.2.10.

7.1.7 Certificate Profile Management

The TOE enables certificate profiles to be configured in accordance with:

- ISO/ITU X.509

- X.509/RFC 5755 attribute certificates
- RFC 5280
- Card Verifiable Certificates (CVC) according to Gematik specification Electronic Health Card, Part 1, v2.0.0. Generations G0, G1 and G2. CPI types: 3, 4, 21, 22 and 70
- Card Verifiable Certificates (CVC) according to the BSI Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token. CPI type: 0.
- IEEE 1609.2 certificates,
- Tachograph Certificates, ISO 9796-2
- Certificate Transparency Precertificates, RFC 6962
- PGP certificates, RFC 4880

Certificate profile management with certificate format and certificate procedures requires Administration Officers role.

Table 14, Certificate Profile Management Rationale

Security Functional Component	Rationale
FMT_MOF_CIMC.3	TOE configuration of certificate profiles by Administration Officer for specifying acceptable values for key owner's identifier, algorithm identifier, certificate issuer identifier, validity period of certificate, keyUsage, basicConstraints, certificatePolicies, and additional fields and extensions.

7.1.8 Certificate Revocation List Profile Management

The TOE enables certificate revocation list profiles to be configured in accordance with:

- ISO/ITU X.509
- RFC 5280
- RFC 5755

Certificate revocation list profile management using CRL formats and CRL procedures requires Administration Officers role.

Table 15, CRL Profile Management Rationale

Security Functional Component	Rationale
FMT_MOF_CIMC.5	TOE configuration of CRL profiles by Administration Officer for specifying acceptable values for Issuer, IssuerAltName extension, nextUpdate and other extensions.

7.1.9 OCSP Profile Management

The TOE enables OCSP responder profiles to be configured for acceptable values, fields and types in OCSP responses in accordance with:

- RFC 6960

OCSP responder profile management requires an Administrator.

Table 16, OCSP Profile Management Rationale

Security Functional Component	Rationale
FMT_MOF_CIMC.6	TOE configuration of OCSP profiles by Administrator for specifying acceptable values for ResponderID and types Basic, Non-issued Basic, Identrus-Basic, Cached, Non-issued Cached or Identrus-Cached, and other parameters of relevance for the OCSP responder.

7.1.10 Certificate Registration

The TOE enables certificate generation of types listed under section Certificate Profile Management.

Certificate and Subject Data Registration
Signed certificate requests (and/or certificate orders) are received via the Request Manager over a secure channel. The Registration Officer signs the data and the Access Manager component checks that the Officer signing the request is properly authorized. The received certificate request data is stored as a signed data record in the AuditLog table in the Certificate Manager Database (CMDB).

Subject data registration is done by a Registration Officer as preparation prior to receiving certificate requests in the scenario the CA operation requires automated validation of certificate request content from end-entities. Automated validation is performed in certain certificate enrolment scenarios, i.e. using certificate enrolment protocols Simple Certificate Enrolment Protocol (SCEP) and Certificate Management Protocol (CMP), with client hardware devices. Subject data registration is also done to prepare for smart card batch production. The Registration Officer signs the subject data and the Request manager and the Access Manager authorizes the request in the same way as with certificate requests.

Certificate Preparation
The data content of a certificate is prepared by the Certificate Factory component using the signed certificate request data plus possibly other data (determined by the CA Policy – see Section 1.4.1.1) and the public key read from the user's smart card. The signed certificate request data is checked for consistency by a 'Modifier' component built into Certificate Factory. The Access Manager is called to verify the requesting Officer's signature.

The user's public key is either included as part of the signed certificate request data (in the case of single issuance of a smart card at a Registration Authority workstation) or as part of batch card production (at a Batch Explorer, Card

Production Workstation). In this latter case, the certificate request data is held as a reference in the 'ProductionOrders' table of the CMDB database. The reference is to the certificate request data held in the AuditLog table. As a production batch is progressed, the user's public keys are read from the smart cards as each card is processed. The Card Production Workstation software then requests certificate creation for each card in turn. The processing of a production batch is initiated by a request to Request Manager signed by a Registration Officer.

Batch Processing
The Certificate Manager issues smart cards with key pairs and certificates that bind the name of the owner of the smart card to the corresponding public key. Batch processing for volume production of smart cards involves steps of card order registration, registration of data for certificates, visual personalization, logistical handling, PIN letter distribution and chip personalization.

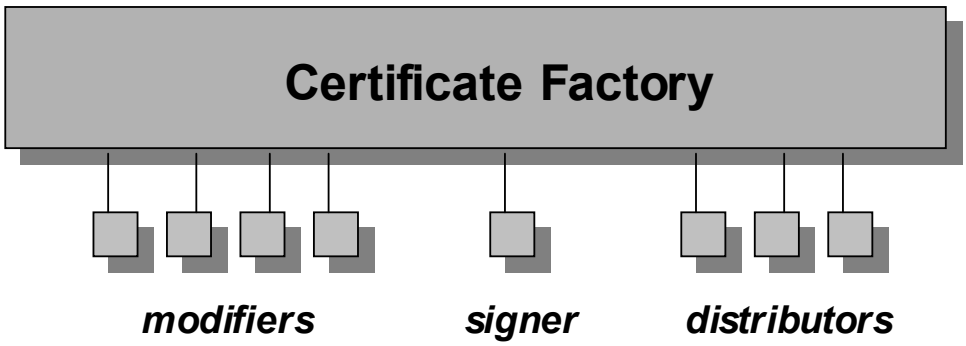

Figure 2: Certificate Factory showing Modifier, Signer and Distributor Components

Certificate Signing
Once the certificate data has been prepared (including the user's public key) it is sent to the 'Certificate Issuing System' (CIS) for signing by a CA key. Signed Certificate Request Data is written as a record to the Audit Log as part of the normal request process. This data is used by Certificate Factory when initiating certificate signature by the CIS. The CA key used by the CIS for certificate signing is held on an evaluated or accredited Hardware Security Module (HSM). The CIS is responsible for signing the certificate by sending the data required by the configured signature algorithm to the HSM driver for signature by the HSM. This means that the hash is either computed by the Certificate Factory or the HSM.

CIS signature requests are logged to the CIS log file.

Certificate Activation
Some accreditation schemes require that certificates may only be activated after some well-defined criteria has been fulfilled, e.g. that the user has proven possession of his smart card. Proof of possession is outside the scope of the TOE but the interface to request certificate activation is included. The Certificate Controller client and CM SDK handles activation requests in a similar way to the Registration Interface, i.e. signed requests are received over a secure channel. Request Manager and Access Manager thereby ensure that the TOE does not accept activation requests through channels that are not secure and does not accept requests that have not been signed by an authorized person. The activated

certificate status is updated by setting the 'ActivationTime' in CMDB to the time of activation. A CIL procedure will populate a Certificate Issuance List with certificate serial numbers of all issued or only with specifically activated certificates. The CIL (and CRL) is distributed to the OCSP responder to enable provision of certificate status information to OCSP clients.

TOE Components Involved in the Certificate Manager Request Process
The (TSF) Certificate Manager Request Process is mapped to a number of TOE components. These are:

- Request Manager: This is the component that manages the interface towards the TOE users i.e. maintaining the context of the current user and establishing the protected TLS communication channel.
- Request Factories: These components perform the actual tasks requested by the TOE users. The various factories are:
    - Request Manager: This is responsible for distributing the incoming requests to the other factory components
    - Certificate Factory: This component builds the certificate data to be signed by the CIS as well as initiating the publication of certificates if they are to be published as soon as they are created.
    - Publication Factory: This component is responsible for initiating the publication of certificates as a result of a delayed publication request from a Registration Officer.
    - CRL Factory: The CRL Factory is responsible for constructing lists of revoked certificates.
- Access Manager: This component is responsible for checking TOE user authorization levels. All other components rely upon Access Manager to perform these checks.
- Certificate Issuing System (CIS): This component is responsible for signing certificates, CRLs and CILs and it's also responsible for signing the CIS Log entries.

Table 17, Certificate Generation Rationale

Security Functional Component	Rationale
FDP_CIMC_CER.1 Certificate Generation	The TOE generates certificates consistent with the configured profiles for respective certificate type, X.509, RFC5280, RFC5755, CVC, ISO 9796-2 tachograph certificate, RFC6962 precertificate, PGP certificates, 1609.2 certificates.

7.1.11 Certificate Revocation (CRL and OCSP Validation)

Signed certificate revocation requests are received by the Request Manager over a secure channel. The Revocation Interface ensures that the TOE does not accept revocation requests through channels that are not secure and does not accept requests that are not signed by an authorized user. Revocation requests are processed by the Request Factory components (in this case the CRL Factory and Revocation Factory) and result in the certificate status being changed in the CMDB

database. Subsequent to certificate revocation, the CRL is updated/the certificate is added to the CRL.

The TOE enables certificate revocation and generation of CRLs according to X.509 and allow OCSP responses according to RFC 6960.

Table 20, Certificate CRL and OCSP Validation Rationale

Security Functional Component	Rationale
FDP_CIMC_CRL.1	The TOE generates CRLs consistent with the configured CRL profiles and CRL procedures in accordance with X.509.
FDP_CIMC_OCSP.1	The TOE generates OCSP responses consistent with the responder configuration in accordance with RFC 6960.

7.1.12 Strength of Function

Please, refer to Section 6.1.13 for detailed information regarding the strength of function requirements.

Table 18, Strength of Function Rationale

Security Functional Component	Rationale
FCS_SOF_CIMC.1	The TOE provides cryptographic mechanisms that fulfil the specific Strength of Function requirements of Section 6.1.13.2

8 Annex

8.1 Abbreviations

AWB	Administrator’s workbench
CA	Certification authority
CC	Common Criteria
CCM	Central certificate manager
CF	Certificate factory
CIL	Certificate issuance list
CIMC	Certificate Issuing and Management Components
CIMS	Certificate Issuing and Management System
CIS	Certificate issuing system
CM	Certificate manager
CRL	Certificate revocation list
EAL	Evaluation assurance level
HSM	Hardware security module
OCSP	Online certificate status protocol
OSP	Organisational security policy
SAR	Security assurance requirements
SFR	Security functional requirements
SSCD	Secure signature creation device (HSM)
TOE	Target of evaluation
TSF	TOE security function
SFP	Security function policy

8.2 References

[CC]	Common Criteria for Information Technology Security Evaluation. - Part 1: Introduction and general model, April 2017, Version 3.1 Revision 5, CCMB-2017-04-001; - Part 2: Security functional Components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002; - Part 3: Security Assurance Components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5, CCMB-2017-04-004.
[SP188]	Swedish Certification Body for IT Security, 188 Scheme Crypto Policy, Issue: 7.0, 2017-04-04 http://fmv.se/Global/SP-188.pdf
[cPPND]	Collaborative Protection Profile for Network Devices, Version 1.0, 27-Feb-2015. https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[RFC5639]	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010. https://tools.ietf.org/html/rfc5639
[ISO15446]	Technical Report ISO/IEC TR 15446, Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets, Second edition 2009-03-01.
[ECDSA]	ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).
[ISO 18033-3]	ISO/IEC 18033 specifies encryption systems (ciphers) for the purpose of data confidentiality.
[FIPS180]	Secure Hash Standard, Federal Information Processing Standards Publication 180-2, 1 August 2002. http://www.csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf
[FIPS186]	Digital Signature Standard (DSS), FIPS-186-4 July 2013. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
[FIPS197]	Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
[FIPS198]	The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198, July 2008. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf
[FIPS202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, Federal Information Processing Standards Publication 202, August 2015.

[SP 800-38A]	NIST Special Publication 800-38A 2001 Edition, NIST Special Publication 800-38A 2001 Edition, Recommendation for Block Cipher Modes of Operation. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf
[PKCS1]	PKCS #1: RSA Cryptography Specifications Version 2.2. https://datatracker.ietf.org/doc/rfc8017/
[CERT-PP]	Certificate Issuing and Management Components Protection Profile, Version 1.5, 11 August 2011.
[CERT-CR]	Certification Report, Evaluation of Certificate Issuing and Management Components Protection Profile, Version 1.5, Issued by the Communications Security Establishment Canada Certification Body, 383-6-3-CR, Version 1.1, 9 September 2011.
[RFC4880]	OpenPGP Message Format. https://www.ietf.org/rfc/rfc4880.txt
[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. https://www.ietf.org/rfc/rfc5280.txt
[RFC6962]	Certificate Transparency, https://tools.ietf.org/html/rfc6962