verizon✓

Verizon UniCERT

Security Target

Common Criteria: EAL2+ALC_FLR.2

Version 0.8

01-Apr-2021

Document management

Document identification

Document ID	EAL2+_ASE
Document title	Verizon UniCERT Security Target
Release authority	Henk Van Wulpen
Product version	Verizon UniCERT – v5.5.1

Document history

Version	Date	Description
0.1	25-Sep-20	Initial internal draft release.
0.2	23-Oct-20	Revisions based in initial comments
0.3	24-Nov-20	Updated table 2
0.4	30-Nov-20	Internal release
0.5	23-Dec-20	Updating as per T2005-3-EOR001 0.3
0.6	06-Jan-21	Updating as per T2005-3-EOR001 0.5
0.7	27-Jan-21	Minor changes for full consistency with the TOE
0.8	01-Apr-21	Changes to the TOE supporting software

Copyright notice

Table of Contents

List of Tables

List of Figures

1 Security Target introduction (ASE_INT)

1.1 ST and TOE identification

ST Title	Verizon UniCERT Security Target
ST Version	0.8, 01-Apr-2021
TOE Name	Verizon UniCERT
TOE Version	v5.5.1
Assurance Level	EAL2+ALC_FLR.2
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1 (Revision 5), April 2017, incorporating: • Part One – Introduction and General Model; • Part Two – Security Functional Components; and • Part Three – Security Assurance Components. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, April 2017, Version 3.1, Revision 5
Keywords	Public Key Infrastructure, Certification Authority, Registration Authority, Key Archival

Within the ST, references (see Section 1.4) are given as mnemonics within square brackets. Terms and abbreviations are defined in the Glossary (see Section 1.2) or in [CC] Part 1.

1.2 Document organization

This document is organized into the following sections:

- Section 1 provides the introductory material for the ST.
- Section 2 provides the conformance claims for the evaluation.
- Section 3 provides the security problem to be addressed by the TOE and the operational environment of the TOE.

- Section 4 defines the security objectives for the TOE and the environment.
- Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE.
- Section 7 provides the rationales for the various sections of the Security Target.

1.3 Terminology

Terminology used in this Security Target is specific to the TOE and more generally a public key infrastructure (see Annex A).

Readers are assumed to be familiar with the main concepts of a PKI system, in addition to a basic understanding of cryptographic terms such as public and private keys, digital signatures and (X.509) certificates. The reader is also assumed to have knowledge of the general concepts and principles of IT security evaluation as described in [CC], Part 1.

1.4 References

[3DES] SP800-67 Rev 2 (https://csrc.nist.gov/publications/detail/sp/800-67/rev-2/final)

[AES] FIPS-197 (http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf)

[CC] Common Criteria for Information Technology Security Evaluation, Parts 1, 2 and 3, CCMB-2017-04-001-3, Version 3.1 Revision 5, April 2017

[CEM] Common Methodology for Information Technology Security Evaluation, CCMB 2017-04-004, Version 3.1 Revision 5, April 2017

[DER] ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) ITU-T Rec. X.690 (07/2002) | ISO/IEC 8825-1, (http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf)

[DSA] Digital Signature Standard (DSS), FIPS-186-4 July 2013 (https://doi.org/10.6028/NIST.FIPS.186-4)

[ECDSA] ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

[OCSP] Online Certificate Status Protocol, RFC 2560, (http://tools.ietf.org/html/rfc2560).

[PEM] Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services (https://tools.ietf.org/rfc/rfc1424.txt)

[PKCS7] PKCS #7 v1.5: Cryptographic Message Syntax Standard, RSA Laboratories, March 1998 (https://tools.ietf.org/html/rfc2315)

[PKCS10] PKCS #10 v1.7: Certification Request Syntax Standard, RSA Laboratories, November 2000 (https://tools.ietf.org/html/rfc2986)

[PKCS11] PKCS #11 Cryptographic Token Interface Standard, OASIS Standard, v2.40 April 2015 (http://docs.oasis-open.org/pkcs11/pkcs11-base/v2.40/os/pkcs11-base-v2.40-os.pdf)

[PKCS12] PKCS#12 Personal Information Exchange Syntax, RSA Laboratories, v1.1, July 2014 (https://tools.ietf.org/html/rfc7292)

[RFC] RFC 5280, IETF (www.ietf.org/rfc/rfc5280.txt)

[RSA] PKCS #1RSA Cryptography Specifications, v2.2, November 2016 (https://www.rfc-editor.org/rfc/rfc8017.txt)

[SCEP] Simple Certificate Enrolment Protocol, https://tools.ietf.org/id/draft-nourse-scep-19.txt

[SEC2] SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research, September 2000, Version 1.

[SHA-1] (Part of) Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August 2015 (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf)

[SHA-2] (Part of) Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August 2015 (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf)

1.5 TOE overview

1.5.1 TOE type and usage

The TOE is Verizon UniCERT v5.5.1, also referred to throughout the document as UniCERT, is a software product which provides all the (PKI-specific) functionality needed to implement a Public Key Infrastructure (PKI) system.

The primary function of a PKI system is to issue and manage digital certificates that allow other IT systems to verify the identity of the holder. UniCERT provides all the functionality needed to implement a PKI system, essentially a system that provides certificate registration, PKI management, a Certification Authority, and certificate lifecycle management functions. The TOE can then be used to manage all the keys necessary for a system requiring security for end users, such as a secure messaging system, or secure use of Web browsers. UniCERT provides the ability to set up a centralized or a distributed PKI for organizations of any size.

The TOE includes the following core components:

- **Certification Authority (CA) core component**. The CA core component is the CA Platform which is responsible for the generation and issuance (i.e. publication or distribution) of certificates and certificate revocation lists, and for the overall management of certificates and the PKI in general. It includes a number of elements described in Sect. 1.6.1.1

- **Registration Authority (RA) core component**. The RA is the RA Platform which is responsible for gathering registration information and revocation requests, authorizing requests, and handling renewals. It also includes the **WebRAO Servers** and **WebRAO Clients** which allow clients to interact with the RA remotely. The control over the functions the Registration Authority components are allowed to perform is provided by the Certification Authority Operator component. It includes a number of elements described in Sect. 1.6.1.2

In addition, the TOE may be configured with certain optional “advanced components” (other Verizon products); however, only two of these components may form part of the TOE:

- **The Key Archiver (KAS)** which allows archiving of the cryptographic keys. It consists of elements as described in Sect. 1.6.1.3

- **The Autoenroll Solution**. This component supports the automatic registration, generation, and distribution of certificates for use with computers in a Microsoft Windows domain. It is further described in Sect. 1.6.1.4.

- Various **Utilities** to assist the operators of the TOE. These are described in Sect. 1.6.1.5.

Although the TOE provides all the PKI-specific functionality needed to implement a PKI system, such a system must be hosted on a hardware platform and must also include a Windows or Linux operating system, a database management system (Oracle), a web server, and a browser.

UniCERT may be deployed in a number of configurations consistent with the requirements identified in this Security Target where the deployed environment satisfies the objectives stated in section 4.2. Valid configurations include the use of hardware security modules (HSMs) or smartcards and:

- Deployment of all TOE components on a single platform;
- Deployment of TOE components across multiple platforms with or without multiple components on a single platform; or
- Deployment of TOE components on virtual servers.

An example UniCERT deployment is illustrated in Figure 1 below. Those components shown in blue are included within the scope of the UniCERT evaluation, and those in green (and the OCSP Server) are external to the TOE.

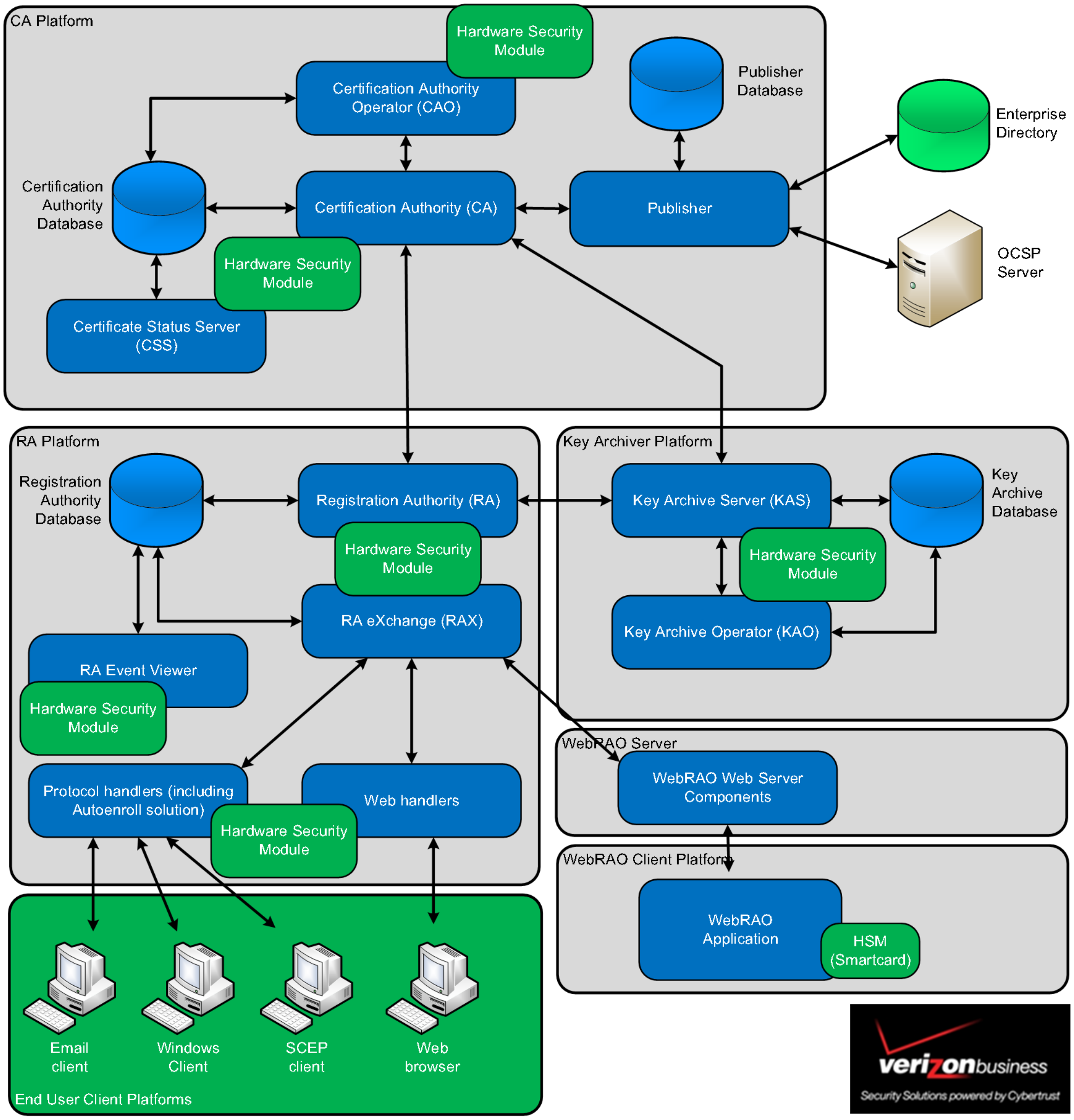

Figure 1 – Example UniCERT deployment

The combination of a correctly configured TOE and its operational environment (i.e. the non-TOE hardware and software) is referred to as “the PKI system” throughout this Security Target.

1.5.2 TOE security functions

From a security viewpoint, the principal requirements of a PKI system are that it should:

- Generate and issue certificates and CRLs with a guarantee of authenticity;
- Protect all private keys that it uses (or is responsible for) from unauthorized disclosure or modification; and
- Perform all tasks in a secure manner.

To meet these requirements, the TOE includes the major security features summarized in the following table.

Table 1 – Summary of TOE security features

Security feature	Description
Standard cryptographic methods	**Digital signature generation.** The TOE implements standard digital signature methods to: • Allow the content of certificates and CRLs to be verifiable and to prevent forgery and tampering; • Protect the integrity of data (including certificates and CRLs) when at rest and when in transit between components of the TOE; • The TOE allows TLS/SSL authentication of itself to the Enterprise Server to ensure that the Enterprise Server only accepts certificates published by a legitimate TOE.; and • Protect the integrity of messages transmitted between components of the TOE (which may or may not be hosted on different platforms).

Security feature	Description
	Data and private key confidentiality. The TOE implements standard cryptographic methods for protecting the confidentiality of data and symmetric keys when at rest and when in transit between components of the TOE. The confidentiality of data is protected by symmetric cryptographic methods and the confidentiality of symmetric keys is protected by asymmetric cryptographic methods.
Certificate lifecycle management	**Certificate generation, renewal, and distribution.** The TOE provides the capability to securely generate or renew digital certificates, in accordance with the operational policies defined for the TOE. The Certification Authorities perform this function for the TOE's own use and for distribution to entities that include users, applications and devices. Certificate generation binds the identity of an entity to a public key with a digital signature.
	Certificate status. The TOE maintains the status of digital certificates issued by the TOE and allows entities to query the status of digital certificates using the Online Certificate Status Protocol (OCSP).
	Certificate revocation, suspension, and expiry. The TOE provides the capability to suspend or revoke digital certificates where necessary, such as in response to suspected private key compromise. The TOE publishes revoked certificates on a Certificate Revocation List (CRL) in accordance with operational policy defined for the TOE.
Integration with hardware security modules and smartcards	While the TOE provides a range of standard cryptographic methods, the TOE may also be securely integrated with dedicated HSM devices and smartcards that are PKCS#11 compliant devices. These devices can be used for the delivery of cryptographic services to the TOE and for physically securing private keys related to the TOE components as required by the end user of the PKI system.

Security feature	Description
Key archival	The TOE provides a secure key repository and retrieval capability for end users' private encryption keys; this enables an end user to recover a key at a later date should the user's copy of the key become corrupt or lost. It also enables an organization to recover encrypted data if a key/certificate owner leaves the company unexpectedly.
PKI management	The TOE provides a range of functions and utilities for secure management of the TOE, and for establishing the public key infrastructure implemented by the TOE. The PKI infrastructure is implemented as a hierarchy of the following components: • Certification Authorities which provide the fundamental functions of the CAs in issuing PKI certificates for the users of the TOE, • Registration Authority which provides a secure registration service to the users of the PKI functions provided by the TOE, and • other TOE components as required. Access to PKI management functions is subject to successful identification and authentication of TOE users. The TOE includes ease-of-use features and utilities aimed at lessening the likelihood of human users making errors that may lead to a violation of security policy.
Security audit	The TOE provides automated auditing facilities that include extensive capabilities for protecting, querying, and archiving of audit records. The TOE supports assignment of authorized auditor roles for the management and review of audit logs generated by the TOE.

1.6 TOE description

1.6.1 Physical scope of the TOE

The TOE is a complex and flexible software product, and is comprised of several components, sub-components and utilities for the implementation of a public key infrastructure system. These components are described in subsequent sections.

1.6.1.1 Certification Authority (CA) Platform

The TOE CA core component is the CA Platform which is the nucleus of the PKI system. It consists of the following sub-components:

- **CA** (i.e. the main CA server), which generates certificates and CRLs and stores them in the CA Database (**CA DB**);
- **CA Operator** (CAO), which provides a GUI for authorized users to manage the PKI system in general;
- **Publisher**, which distributes and publishes certificates and CRLs, using a variety of distribution methods and directory formats, as well as stores them in the Published Database (**Publisher DB**); and
- **Certificate Status Server** (CSS), which responds to Online Certificate Status Protocol (OCSP) requests from other TOE components by providing real time certificate status information.

The CA core component and its external interfaces are illustrated in Figure 2 below. Sub-components shown in blue are included within the evaluation scope. Those sub-components shown in green are external to the TOE and not included within the scope of the evaluation.

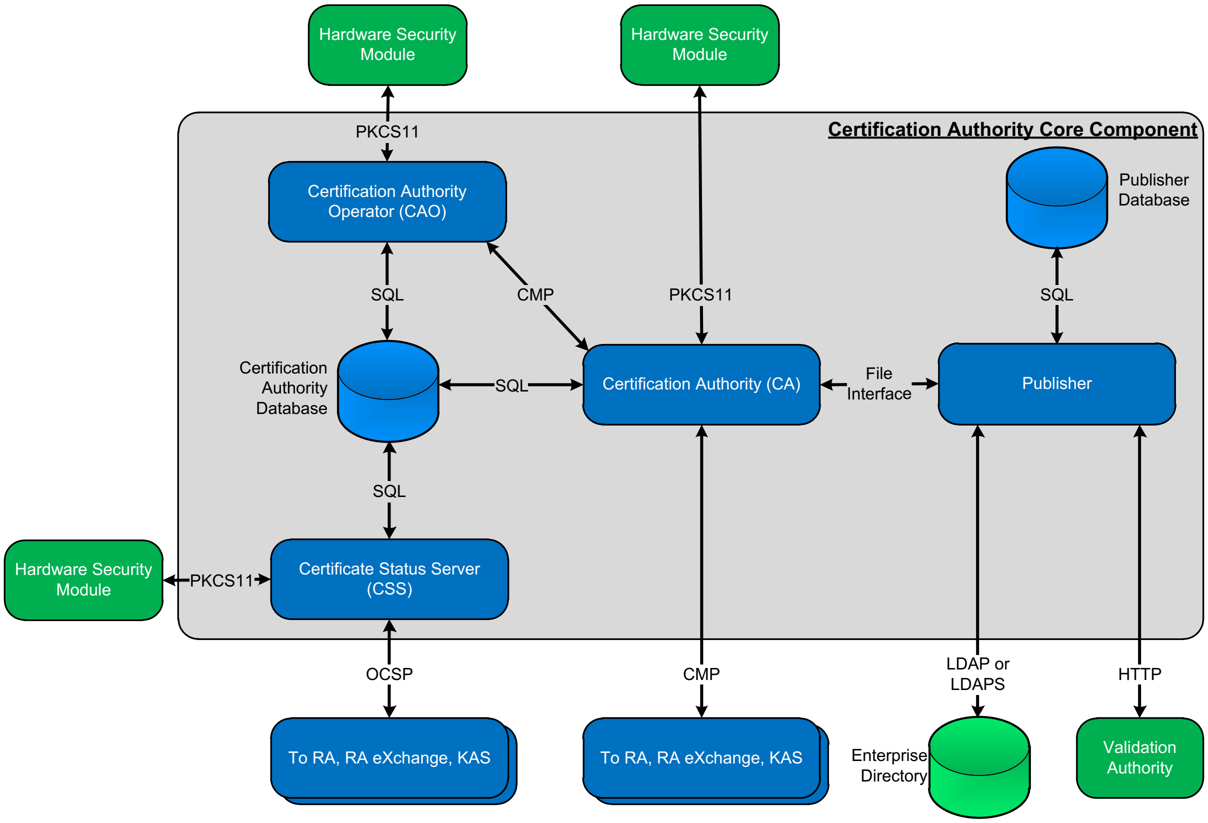

Figure 2 – Certification Authority (CA) core component

1.6.1.2 Registration Authority (RA) Platform

The TOE RA core component is the RA Platform which provides a registration portal for the PKI system, and an interface to the CA component. It receives, verifies and forwards requests to the CA[1] and sends back the CA's response. It consists of the following sub components:

- **RA** (i.e. the main RA server), which essentially acts as a router, transferring information between the CA and other RA sub-components and stores the Registration related data to the Registration Authority Database (**RA DB**);

- A number of **Web Registration Authorities Operators** (WebRAOs), each of which enables a WebRAO user to authorize certificate and revocation requests. A WebRAO consists of **Web Handlers** which are the routines managing the WebRAO interfaces, a **WebRAO Servlets** part, which resides on the operational environment, and a **WebRAO Client** application, which may be (and usually is) hosted on an external system;

[1] Typically requests for certificates or certificate status information from an external system

- A number of **protocol handlers** (Web Handler, Email Handler, SCEP Handler), which convert requests received from an external system (in a variety of formats) into a common internal format;

- **RA eXchange** (RAX), which provides a communication link between the RA, protocol handlers and WebRAOs; and

- **RA Event Viewer**, which provides a GUI for authorized users to access audit records produced by the RA sub-components.

The RA core component and its external interfaces are illustrated in Figure 3 below. Sub-components shown in blue are included within the evaluation scope. Those sub-components shown in green are external to the TOE and not included within the scope of the evaluation. Those sub-components shown in red are explicitly excluded from the TOE. Note that the WebHandler servlets and JSPs, WebRAO servlets and JSPs, and the WebRAO client application are all sub-components that are part of the RA core component, but are shown outside of the component boundary to illustrate their deployment on web technologies.

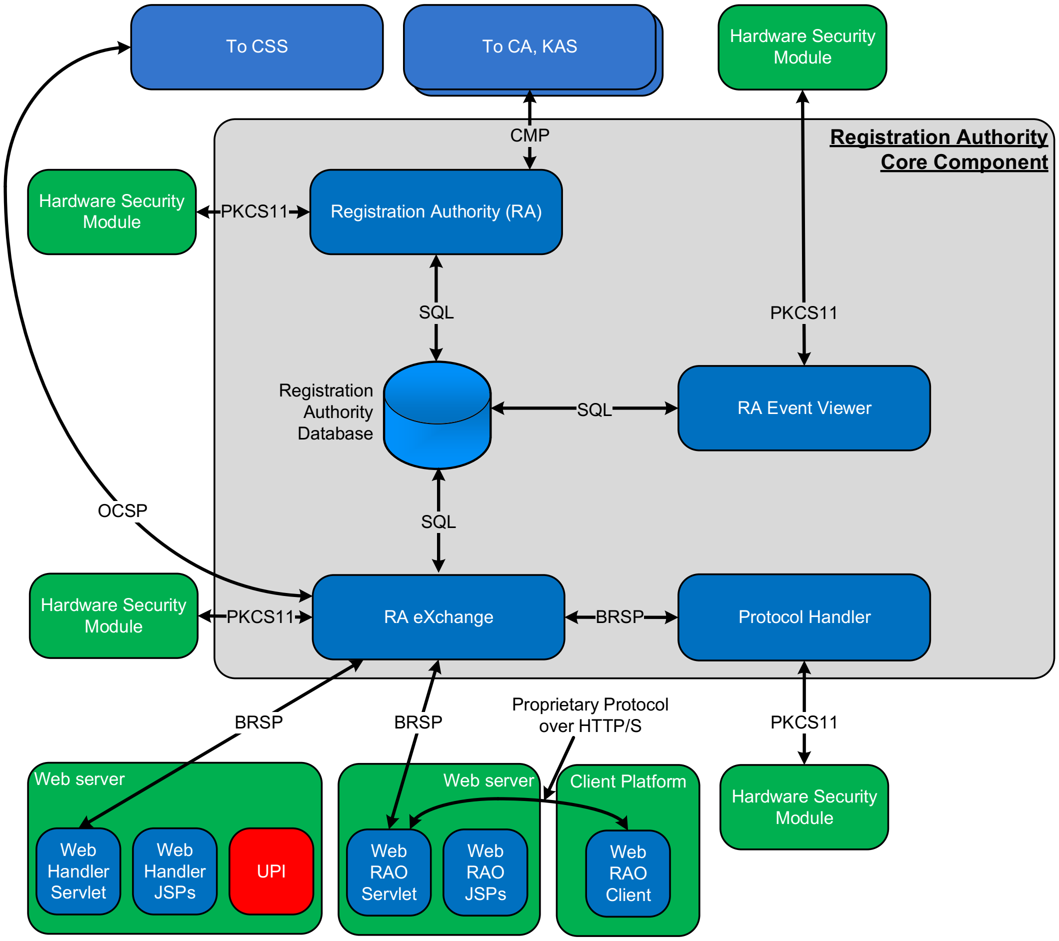

Figure 3 – Registration Authority (RA) core component

The following protocol handlers and interface items are explicitly excluded from the evaluation scope for the CA and RA core components:

- The CMP Handler (a protocol handler, not shown in Figure 3); and
- The UniCERT Programmatic Interface (UPI).

1.6.1.3 Key Archiver

Key Archiver provides a facility to archive and retrieve private keys and consists of the following sub components:

- **Key Archive Server (KAS)**, which securely archives - in a **KAS database** - private keys received via the RA and KAO components. It also provides mechanisms to recover a key at a later date, e.g. should (the original copy of) the key become corrupted, or should a cryptographic token on which (the original copy of) the key is stored be damaged or lost; and

- **Key Archive Operator (KAO)**, which provides a GUI for authorized users to manage the KAS.

The Key Archiver component and its external interfaces are illustrated in Figure 4 below. Sub-components shown in blue are included within the evaluation scope. Those sub-components shown in green are external to the TOE and not included within the scope of the evaluation.

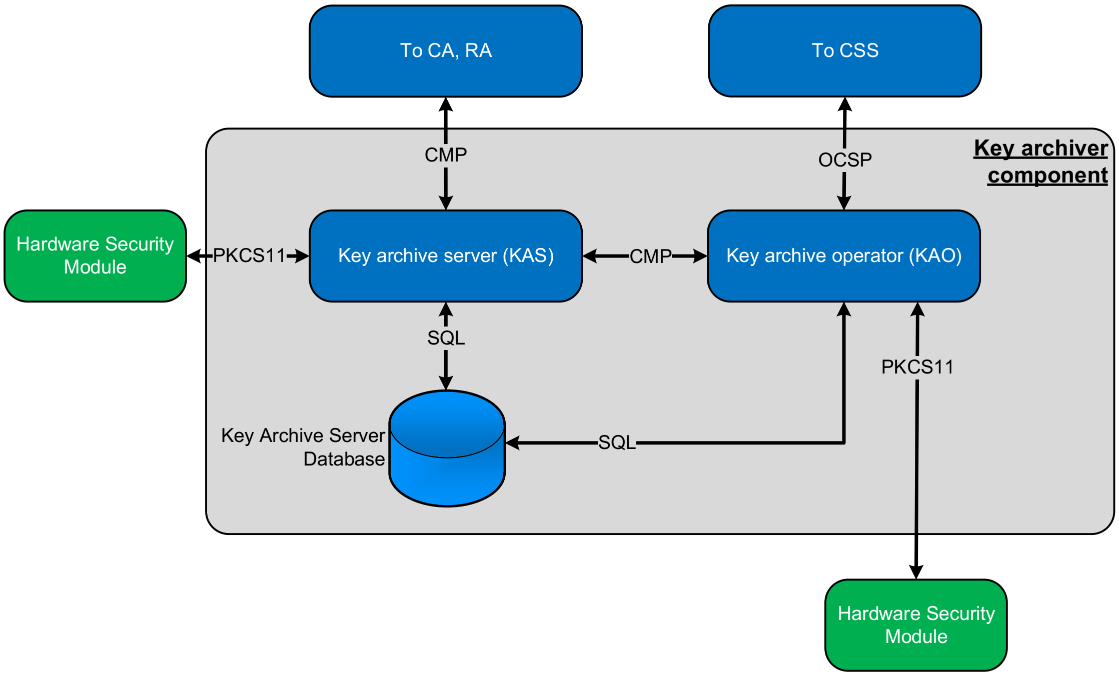

Figure 4 – Key Archiver core component

1.6.1.4 Autoenroll Solution

The Autoenroll Solution supports the automatic registration, generation and distribution of certificates to be used with computers in a Microsoft Windows domain. It consists of the following sub components:

- **Autoenroll Handler**, which is a protocol handler that handles Microsoft Autoenroll requests, but differs somewhat from other protocol handlers in that it may be hosted on an external system. Hence, it is not classed as an RA sub-component (but it does communicate with the RA eXchange);

- **Autoenroll Publisher**, which functions in a similar manner to the CA Publisher sub-component, but - because it needs to be co-located with the Autoenroll Handler - may be hosted on an external system. Hence, the CA communicates with the Autoenroll Handler (via the RAX) rather than with the Autoenroll Publisher directly.

The Autoenroll components and its external interfaces are illustrated in Figure 5 below. Sub-components shown in blue are included within the evaluation scope. Those sub-components shown in green are external to the TOE and not included within the scope of the evaluation.

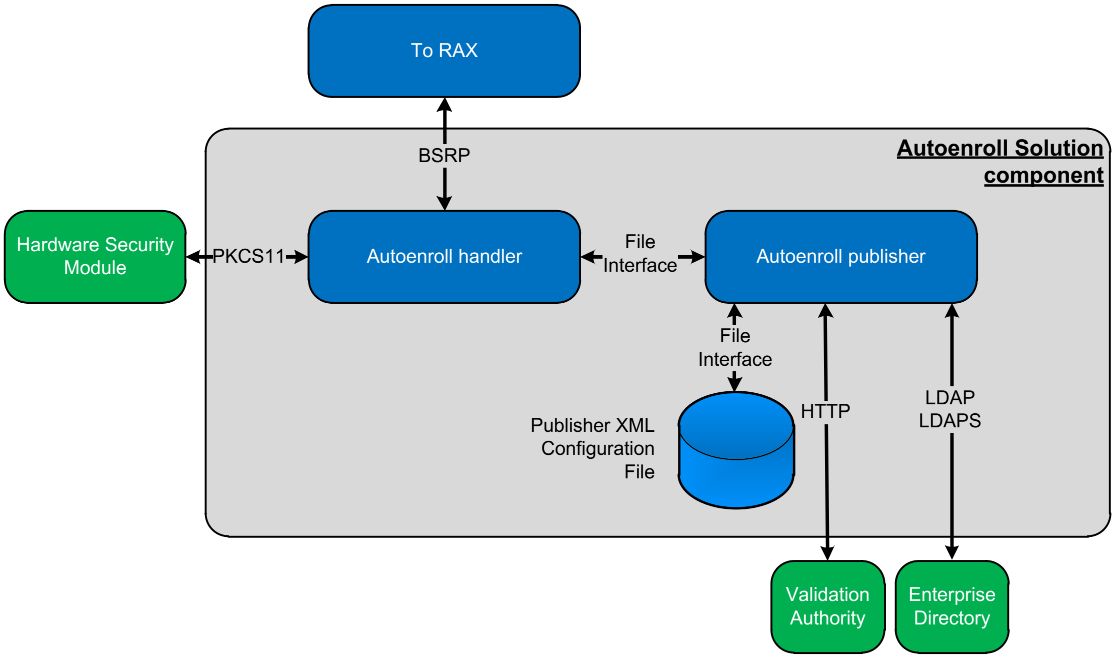

Figure 5 – Autoenroll solution component

1.6.1.5 Support utilities

The TOE implements utilities that support all the components identified in sections 1.6.1.1, 1.6.1.3 and 1.6.1.4 to reduce the likelihood of misconfiguration or errors by TOE users. The support utilities are in the scope of the evaluation. These utilities are:

- **Database Wizard**. The Database Wizard is used when first installing the TOE in order to create the required Oracle tables (i.e. schemas), and to create the necessary database user accounts. The Database Wizard is unable to modify data in the tables or the account privileges (but it can be used to change a database account’s password). The Database Wizard does not implement any of the TOE’s SFRs, and does not handle TSF data; it is provided solely to assist in the installation and setup of the TOE.

- **Database Upgrade Utility**. The Database Upgrade Utility is used where the TOE requires new or changed (Oracle) database tables (i.e. schemas) to be in place. The utility upgrades the existing schemas.

- **Key Generator**. The Key Generator utility allows a CAO user to generate keys for TOE sub-components that reside on a different platform from where the CAO is installed. The generated public key can be transferred to the CAO platform (using removable media) in order to create a certificate, which can then be transferred to the TOE sub-component's platform (again using removable media). This is required where a TOE sub-component stores its keys in PKCS#11 compliant hardware that is not accessible from the CAO platform.

- **Publisher Configuration Utility**. The Publisher Configuration utility (also referred to as the Publisher Configuration program) allows an administrator to configure the Publisher and Autoenroll Publisher components of the TOE. This allows for the publication of certificates, CRLs and ARLs to a repository (LDAP or OCSP responder) external to the TOE.

- **Token Manager**. The Token Manager allows a TOE user to manage personal secure environment files (PSEs), PKCS#12 files, and PKCS#11 tokens, used in the PKI system. It is a stand-alone utility that enables the user to view the contents of these files and tokens.

- **Service Manager**. The Service Manager utility provides an interface that allows a TOE user to start and stop those TOE sub-components that provide a TOE service. For example, the CA, CSS, RA and RA eXchange sub-components.

1.6.2 Logical scope of the TOE

The TOE consists of the UniCERT core components (and their sub-components), the "advanced" components (and their sub-components), the utilities that are identified in section 1.6.1, and the security functions as defined in this section.

1.6.2.1 Standard cryptographic methods

The TOE provides capabilities for the generation, destruction, export, splitting, and updating of cryptographic keys associated with the PKI system, TOE components, and TOE users based on standardized methods.

The TOE implements standard digital signature methods to:

- Allow the content of certificates and CRLs to be verifiable and to prevent forgery and tampering;
- Protect the integrity of data (including certificates and CRLs) when at rest and when in transit between components of the TOE;
- Protect the integrity of messages transmitted between components of the TOE (which may or may not be hosted on different platforms).

The TOE generates a digital signature for every X.509 digital certificate generated by the TOE, for CRLs, and for some messages transmitted between TOE components. Digital signatures use a hash of the data that is then encrypted using the private key of the TOE component. Other TOE components and entities external to the TOE can verify the authenticity of certificates, CRLs, and messages using the public key of the TOE components that generated the digital signature. Digital signature functions are based on published standards and include the following algorithms in a range of key lengths:

- RSA ([RSA]) and the Secure Hash Algorithm ([SHA-1] or [SHA-2]);
- DSA ([DSA]) and the Secure Hash Algorithm ([SHA-1]; and
- The Elliptic Curve Digital Signature Algorithm ([ECDSA]) and the Secure Hash Algorithm ([SHA-1] or [SHA-2]).

The TOE implements standard symmetric cryptographic methods for protecting the confidentiality of messages and data when at rest and when in transit between components of the TOE. These methods are based on the following algorithms in a range of key lengths:

- Triple-DES ([3-DES]); and
- The Advanced Encryption Standard ([AES]).

Additionally, the TOE implements asymmetric cryptographic methods, namely RSA public key cryptographic methods for protecting the confidentiality of symmetric keys whilst in transit between TOE components and for key archival.

1.6.2.2 Certificate lifecycle management

The TOE provides the capability to register entities for digital certificates through a range of methods, protocols and interfaces in accordance with operational policies defined for the TOE including:

- Email clients;
- Windows clients;
- Simple Certificate Enrol ment Protocol (SCEP), primarily used for routers and VPN devices; and
- Web browsers.

The TOE also provides an automated means for end users of a Microsoft Windows domain (both human users and server components, such as domain controllers) to request certificates via the Autoenroller and RA component of the TOE. Windows allows a user's request for a certificate to be submitted automatically when the user logs on to the domain; and when a certificate has been issued, a renewal request can be submitted automatically shortly before the certificate's expiration time (with virtually no user involvement).

The TOE provides the capability to securely generate or renew digital certificates, in accordance with defined operational policies, via Certification Authorities, for its own use and for distribution to entities that include users, applications and devices. Certificate generation binds the identity of an entity to a public key with a digital signature through the registration process.

The TOE maintains the status of digital certificates issued by the TOE, stored centrally within the Certification Authority database. Through the use of the CSS, other TOE components are able to utilize OCSP requests/responses to determine the current status of each digital certificate previously issued by the TOE. The TOE also provides the capability to suspend or revoke digital certificates where necessary, such as in response to suspected private key compromise. The TOE updates the status of certificates in its database and publishes revoked certificates on a digitally signed Certificate Revocation List (CRL) in accordance with operational policies defined for the TOE.

1.6.2.3 Integration with hardware security modules and smartcards

While the TOE provides a range of standard cryptographic methods, the TOE may also be securely integrated with dedicated HSM devices and smartcards (another form of HSM) that are PKCS#11 [PCKS#11] compliant devices. These devices can be used for the delivery of cryptographic services to the TOE and for securing of private keys related to the TOE components as required by the end user of the PKI system.

The use of HSM devices reduces the potential for the exposure of the private key associated with TOE components. Those components that can be integrated with a HSM are:

- Certification Authority;
- Certificate Status Server;
- Certification Authority Operator;
- Registration Authority;
- RA Event Viewer;
- RA eXchange;
- Protocol Handlers (including the Autoenroll Solution);

- Key Archive Server; and
- Key Archive Operator.

1.6.2.4 Key archival

The TOE provides a secure key repository and retrieval capability for end users' private encryption keys; this enables an end user to recover a key at a later date should the user's copy of the key become corrupt or lost. It also enables an organization to recover encrypted data if a key/certificate owner leaves the company unexpectedly. The Key Archive Server is under the control and management of the Key Archive Operator component of the TOE.

1.6.2.5 PKI management

The TOE provides a range of functions and utilities for secure management of the TOE and establishing the public key infrastructure implemented by the TOE as a hierarchy of Certification Authorities, Registration Authorities and other TOE components as required.

The TOE provides management functions for:

- Managing the overall PKI implemented by the TOE (creation, export, modification, protection and verification);
- Managing TOE components and TOE users (entities) within the PKI system and their certificate lifecycles (as described in section 1.6.2.2);
- Managing groups of TOE components within the PKI system under common authorization and registration paths for certificate lifecycle management functions (as described in section 1.6.2.2);
- Viewing and modifying the authorizations assigned to TOE users;
- Viewing and modifying the TOE configuration (and TOE component configurations) and registration policies;
- Querying and archiving audit records;
- Cloning the CA, CSS, KAS, RAX and RA components of the TOE for load balancing and failover; and
- Archiving and recovering private encryption keys.

To access the management functions, a TOE user with a defined role must first be identified and authenticated within the PKI system, with TOE users only able to access those PKI management functions authorized by their role. The TOE includes ease-of-use features and utilities aimed at lessening the likelihood of human users making errors that may lead to a violation of security policy. These utilities have been described previously in Section 1.6.1.5.

1.6.2.6 Secure registration

The TOE implements optional LDAP over TLS/SSL authentication of the Published and the Enterprise Directory to ensure that the Enterprise Directory only accepts authentic certificates from the TOE. The administrator of the TOE may configure the authentication to take place.

1.6.2.7 Security audit

The TOE provides automated auditing facilities that include extensive capabilities for protecting, querying, and archiving of audit records. Audit records are generated by the TOE for the following TOE sub-components:

- CA;
- CAO;
- CSS;
- RA;
- RA Event Viewer;
- RA eXchange;
- Key Archive Server; and
- Key Archive Operator.

Audit records are digitally signed when they are created (so unauthorized modifications can be detected) and written to the database associated with the component that generated the audit event. The TOE supports assignment of authorized auditor roles to TOE users for the management and review of audit logs generated by the TOE. Audit records can only be removed from the database(s) by authorized TOE users (who have been granted explicit write-access) through the archive function. The audit record archive function allows for the archival of logs in an extensible markup language (XML) format to be stored outside of the TOE. Once audit records are archived, the TOE no longer maintains control of these records and is unable to prevent their unauthorized access or modification.

1.7 TOE delivery

The TOE is delivered to the customer on a recordable compact discs (CDRs) that are delivered via mail in a tamper-evident bag with a delivery note attached to it. The tamper-evident bag is a DHL shipping bag with a unique ID. Once sealed, the bag can only be ripped to open which will ensure that the recipient will notice any attempted tampering. A tracking email is also sent by DHL to the customer. The tracking email includes information detailing the delivery and bag contents.

Upon receipt of the bag, the customer is required to check the tamper-evident bag to ensure that it has not been opened or otherwise tampered with, and to check that the ID of the tamper-evident bag (bag number) matches the information provided in both the delivery note and DHL's tracking email (sent directly to the customer) to ensure that the tamper-evident bag was not replaced with another one.

1.8 Requirements on the environment

The operational environment consists of the non-TOE hardware and software that the TOE requires in order to function. It may also include HSMs and smart cards that meet certain certification requirements.

The TOE requires the following from the environment to deliver its functions. While the TOE requires operating systems, web servers, servlet managers, web browsers and database management systems for its operations, these are not and do not form part of the TOE.

Table 2 – TOE supporting software

Type	Description
Server operating system	Microsoft Windows Server platforms, for Windows components (CAO, RA Auditor, WebRAO, Webhandler, Autoenrol) • Windows Server 2012 • Windows Server 2016 Unix platforms, for Linux components (CA, protocol handlers, Service Manager…) • CentOS v7.8 x64 (or later) • Redhat Enterprise Linux and CentOS v7.8 x64 (or later)
Client operating system	Microsoft Windows Server platforms, for Windows components (CAO, RA Auditor, WebRAO) • Windows 8.1 • Windows 10
Web servers and servlet managers	• Apache v2.4.6 (or later) with Jakarta Tomcat v9.0.5 (or later) • Internet Information System v7.0 (or later) with ServletExec v6.0 (or later); or • Internet Information System v7.5 (or later) with ServletExec v6.0 (or later); or
Browsers	• Mozilla Firefox v83.0 (or later)
Database management systems	Oracle Database 19c: • Linux server; • Linux client; • Windows client.

Type	Description
Hardware	The TOE requires the minimum hardware specifications for the OS, with the following additional storage capacities: • 5.5 GB data storage for Oracle DBMS and Oracle data; and • 1500MB data storage for TOE components.

The TOE may also be integrated with hardware security modules. These modules must be PKCS#11 compliant to integrate with the TOE and have a suitable level of security assurance in the following functions:

- Cryptographic key management (generation/destruction);
- Cryptographic operations (digital signature generation);
- Identification, authentication and access control; and
- Physical protection.

There are a number of security objectives that must be in place for the environment as described in section 4.2 to address the overall security problem defined in section 3. End users should ensure that these security objectives are satisfied.

2 Conformance claim (ASE_CCL)

2.1 Conformance claim statement

The ST and TOE claim conformance to Common Criteria v3.1 Release 5 Part 1, Common Criteria v3.1, Release 5 Part 2, and Common Criteria v3.1 Release 5 Part 3. Common Criteria v3.1 Release 5 Part 1 is fully identified in [CC Part 1], Common Criteria v3.1 Release 5 Part 2 in [CC Part 2] and Common Criteria v3.1 Release 5 Part 3 in [CC Part 3].

The ST is CC Part 2 conformant.

The ST is CC Part 3 Augmented conformant.

The ST claims conformance to the following Protection Profiles and Packages: **None**.

The ST claims package conformance to the following: Evaluation Assurance Level EAL2 Augmented with ALC_FLR.2.

2.2 Conformance claims rationale

The ST does not claim conformance to any Protection Profile. Therefore, the Conformance Claims Rationale is not applicable.

3 Security problem definition

3.1 Threats

Table 3 – List of identified threats

Threat	Statements
T.DATA_COMPROMISE	The confidentiality or integrity of user data or TSF data - which is not being transmitted in a message - is compromised. This is particularly serious if the data is a private key used by a TOE user; compromise of a private key could lead to the production of certificates that cannot be trusted, as well as compromise of other keys, or the masquerading as an authorized user by an attacker.
T.MESSAGE_COMPROMISE	The confidentiality or integrity of user data or TSF data - which is being transmitted in a message - is compromised. This is particularly serious if the data is a key which is being transmitted in a form that a (potential) attacker could intercept, interpret, and use; or if the data is such that the attacker could modify it in a manner that enables a further attack on the TOE.
T.USER_ERROR	A TOE user or a user in the TOE operational environment unintentionally performs an action or commits an error that compromises the confidentiality and/or integrity of data used by the TOE in defining the PKI system or end user certificates generated by the TOE.
T.REPUDIATE	A TOE user or a user in the TOE operational environment denies having performed an action that that compromises the confidentiality and/or integrity of data used by the TOE in defining the PKI system or end user certificates generated by the TOE.
T.AUDIT_LOSS	An attacker gains access to the TOE's audit records and then deletes or modifies audit data in order to mask an attack on the TOE.

Threat	Statements
T.UNAUTH_CHANGE	An attacker modifies the TOE, e.g. by replacing some or all of its components with flawed versions that masquerade as authentic, which compromises the integrity of the TOE, the defined PKI system and/or the end user certificates generated by the TOE.

3.2 Assumptions

The following assumptions govern the operational environment of the TOE:

Table 4 – Assumptions for the TOE environment

Assumption	Statements
A.AUTH_DATA_DISPOSAL	Authentication data and associated privileges are properly disposed of and/or removed as appropriate when no longer required within the PKI system. This includes both removal (secure deletion) of data from the PKI system, and the revocation of certificates. (For example, if CAO users leave the organization that runs the PKI system, then their certificate should be revoked and their private key securely destroyed. Similarly, if it is suspected that a private key has been compromised, then the associated certificate should be promptly suspended or revoked.)
A.AUDIT_REVIEW	Authorized auditor(s) regularly review audit records produced by the TOE, respond promptly to any indication of an attempted or actual security breach, and ensure that audit records are regularly archived to prevent audit data storage exhaustion.
A.COMPETENT_USERS	All (human) TOE users and those users managing the operational environment are competent, either by training or experience, to manage, operate and use the PKI system, and to maintain the security and privacy of the data it handles.
A.TRUSTED_USERS	All (human) TOE users and those users managing the operational environment are trusted, as far as is reasonably possible, not to abuse the PKI system facilities that they are authorized to use; in particular, they are trusted to not install or execute malicious software within the PKI system.

Assumption	Statements
A.SECURE_INSTALL	The (human) TOE users and those users managing the operational environment install, configure and maintain the PKI system securely, i.e. in accordance with all relevant guidance documentation.
A.COMMS_PROTECTION	There is adequate logical and physical protection on the communication channels used by the TOE. The protection extends to the boundary of the PKI system, and includes the use of firewall(s) to prevent unauthorized access to the PKI system via a communication channel.
A.PHYSICAL_PROTECTION	The PKI system has adequate physical protection against, in particular, unauthorized physical access by potential attackers.
A.TIME_SOURCE	There is a trusted, accurate, and reliable time source within the PKI system that may be used to timestamp TOE audit records.
A.ACCOUNTABILITY	The PKI system is configured and operated such that individual administrators or users can be held accountable for their actions.
A.ROLE_SEPARATION	The PKI system is configured and operated such that any separation of roles (as recommended in guidance documentation) is maintained.
A.HSM	Any HSM that will be integrated with the TOE is PKCS#11 compliant and the following security features are suitably assured: • Cryptographic key management (generation/destruction); • Cryptographic operations (digital signature generation); • Identification, authentication and access control; • Physical protection; and • Secure data exchange between the TOE and the HSM.

3.3 Organisational security policies

There are no organisational security policies defined for the TOE.

4 Security objectives (ASE_OBJ)

4.1 Security objectives for the TOE

Table 5 – Security objectives for the TOE

Identifier	Objective statements
O.PROTECT_DATA	The TOE shall protect the confidentiality and integrity of TSF data and/or user data that is stored under the control of the TOE.
O.PROTECT_MESSAGE	The TOE shall protect the confidentiality and integrity of TSF data and/or user data which is being transmitted in a message.
O.EVIDENCE_OF_ORIGIN	The TOE shall provide evidence of the origin of certain messages produced by the CA, RA eXchange, protocol handlers and web components of the TOE.
O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions (algorithms and parameters) for the following operations: • TLS/SSL authentication of the TOE to the Enterprise Directory; • Authentication (creating and verifying digital signatures, hashing); • Encryption and decryption; and • Key management (key generation, storage, access, and destruction).
O.PASSPHRASE	The TOE shall enforce quality standards on the passphrases used for the protection of private keys and other sensitive TSF or user data.
O.AUDIT	The TOE shall record details of security-related events in audit records, provide the means for authorized TOE users to review these records, and provide secure storage of audit records.
O.PROTECTED_CONFIG	The TOE shall protect the TSF configuration from unauthorized modification.

Identifier	Objective statements
O.PROTECTED_AUDIT	The TOE shall be capable of detecting unauthorized modification of audit records, and to preventing unauthorized deletion of audit records.

4.2 Security objectives for the environment

Table 6 – Security objectives for the environment

Identifier	Objective statements
OE.AUTH_DATA_DISPOSAL	The operational environment shall include procedures to ensure that authentication data and associated privileges are properly disposed of and/or removed as appropriate when no longer required within the PKI system.
OE.AUDIT_REVIEW	The operational environment shall include procedures to ensure that: • Audit records produced by the TOE are regularly reviewed; • Any indication of an attempted or actual security breach is responded to; and • Audit records are regularly archived to prevent audit data storage exhaustion.
OE.COMPETENT_USERS	The operational environment shall include procedures to ensure that all (human) TOE users and those users managing the operational environment are competent, either by training or experience, to manage, operate, and use the PKI system, and to maintain the security and privacy of the data it handles.
OE.TRUSTED_USERS	The operational environment shall include procedures (e.g. staff vetting and training) to ensure that all (human) TOE users and those users managing the operational environment are trusted, as far as is reasonably possible, not to abuse the PKI system facilities that they are authorized to use; in particular, they are trusted to not install or execute malicious software within the PKI system.

Identifier	Objective statements
OE.SECURE_INSTALL	The operational environment shall include procedures to ensure that (human) TOE users and those users managing the operational environment install, configure, and maintain the PKI system securely, i.e. in accordance with all relevant guidance documentation for the TOE and non-TOE hardware and software.
OE.COMMS_PROTECTION	The operational environment shall include measures and procedures to ensure that there is adequate logical and physical protection on the communication channels used by the TOE. The protection extends to the boundary of the PKI system, and includes the use of firewall(s) to prevent unauthorized access to the PKI system via a communication channel.
OE.PHYSICAL_PROTECTION	The operational environment shall include measures and procedures to ensure that the PKI system has adequate physical protection against, in particular, unauthorized physical access by potential attackers.
OE.TIME_SOURCE	The operational environment shall include a trusted, accurate and reliable time source within the PKI system (for example, a time source provided by the underlying operating system) that may be used to timestamp TOE audit records.
OE.ACCOUNTABILITY	The operational environment shall include procedures to ensure that individual administrators or users, of the environment, can be held accountable for their actions.
OE.ROLE_SEPARATION	The operational environment shall include procedures to ensure that the PKI system is configured and operated such that any separation of roles (as recommended in guidance documentation) is maintained.

Identifier	Objective statements
OE.HSM	The operational environment shall include procedures to ensure that any HSM that will be integrated with the TOE is PKCS#11 compliant and that the following security features are assured suitable for the threat environment: • Cryptographic key management (generation/destruction); • Cryptographic operations (digital signature generation); • Identification, authentication and access control; • Physical protection; and • Secure data exchange between the TOE and the HSM.

5 Security requirements (ASE_REQ)

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

5.2 SFR conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a slash "/" at the end of the component identifier and a unique name for the iteration.

5.3 Security functional requirements

5.3.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.2 and summarized in the table below.

Table 7 – List of security functional requirements

Identifier	Title
Audit	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
Communication	
FCO_NRO.2	Enforced proof of origin
Cryptographic support	
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2/publickey	Cryptographic key distribution/public key
FCS_CKM.2/otherkey	Cryptographic key distribution/other key
FCS_CKM.3	Cryptographic key access
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/asymmetric	Cryptographic operation/asymmetric

Identifier	Title
FCS_COP.1/digitalsign	Cryptographic operation/digital sign
FCS_COP.1/hash	Cryptographic operation/hash
FCS_COP.1/symmetric	Cryptographic operation/symmetric
User data protection	
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_DAU.2	Data authentication with identity of guarantor
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_ITT.1	Basic internal transfer protection
FDP_ITT.3	Integrity monitoring
FDP_RIP.1	Subset residual information protection
Identification and authentication	
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
Security management	
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes

Identifier	Title
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SAE.1	Time-limited authorisations
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
Protection of the TSF	
FPT_ITT.1/alldata	Basic internal TSF data transfer protection/alldata
FPT_ITT.1/private-secretkeys	Basic internal TSF data transfer protection/private-secretkeys
Trusted path/channels	
FTP_TRP.1	Trusted path

5.3.2 Audit (FAU)

5.3.2.1 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
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 [***not specified***] level of audit; and c) [**The auditable events specified in Annex B**].
FAU_GEN1.2	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 contents column of each table in Annex B**].
Dependencies:	FPT_STM.1 Reliable time stamps
Notes:	The operational environment (outside of the scope of the TOE) provides a trusted, accurate and reliable time stamp for use by the TOE, as defined in OE.TIME_STAMP; satisfying the FPT_STM.1 dependency.

5.3.2.2 FAU_GEN.2 User identity association

Hierarchical to:	No other components.
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.
Dependencies:	FAU_GEN.1 Audit data generation FAU_UID.1 Timing of identification
Notes:	None.

5.3.2.3 FAU_SAR.1 Audit review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [**CAO Audit Manager, CAO Auditor, RA Audit Manager, RA Auditor, KAO Audit Manager, KAO Auditor**] with the capability to read [**all audit records**] 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.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

5.3.2.4 FAU_SAR.2 Restricted audit review

Hierarchical to:	No other components.

FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
Dependencies:	FAU_SAR.1 Audit review

5.3.2.5 FAU_SAR.3 Selectable audit review

Hierarchical to:	No other components.
FAU_SAR.3.1	The TSF shall provide the ability to **perform** ~~apply~~ [**searches, sorting and ordering**] of audit data based on [**queries as defined in the CAO documentation or RA Event Viewer documentation or Key Archive Operator documentation**].
Dependencies:	FAU_SAR.1 Audit review
Notes:	None.

5.3.2.6 FAU_STG.1 Protected audit trail storage

Hierarchical to:	No other components.
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.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

5.3.3 Communication (FCO)

5.3.3.1 FCO_NRO.2 Enforced proof of origin

Hierarchical to:	FCO_NRO.1
FCO_NRO.2.1	The TSF shall enforce the generation of evidence of origin for transmitted [**a) BRSP messages from protocol handlers except the WebHandler:** **i. Registration request messages;**

	ii. **Renewal request messages;**
	iii. **Revocation request messages;**
	b) **BRSP messages from all protocol handlers:**
	i. **Authorization request messages;**
	ii. **Key recovery request messages;**
	c) **BRSP messages between the WebRAO and the RAX;**
	d) **CMP messages between:**
	i. **The CA and the RA;**
	ii. **The RA and the KAS; and**
	iii. **The CA and the KAS**] at all times.

FCO_NRO.2.2	The TSF shall be able to relate the [**digital signature**] of the originator of the information, and [**the entire transmitted message**] ~~of the information~~ to which the evidence applies.
FCO_NRO.2.3	The TSF shall provide a capability to verify the evidence of origin of information to [***originator, recipient and all other users***] given [**the PKI system's Operational Policy, the originator's public key certificate and access to the certificate's status**].
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.3.4 Cryptographic support (FCS)

5.3.4.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**AES, 3DES, DSA, RSA, ECDSA**] and specified cryptographic key sizes [a) **128, 192 bit or 256 bit (AES),** b) **168 bit (3DES),**

	c) 1024 bit (DSA), **d) 1024, 1536, 2048, 3072, 4096 or 8192 bit (RSA),** **e) between 160 and 571 bits over F_p and F_{2m} (ECDSA)**] that meet the following: [**[AES], [3DES], [DSA], [RSA], and [ECDSA] and [SEC2]**].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.3.4.2 FCS_CKM.2 Cryptographic distribution/publickey

Hierarchical to:	No other components.
FCS_CKM.2.1/publickey	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**a. X.509 public key certificate in PEM format,** **b. X.509 public key certificate in DER format,** **c. X.509 public key certificate in PKCS#7 format,** **d. PKCS#10 certificate request**] that meets the following: [**[PEM], [DER], [PKCS#7], [PKCS#10]**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.3.4.3 FCS_CKM.2 Cryptographic distribution/otherkey

Hierarchical to:	No other components.

FCS_CKM.2.1/otherkey	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**PKCS#11, PKCS#12, PSE (Verizon proprietary)**] that meets the following: [**[PKCS#11], [PKCS#12], [PSE]**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.3.4.4 FCS_CKM.3 Cryptographic key access

Hierarchical to:	No other components.
FCS_CKM.3.1	The TSF shall perform [**cryptographic key archival and cryptographic key recovery]** in accordance with a specified cryptographic key access method [**encryption using LTSK**] that meets the following: [**none**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.3.4.5 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**memory overwrite**] that meets the following: [**none**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

Notes:	None.

5.3.4.6 FCS_COP.1 Cryptographic operation/asymmetric

Hierarchical to:	No other components.
FCS_COP.1.1/asymmetric	The TSF shall perform [**asymmetric encryption and decryption**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**1024, 1536, 2048, 3072, 4096 or 8192 bit**] that meet the following: [**[RSA]**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None

5.3.4.7 FCS_COP.1 Cryptographic operation/digitalsign

Hierarchical to:	No other components.
FCS_COP.1.1/digitalsign	The TSF shall perform [**digital signature creation and verification**] in accordance with a specified cryptographic algorithm [**a) RSA and SHA-2,** **b) RSA and SHA-1,** **c) DSA and SHA-1,** **d) ECDSA and SHA-2,** **e) ECDSA and SHA-1**] and cryptographic key sizes [**a) RSA 1024, 1536, 2048, 3072, 4096 or 8192 bit and SHA-2 224, 256, 384 or 512 bit,** **b) RSA 1024, 1536, 2048, 3072, 4096 or 8192 bit and SHA-1 160 bit,** **c) DSA 1024 bit and SHA-1 160 bit,**

	d) ECDSA using curves between 160 and 571 bits over F_p and F_{2m} and SHA-2 224, 256, 384 or 512 bit, **e) ECDSA using curves between 160 and 571 bits over F_p and F_{2m} and SHA-1 160 bit**] that meet the following: [**[RSA] and [SHA-2], [RSA] and [SHA-1], [DSA] and [SHA-1], [ECDSA] and [SEC2] and [SHA-2], [ECDSA] and [SEC2] and [SHA-1]**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	The primary purpose of the TOE is to enable the establishment and management of a public key infrastructure. Digital signature cryptography is a critical component of the PKI systems that are established by the TOE providing the basis for trust in the management of digital certificates.

5.3.4.8 FCS_COP.1 Cryptographic operation/hash

Hierarchical to:	No other components.
FCS_COP.1.1/hash	The TSF shall perform [**secure hashing**] in accordance with a specified cryptographic algorithm [**SHA-2, SHA-1**] and cryptographic key sizes [**none**] that meet the following: [**[SHA-2], [SHA-1]**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None

5.3.4.9 FCS_COP.1 Cryptographic operation/symmetric

Hierarchical to:	No other components.

FCS_COP.1.1/symmetric	The TSF shall perform [**symmetric encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES, 3DES**] and cryptographic key sizes [**a) 128, 192 or 256 bit (AES),** **b) 168 bit (3DES)**] that meet the following: [**[AES], [3DES]**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None

5.3.5 User data protection (FDP)

5.3.5.1 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**PKI access SFP**] on [**the subjects, object and operations referenced in Annex C**].
Dependencies:	FDP_ACF.1 Security attribute based access control
Notes:	None.

5.3.5.2 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**PKI access SFP**] to objects based on the following: [**a. subjects as defined as a role referenced in Table 20 and Table 21 of Annex C with the following attributes:** **i. Assigned Permissions** **ii. Private key and associated passphrase to access the key** **iii. X.509 Certificate** **b. Objects and their associated attributes as referenced in Table 22 of Annex C**].
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**An operation by a subject on an object is allowed to take place only if:** • **The action is valid for the object; and** • **The subject possesses the required permission for the action as an Assigned Permission.**]
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**].

Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialization
Notes:	The Web Handler (subject) submits un-authenticated requests into the PKI system. This subject has no need for a private key or certificate and hence these attributes are not relevant for this subject. The means of I&A at any given time is linked to whatever role is being adopted for that time. The rule FDP_ACF.1.2 of the access control SFP does not apply to subjects that act on behalf of the TSF itself, e.g. the CA (server), because such subjects are trusted (to an EAL2+ level of assurance) to function in accordance with the TOE's overall SFP (i.e. to have been specified, designed and implemented correctly).

5.3.5.3 FDP_DAU.2 Data authentication with identity of guarantor

Hierarchical to:	FDP_DAU.1
FDP_DAU.2.1	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [**each certificate and CRL generated by the TSF**].
FDP_DAU.2.2	The TSF shall provide [**any subject**] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated that evidence.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None

5.3.5.4 FDP_IFC.1 Subset information flow control

Hierarchical to:	No other components.
FDP_IFC.1.1	The TSF shall enforce the [**PKI messaging SFP**] on [**a) Subjects** **i. Subjects as referenced in Table 21 of Annex C** **b) Information** **i. Messages containing user data as referenced in Table 23, Annex C**

	c) Operations **i. Operations as referenced in Table 22**].
Dependencies:	FDP_IFF.1 Simple security attributes
Notes:	None.

5.3.5.5 FDP_IFF.1 Simple security attributes

Hierarchical to:	No other components.
FDP_IFF.1.1	The TSF shall enforce the [**PKI messaging SFP**] based on the following types of subject and information security attributes: [**a) Subjects as referenced in Table 21 of Annex C** **b) Messages (Information) as referenced in Table 23 of Annex C].**
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**all traffic between authenticated components of the TOE is allowed.**].
FDP_IFF.1.3	The TSF shall enforce the [**message authenticity for all information and confidentiality for private and secret keys transmitted between components of the TOE**].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [**none**].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [**none**].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
Notes:	None.

5.3.5.6 FDP_ITT.1 Basic internal transfer protection

Hierarchical to:	No other components.

FDP_ITT.1.1	The TSF shall enforce the [**PKI messaging SFP**] to prevent the [***modification***] of user data when it is transmitted between physically-separated parts of the TOE.
Dependencies:	FDP_ACC.1 Subset access control FDP_IFC.1 Subset information flow control.
Notes:	Providing reliable (i.e. available) communication channels is a function of the operating environment.

5.3.5.7 FDP_ITT.3 Integrity monitoring

Hierarchical to:	No other components.
FDP_ITT.3.1	The TSF shall enforce the [**PKI messaging SFP**] to monitor user data transmitted between physically-separated parts of the TOE for the following errors: [**unverified signature for a message containing user data that has been signed**].
FDP_ITT.3.2	Upon detection of a data integrity error, the TSF shall [**logically disconnect the TOE sub-component that transmitted the user data**].
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FDP_ITT.1 Basic internal transfer protection
Notes:	None

5.3.5.8 FDP_RIP.1 Subset residual information protection

Hierarchical to:	No other components.
FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***deallocation of the resource from***] the following objects: [**a) private key material held in memory when a software cryptographic operation (e.g., sign/encrypt) has occurred;** **b) passphrase used to open PSE/P12 files or P11 devices**].
Dependencies:	None

Notes:	Prior to deallocation, the resource (memory location) is overwritten with a hexadecimal value of 0xFF per byte.

5.3.6 Identification and authentication (FIA)

5.3.6.1 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**Role, Assigned Permissions (as defined in Table 21 of Annex C), Private key and associated passphrase to access the key, Entity type certificate extension, X.509 Certificate**].
Dependencies:	None.
Notes:	None.

5.3.6.2 FIA_SOS.1 Verification of secrets

Hierarchical to:	None
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [• **All passphrases must contain a minimum of eight characters.** • **Passphrases can contain non-ASCII (including foreign language) characters.** • **Passphrases consisting of all ASCII characters must contain at least one lowercase letter, one uppercase letter, one numerical digit, and one punctuation mark.**].
Dependencies:	None
Notes:	FIA_SOS.1 applies to the CAO when exporting PKCS#12 formatted files.

5.3.6.3 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	A user who has the ability to load the CAO or KAO may configure logging options for the CAO or KAO (respectively) prior to authentication. Enabling this logging allows for the specification of a text file to log debugging (non-security related) information. The configuration of this logging does not however take effect until a CAO or KAO authenticates to the TOE.

5.3.6.4 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	None
Notes:	A user who has the ability to load the CAO or KAO may configure logging options for the CAO or KAO (respectively) prior to identification. Enabling this logging allows for the specification of a text file to log debugging (non-security related) information. The configuration of this logging does not however take effect until a CAO or KAO authenticates to the TOE.

5.3.6.5 FIA_USB.1 User-subject binding

Hierarchical to:	None
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on behalf of that user: [**Role, Assigned Permissions (as defined in Table 21 of Annex C), Entity type certificate extension, X.509 Certificate**].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on behalf of users: [**none**].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on behalf of users: [**none**].

Dependencies:	FIA_ATD.1 User attribute definition
Notes:	None.

5.3.7 Security management (FMT)

5.3.7.1 FMT_MOF.1 Management of security functions behaviour

Hierarchical to:	None
FMT_MOF.1.1	The TSF shall restrict the ability to [***determine the behaviour of, disable, enable, modify the behaviour of***] the functions [• **CA audit functions;** • **RA audit functions;** • **KAS Audit functions;** • **Cloning the PKI configuration established by the TOE;** • **Managing the overall PKI implemented by the TOE (creation, export, modification, protection and verification);** • **Managing TOE components and TOE users (entities) within the PKI system and their certificate lifecycles;** • **Managing groups of TOE components within the PKI system under common authorisation and registration paths for certificate lifecycle management functions; and** • **HSM integration]** **to [respectively:** • **CAO Audit Manager;** • **RA Audit Manager;** • **KAO Audit Manager (see Table 20, Annex C); and** • **CAO User; KAO User and WebRAO User (RAO, KRO and RRO User) with appropriate permissions**].
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles.

Notes:	The management of HSM integration is limited to the selection of the cryptographic profile or PKCS#11 interface by the relevant user role via their respective interface. No other management functions regarding HSM integration are controlled by the TOE.

5.3.7.2 FMT_MSA.1 Management of security attributes

Hierarchical to:	None
FMT_MSA.1.1	The TSF shall enforce the [**PKI access SFP**] to restrict the ability to [***query, modify, delete***] the security attributes [**Viewing and modifying the authorisations assigned to TOE users (including Role, Possible Permissions, Assigned Permissions, X.509 Certificate)**] to [**a CAO User with any necessary permissions**].
Dependencies:	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles
Notes:	Revoking a certificate which is used for I&A purposes is equivalent to modifying a security attribute.

5.3.7.3 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	None
FMT_MSA.3.1	The TSF shall enforce the [**PKI access SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**a CAO User with any necessary permissions**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles.
Notes:	None.

5.3.7.4 FMT_MTD.1 Management of TSF data

Hierarchical to:	None
FMT_MTD.1.1	The TSF shall restrict the ability to [***change default, query, modify, delete, clear***] the [**Viewing and modifying the TOE configuration (and TOE component configurations) and registration policies (including:** - **operational policy, registration policy, certificates, private keys, PSE or P12 files (see Table 23 of Annex C)** - **CA audit records;** - **RA audit records; and** - **KAS Audit records)**] to [respectively: - **CAO User with any necessary permissions (except for audit records);** - **CAO Audit Manager (for CA audit records);** - **RA Audit Manager (for RA audit records); and** - **KAO Audit Manager (for KAS audit records)**].
Dependencies:	FMT_SMF.1 Specification of management functions FMT_SMR.1 Security roles.
Notes:	Roles are listed in Table 20 of Annex B. Audit Managers cannot modify, delete or clear audit records (see FAU_STG.1). Audit Managers may archive audit records (see FMT_SMF.1.1) to a location outside of the TOE's control (removing the audit records from the control of the TOE).

5.3.7.5 FMT_SAE.1 Time-limited authorisation

Hierarchical to:	None
FMT_SAE.1.1	The TSF shall restrict the capability to specify an expiration time for [**certificate validity**] to [**a CAO User or a WebRAO user (with any necessary permissions)**].
FMT_SAE.1.2	For each of these security attributes, the TSF shall be able to [**disallow the use of the relevant certificate**] after the expiration time for the indicated security attribute has passed.

Dependencies:	FMT_SMR.1 Security roles FPT_STM.1 Reliable time stamps.
Notes:	“Specify an expiration time” here means specify a certificate’s expiration time in a request message; “action immediate revocation” means the certificate’s status attribute is immediately changed to a value that represents “this certificate has expired”. (Note that immediate revocation of a certificate can also be achieved by a CAO user or a WebRAO user via an approved Certificate Revocation Request message; see also the FMT_MSA.1 application note.) The operational environment (outside of the scope of the TOE) provides a trusted, accurate and reliable time stamp for use by the TOE, as defined in OE.TIME_STAMP; satisfying the FPT_STM.1 dependency.

5.3.7.6 FMT_SMF.1 Specification of management functions

Hierarchical to:	None
FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: [• **Managing the overall PKI implemented by the TOE (creation, export, modification, protection and verification);** • **Configuring the TLS/SSL authentication of the TOE to the Enterprise Server;** • **Managing TOE components and TOE users (entities) within the PKI system and their certificate lifecycles;** • **Managing groups of TOE components within the PKI system under common authorisation and registration paths for certificate lifecycle management functions;** • **Viewing and modifying the authorisations assigned to TOE users;** • **Viewing and modifying the TOE configuration (and TOE component configurations) and registration policies;** • **Querying and archiving audit records;** • **Cloning the RAX, CA, CSS, KAS and RA components for load balancing and recovery;**

	- **Archiving and recovering private encryption keys; and** - **Manage HSM integration].**
Dependencies:	None
Notes:	Once an audit record has been archived it is removed from the control of the TOE.

5.3.7.7 FMT_SMR.1 Security roles

Hierarchical to:	None
FMT_SMR.1.1	The TSF shall maintain the roles: [**as listed in Table 20 of Annex C**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1
Notes:	The archive audit records management function includes the capability to delete an audit record if, and only if, it has been archived.

5.3.8 Protection of the TSF (FPT)

5.3.8.1 FPT_ITT.1 Basic internal TSF data protection/alldata

Hierarchical to:	None
FPT_ITT.1.1/alldata	The TSF shall protect TSF data from [***modification***] when it is transmitted between separate parts of the TOE.
Dependencies:	None
Notes:	None

5.3.8.2 FPT_ITT.1 Basic internal TSF data protection/private-secretkeys

Hierarchical to:	None
FPT_ITT.1.1/private-secretkeys	The TSF shall protect **private keys and symmetric keys** ~~TSF data~~ from [***disclosure***] when it is transmitted between separate parts of the TOE.
Dependencies:	None

Notes:	While all TSF data transfers are protected from modification, private keys and symmetric keys are also protected from disclosure during transmission between separate parts of the TOE.

5.3.9 Trusted path/channels (FTP)

5.3.9.1 FTP_TRP.1 Trusted path

Hierarchical to:	None
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [**remote**] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [[***masquerading as a TOE***]].
FTP_TRP.1.2	The TSF shall permit [**the TSF**] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [[***TLS/SSL authentication of LDAP connection***]].
Dependencies:	None
Notes:	None

5.4 Security assurance requirements

Table 8 – List of security assurance requirements

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.2 Use of a CM System

Assurance class	Assurance components
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6 TOE summary specification (ASE_TSS)

6.1 Overview

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

The primary function of a PKI system is to issue and manage digital certificates that allow other IT systems to verify the identity of the holder. The following table demonstrates how the TOE meets the specified SFRs.

Table 9 – Satisfaction of TOE SFRs

Identifier	Description of how SFR is met by the TOE.
Audit	
FAU_GEN.1	The TOE provides automated auditing facilities that include extensive capabilities for protecting, querying and archiving of audit records. Audit records are generated by the TOE for the following TOE sub-components: • CA; • CAO; • RA; • RA Event Viewer; • RA eXchange; • Key Archive Server; and • Key Archive Operator. A complete listing of audit events generated by the TOE is provided at Annex B. The TOE records the following information in each audit record: • Date and time of the event;

Identifier	Description of how SFR is met by the TOE.
	• type of event; • subject identity (if applicable); • the outcome (success or failure) of the event; and • the information specified in the contents column of each table in Annex B.
FAU_GEN.2	The TOE stores the username that caused the event in the audit log.
FAU_SAR.1	The TOE provides an interface for users with appropriate permissions to read and understand audit records.
FAU_SAR.2	The TOE supports assignment of authorised auditor roles to TOE users for the management and review of audit logs generated by the TOE.
FAU_SAR.3	The TOE provides the ability to search, sort and filter the audit records based on various log attributes.
FAU_STG.1	Audit records are digitally signed when they are created (so unauthorized modifications or deletion of the audit records can be detected) and written to the database associated with the component that generated the audit event.
Communication	
FCO_NRO.2	The TOE requires that all BRSP messages from protocol handlers and between the WebRAO and the RAX are validly signed before they are accepted. The only exceptions are the following messages received from the web handler: i. Registration request messages; ii. Renewal request messages; and iii. Revocation request messages. The TOE also required that all CMP messages between the CA and the RA, the RA and the KAS and the CA and the KAS are validly signed before they are accepted.

Identifier	Description of how SFR is met by the TOE.
Cryptographic support	
FCS_CKM.1	The TOE provides a cryptographic library to generate the following keys: a) 128, 192 or 256 bit (AES), b) 168 bit (3DES), c) 1024 bit (DSA), d) 1024, 1536, 2048, 3072, 4096 or 8192 bit (RSA), e) between 160 and 571 bits over F_p and F_{2m} (ECDSA)
FCS_CKM.2/publickey	The TOE distributes cryptographic public keys in the following formats: a. X.509 public key certificate in PEM format, b. X.509 public key certificate in DER format, c. X.509 public key certificate in PKCS#7 format, d. PKCS#10 certificate request
FCS_CKM.2/otherkey	The TOE distributes cryptographic keys in the following formats: a. PKCS#11, b. PKCS#12, c. PSE (Verizon proprietary)
FCS_CKM.3	The TOE provides a secure key archival and retrieval capability for end users' private encryption keys; this enables an end user to recover a key at a later date should the user's copy of the key become corrupt or lost. It also enables an organization to recover encrypted data if a key/certificate owner leaves the company unexpectedly. The TOE provides key archival and key recovery functions through the encryption of the private encryption key with a random symmetric key. This symmetric key is subsequently encrypted by the LTSK's public key prior to storage. The Key Archive Server is under the control and management of the Key Archive Operator component of the TOE.
FCS_CKM.4	The TOE ensures that keys are overwritten before a resource is deallocated from a key object.

Identifier	Description of how SFR is met by the TOE.
FCS_COP.1/asymmetric	The TOE performs asymmetric encryption and decryption using the following algorithm: a) RSA.
FCS_COP.1/digitalsign	The TOE can generate digital signatures using the following algorithms: a) RSA and SHA-2, b) RSA and SHA-1, c) DSA and SHA-1, d) ECDSA and SHA-2, e) ECDSA and SHA-1.
FCS_COP.1/hash	The TOE can generate hashes using the following algorithms: a) SHA-2, b) SHA-1.
FCS_COP.1/symmetric	The TOE performs symmetric encryption using the following algorithms: a) AES, b) 3DES.
User data protection	
FDP_ACC.1	The TOE implements the “PKI access SFP” on all items referenced in Annex C.
FDP_ACF.1	The TOE enforces the “PKI access SFP” to ensure that only those TOE users that are authorized and have appropriate permissions are able to access objects controlled by the TOE. In particular the TOE provides control over access to and the use of the TOE’s private keys.
FDP_DAU.2	The TOE provides the capability to register entities for digital certificates through a range of methods, protocols and interfaces in accordance with operational policies defined for the TOE including: • Email clients; • Windows clients;

Identifier	Description of how SFR is met by the TOE.
	• Simple Certificate Enrolment Protocol (SCEP) primarily used for routers and VPN devices; and • Web browsers. The TOE also provides an automated means for end users of a Microsoft Windows domain (both human users and server components, such as domain controllers) to request certificates from the CA component of the TOE. A user's request for a certificate can be submitted automatically when the user logs on to the domain; and when a certificate has been issued, a renewal request can be submitted to the CA shortly before the certificate's expiration time (with virtually no user involvement). The TOE provides the capability to securely generate or renew digital certificates, in accordance with operational policies defined for the TOE, via Certification Authorities, for its own use and for distribution to entities that include users, applications and devices. Certificate generation binds the identity of an entity to a public key with a digital signature. The TOE generates a digital signature for every X.509 digital certificate generated by the TOE, for CRLs and for messages transmitted between TOE components. Digital signatures use a hash of the data that is then encrypted using the private key of the TOE component. Other TOE components and entities external to the TOE can verify the authenticity of certificates, CRLs and messages using the public key of the TOE components that generated the digital signature. The TOE maintains the status of digital certificates issued by the TOE with certificates published to a Certification Authority database. The TOE allows entities to query the status of digital certificates using the OCSP ([OCSP]). The TOE also provides the capability to suspend or revoke digital certificates where necessary, such as in response to suspected private key compromise. The TOE updates the status of certificates in its database and publishes revoked certificates on a digitally signed Certificate Revocation List (CRL) in accordance with operational policies defined for the TOE.

Identifier	Description of how SFR is met by the TOE.
FDP_IFC.1	The TOE implements the "PKI messaging SFP" using the subjects, information and operations defined in Table 21, Table 22 and Table 23 of Annex C respectively.
FDP_IFF.1	The TOE implements the "PKI messaging SFP" by signing traffic transmitted between TOE components, and additionally encrypting this traffic when it contains private or secret key, as well as controlling the flow of information using the message checks defined in Table 23 of Annex C.
FDP_ITT.1	The TOE ensures that information sent between TOE components is protected from modification by signing the data and checking the signature on all information received by TOE components.
FDP_ITT.3	The TOE ensures that modified information is not accepted by the TOE. Additionally, the TOE will not accept any packets from a TOE component that is responsible for a packet that cannot be verified until a TOE user with appropriate permissions re-connects the component.
FDP_RIP.1	The TOE ensures that all resources that handle private keys and passwords are overwritten before deallocation.
Identification and authentication	
FIA_ATD.1	The TOE maintains the following attributes for all TOE users: • Role, • Assigned Permissions, • Private key and associated passphrase to access the key, • X.509 Certificate.
FIA_SOS.1	The TOE checks that all new passwords inputted by the CAO meet the following requirements: • All passphrases must contain a minimum of eight characters. • Passphrases can contain non-ASCII (including foreign language) characters. • Passphrases consisting of all ASCII characters must contain at least one lowercase letter, one uppercase

Identifier	Description of how SFR is met by the TOE.
	• letter, one numerical digit, and one punctuation mark.
FIA_UAU.2	Users are required to authenticate themselves, using messages signed with the TOE user's private key, before the TOE will perform any actions.
FIA_UID.2	Users are required to identify themselves, before the TOE will perform any actions.
FIA_USB.1	The TOE maintains the following attributes for subjects that are linked to human users: • Role, • Assigned Permissions, • X.509 Certificate
Security management	
FMT_MOF.1	Using permissions associated to the user account, the TOE restricts access to the following TOE management functions: • Cloning the PKI system established by the TOE; • Managing the overall PKI implemented by the TOE (creation, export, modification, protection and verification); • Managing TOE components and TOE users (entities) within the PKI system and their certificate lifecycles; • Managing groups of TOE components within the PKI system under common authorization and registration paths for certificate lifecycle management functions; and • HSM integration
FMT_MSA.1	Using permissions associated to the user account, the TOE restricts access to the authorizations assigned to TOE users (including: • Role, • Possible Permissions, • Assigned Permissions, • Private key and associated passphrase to access the key,

Identifier	Description of how SFR is met by the TOE.
	• X.509 Certificate).
FMT_MSA.3	The TOE provides all "possible permissions" as assigned permissions when a role is added to a new user.
FMT_MTD.1	Using permissions associated to the user account, the TOE restricts access to TOE configuration (and TOE component configurations) and registration policies (including: • operational policy, registration policy, announce messages, certificates, private keys, PSE or P12 files, message (request/response) where message checks are required (see Table 23) • CA audit records; • RA audit records; and • KAS Audit records).
FMT_SAE.1	The TOE limits the validity of all certificates issued as configured by a CAO or WebRAO user.
FMT_SMF.1	The TOE provides a range of functions and utilities for secure management of the TOE and establishing the public key infrastructure implemented by the TOE as a hierarchy of Certification Authorities, Registration Authorities and other TOE components as required. The TOE provides the following TOE management functions: • Managing the overall PKI implemented by the TOE (creation, export, modification, protection and verification); • Configuring the TLS/SSL authentication of the TOE to the Enterprise Service; • Managing TOE components and TOE users (entities) within the PKI system and their certificate lifecycles (as described in section 1.6.2.2);

Identifier	Description of how SFR is met by the TOE.
	• Managing groups of TOE components within the PKI system under common authorization and registration paths for certificate lifecycle management functions; • Viewing and modifying the authorizations assigned to TOE users; • Viewing and modifying the TOE configuration (and TOE component configurations) and registration policies; • Querying and archiving audit records; • Cloning the PKI system established by the TOE; and • Archiving and recovering private encryption keys.
FMT_SMR.1	The TOE provides the following TOE security roles: • CAO User, • Web RAO User, • CAO Audit Manager, • RA Audit Manager, • KAO Audit Manager
Protection of the TSF	
FPT_ITT.1/alldata	The TOE ensures that all data is protected from modification, by signing, when it is transmitted between components of the TOE.
FPT_ITT.1/private-secretkeys	The TOE ensures that private and secret keys are protected from disclosure, by encryption, when they are transmitted between components of the TOE.
Trusted path/channels	
FTP_TRP.1	The allows Administrator to configure LDAP communication between the TOE and the Enterprise Server to require TLS/SSL authentication. When so configured, the TOE shall establish require authentication to take place prior to communicating with the Enterprise Server to ensure that the Enterprise Server only accepts certificates from a legitimate TOE.

7 Rationale

7.1 Security objectives rationale

Security objectives rationale is provided to demonstrate that the threats are countered, and the assumptions are met.

7.1.1 Threat/OSP rationale

Below provides a mapping of the TOE Security objectives, threats and a justification for the mapping

Table 10 – Threat rationale

Threat/OSP	Objective	Justification
T.DATA_COMPROMISE	O.PROTECT_DATA O.PASSPHRASE O.CRYPTOGRAPHY O.PROTECTED_CONFIG OE.SECURE_INSTALL OE.PHYSICAL_PROTECTION OE.HSM	O.PROTECT_DATA requires that the TOE protect all data within the TOE scope of control. OE.HSM requires that any HSM utilised by the TOE protects all data and operations performed. This objective is supported by O.PASSPHRASE, O.CRYPTOGRAPHY, and O.PROTECTED_CONFIG, which ensure that the objective cannot be undermined by weak controls on passwords, cryptography or TOE configuration. OE.SECURE_INSTALL, and OE.PHYSICAL_PROTECTION provide additional environmental protection.
T.MESSAGE_COMPROMISE	O.PROTECT_MESSAGE O.EVIDENCE_OF_ORIGIN O.PROTECT_DATA O.PASSPHRASE O.CRYPTOGRAPHY	O.PROTECT_MESSAGE requires that the TOE ensure that messages are protected when they are being transmitted. This objective is primarily supported by O.EVIDENCE_OF_ORIGIN which

Threat/OSP	Objective	Justification
	O.PROTECTED_CONFIG OE.COMMS_PROTECTION OE.SECURE_INSTALL OE.PHYSICAL_PROTECTION	ensures that the TOE and relying systems can trust the identity of the sender. O.PROTECT_DATA provides additional support by ensuring that data is maintained with integrity. O.PASSPHRASE, O.CRYPTOGRAPHY, O.PROTECTED_CONFIG provide additional support by ensuring that the objective cannot be undermined by weak controls on passwords, cryptography or TOE configuration. OE.COMMS_PROTECTION, OE.SECURE_INSTALL and OE.PHYSICAL_PROTECTION, provide additional environmental protection.
T.USER_ERROR	O.AUDIT O.PROTECTED_AUDIT O.PROTECTED_CONFIG OE.COMPETENT_USERS OE.TRUSTED_USERS OE.ACCOUNTABILITY OE.ROLE_SEPARATION OE.AUTH_DATA_DISPOSAL OE.HSM OE.AUDIT_REVIEW OE.TIME_SOURCE	OE.COMPETENT_USERS and OE.TRUSTED_USERS directly counter the threat by ensuring that users are aware of the consequences of their actions. The other objectives diminish the threat, either by making it more difficult for a user to breach the SFP (e.g. O.PROTECTED_CONFIG, OE.ROLE_SEPARATION, OE.AUTH_DATA_DISPOSAL, OE.HSM). The remaining objectives reduce the time to resolve any issues, by providing a detailed log of actions.
T.REPUDIATE	O.AUDIT O.PROTECTED_AUDIT	The objectives O.AUDIT, O.PROTECTED_AUDIT, O.PASSPHRASE provide protected audit logs and

Threat/OSP	Objective	Justification
	O.PASSPHRASE	confidence in user identity for all significant TOE actions.
T.AUDIT_LOSS	O.PROTECTED_AUDIT O.PROTECT_DATA O.CRYPTOGRAPHY O.PASSPHRASE OE.ROLE_SEPARATION	O.PROTECT_DATA, O.PASSPHRASE and OE.ROLE_SEPARATION provides protected audit trail that ensures that only authorized and authenticated TOE users can review and manage the audit log. O.PROTECTED_AUDIT provides the capability to detect and alert upon the unauthorized modification the audit log. O.CRYPTOGRAPHY supports this objective through the provision of digital signing and signature verification operations.
T.UNAUTH_CHANGE	O.PROTECTED_CONFIG O.AUDIT OE.PHYSICAL_PROTECTION OE.COMPETENT_USERS OE.TRUSTED_USERS OE.SECURE_INSTALL	O.PROTECTED_CONFIG, and OE.PHYSICAL_PROTECTION counter this threat by protecting the TOE both physically and logically. OE.COMPETENT_USERS, OE.TRUSTED_USERS and OE.SECURE_INSTALL also support the above objectives by ensuring that users are aware of their actions and the ramifications of setting insecure configurations. O.AUDIT provides the generation of audit records in the event that a TOE component is modified in an unauthorized manner.

7.1.2 Assumption rationale

Below provides a mapping of the Security objectives for the environment of the TOE to relevant assumptions, as well as a justification for the mapping.

Assumptions	Objective	Justification
A.AUTH_DATA_DISPOSAL	OE.AUTH_DATA_DISPOSAL	This objective directly upholds the assumption.
A.AUDIT_REVIEW	OE.AUDIT_REVIEW	This objective directly upholds the assumption.
A.COMPETENT_USERS	OE.COMPETENT_USERS	This objective directly upholds the assumption.
A.TRUSTED_USERS	OE.TRUSTED_USERS	This objective directly upholds the assumption.
A.SECURE_INSTALL	OE.SECURE_INSTALL	This objective directly upholds the assumption.
A.COMMS_PROTECTION	OE.COMMS_PROTECTION	This objective directly upholds the assumption.
A.PHYSICAL_PROTECTION	OE.PHYSICAL_PROTECTION	This objective directly upholds the assumption.
A.TIME_SOURCE	OE.TIME_SOURCE	This objective directly upholds the assumption.
A.ACCOUNTABILITY	OE.ACCOUNTABILITY	This objective directly upholds the assumption.
A.ROLE_SEPARATION	OE.ROLE_SEPARATION	This objective directly upholds the assumption.
A.HSM	OE.HSM	This objective directly upholds the assumption.

7.2 Security requirements rationale

7.2.1 Tracing of SFRs to security objectives

Below provides the mapping of the TOE SFRs and the security objectives for the TOE.

Table 11 – SFRs to security objectives mapping

Objective	SFR and Demonstration
O.PROTECT_DATA	FDP_ACC.1 and FDP_ACF.1 specify an access control policy which requires the confidentiality and integrity of TSF data “at rest” to be protected. FCS_COP.1* supports the confidentiality and integrity of TSF data stored through the provisioning of hashing, signing and encryption operations to protect this data. FIA_* supports the access control policy by requiring that all TOE users are successfully identified and authenticated before any other TSF-mediated action on their behalf is permitted. FTP_TRP.1 further requires that the TOE is authenticated to the Enterprise Server using TLS/SSL prior to a connection is being established between itself and the Enterprise Server. FDP_RIP.1 requires that all resources that handle private keys and passwords are overwritten before deallocation.
O.PROTECT_MESSAGE	FDP_IFC.1 and FDP_IFF.1, supported by FDP_ITT.1, FDP_ITT.3 and FPT_*, specify an information flow control policy which requires the confidentiality and integrity of TSF data and user data to be protected. FCS_COP.1* supports message authenticity and private/secret key confidentiality through cryptographic hashing, signing and encryption operations. FIA_* supports the information flow control policy by requiring that all TOE users are successfully identified and authenticated before any other TSF-mediated action on their behalf is permitted. FDP_RIP.1 requires that all resources that handle private keys and passwords are overwritten before deallocation.
O.EVIDENCE_OF_ORIGIN	FCO_NRO.2 requires the use of digital signatures to provide evidence of origin for selected message between the CA and the RA, the CA and the KAS, and the RA and the KAS, from protocol handlers; and between the WebRAO and RAX. FDP_DAU.2, supported by FIA_*, also directly implement the objective by requiring identity authentication for certificates and CRLs produced by the CA.

Objective	SFR and Demonstration
O.CRYPTOGRAPHY	The chosen FCS class of SFRs directly implement the objective. Encryption and decryption, authentication via signatures and hashing are required by FCS_COP.1.1. Key generation is required by FCS_CKM.1, key access and storage by FCS_CKM.3, and key destruction by FCS_CKM.4. FDP_RIP.1 requires that all resources that handle private keys and passwords are overwritten before deallocation. The TOE also implements TLS/SSL authentication to allow itself to be authenticated to the Enterprise Services (FTP_TRP.1).
O.PASSPHRASE	FIA_SOS.1 requires minimum password complexity for passphrases.
O.AUDIT	FAU_GEN.1 and FAU_GEN.2 directly implement part of the objective (generate audit records), and FAU_SAR.1, SAR.2 and SAR.3 directly implement the other part (provide the means to review audit records).
O.PROTECTED_CONFIG	FMT_* requires the implementation of mechanisms to secure the management functions that control the configuration of the TSF. Specifically, FMT_ MOF an requires selected management function to be only effected by particular user roles with concrete permissions . FMT_MSA requires the implementation of a security policy to control adjudication of security attributes. FMT_MTD and FMT_SA explicitly require access control to configuration data. FMT_SMF requires the TOE to implement specific security management functions. FMT_SMR, FIA_ATD, FIA_SOS, FIA_UAU and FIA_UID together require the implementation of role-based access control.
O.PROTECTED_AUDIT	FAU_STG explicitly requires the protection of audit records against tampering.

7.2.2 Security requirement dependency rationale

With the exception of dependencies to reliable time stamps, all dependencies of the Security Functional Requirements of the TOE are satisfied by the TOE. The satisfaction of dependencies is given for each SFR in the statement of that SFR in Sect. 5.3.

7.2.3 Security assurance requirements justification

The TOE is a commercial product whose users require a moderate level of independently assured security. The TOE is targeted at an environment with good physical access security where it is assumed that attackers will have Basic attack potential. Thus, EAL2 is an adequate assurance level for the TOE and its intended environment. EAL2 constitutes a well defined, standard assurance package fully defined in [CC] Part 3 and is therefore consistent.

This EAL2 assurance has been augmented with ALC_FLR.2. Augmentation with this specific flaw remediation security assurance requirement has been performed to provide additional assurance regarding the flaw remediation practices employed.

Annex A Terminology

The following terminology is used in this Security Target and/or is applicable to public key infrastructures more broadly.

Table 12 - Terminology

Term	Description
ACE	Adaptive Communication Environment (used in the TOE for socket communications and threading).
Administrator	A user that has a level of trust (with respect to the TOE's security functionality) compared with a TOE user that is not an administrator.
AES	Advanced Encryption Standard.
Announce message	A message sent to the CA server by another TOE subcomponent when it (the other TOE subcomponent) starts up.
ANSI	American National Standards Institute.
ARL	See *Authority revocation list.*
ARM	Advanced Registration Module. An optional component used to implement custom automated request submission and authorization flows. (Not part of the TOE.)
ASN	Abstract Syntax Notation.
Attacker	A (potential) threat agent, which may be a user, or any other human or IT entity that attempts to interact, logically or physically, with the TOE
Audit log	Security relevant events occurring during the operation of the TOE are recorded in audit logs (collections of audit records).
Auditor	A special class of administrator that is given permissions to perform functions on the audit logs.
Authorization	The process of approving a request against criteria set forth in a registration policy.

Term	Description
Authorization group	An authorization group is a specific set of authorizers (human or automated processes). Membership within an authorization group may be indicated by a specify DN or DN attribute. Authorization groups are set up using the CAO, and are used to control which authorizers can process requests submitted using a particular registration policy.
Authorizer	Human or automated process, which approves a request against criteria set forth in a registration policy, whereupon a certificate is generated and issued upon affirmative approval.
Authority Revocation list	A revocation list containing identification of public-key certificates issued to Certification Authorities (CA) that are no longer considered valid by the certificate issuer. This is essentially a list of authorities that have been compromised in some way and can no longer be trusted. (It is effectively a form of CRL.)
Autoenroll Handler	A *protocol handler* (see *protocol handler below)* component that implements the Microsoft Autoenrollment protocol. The autoenroll handler supports automatic registration of users and computers in Microsoft Windows domains.
Bootstrap	The process of creating a PKI, which involves creating the CA and CAO.
BRSP	A set of clearly defined protocols that allow remote applications to send requests into the RA eXchange and then to receive a response.
CA	See *Certification Authority.*
CA clone	Separate instances of the CA executable, which use the same key material and the same database.
CA sub-components	Combination of CA (Server), CAO, Publisher and Certificate Status Server (CSS) that, together with a CA database, provide the certification part of the PKI system.
CAO	See *Certification Authority Operator.*
CAO User	Person who operates the CAO.

Term	Description
CDP	See *CRL distribution point.*
Certificate	For the purposes of this document, certificate refers to *X.509 Certificate* - see below.
Certificate extensions	Optional fields within an X.509 v3 formatted certificate that contain information designed to enhance the certificate verification process and to convey additional information about the subject and issuer of the certificate.
Certificate revocation list	A signed list of certificates (serial numbers) that have been revoked and can no longer be trusted (according to the standard for CRL v2 as defined in X.509).
Certification Authority	The component within the TOE which is responsible for the creation, distribution, or revocation of X.509 public key certificates.
Certification Authority Operator	The interface through which the elements of a public-key infrastructure (PKI) are defined, configured and controlled. The CAO is used to configure the PKI, define registration policies, and administer certificates. It is the trusted system management component for a CA.
Certification Practices Statement	A detailed document issued by a Certification Authority that prescribes the operational procedures on the operational and registration policies under which that authority issues public-key certificates.
Clone	See *CA clone, RA clone, KAS clone, RAX clone* or *CSS clone.*
CMP	Certificate Management Protocol. (The CMP Handler is not part of the TOE.)
Communication channel	Used in this ST in a very general sense; for example, one TOE sub-component may send a message to a second TOE sub-component by writing some data into the CA database (which is managed by the operating environment), for subsequent retrieval by the second TOE sub-component.
CPS	See *Certification Practices Statement.*
CRL	See *Certificate revocation list.*

Term	Description
CRL distribution point	The location from which a CRL or partitioned CRL can be obtained. Specifically, an X.500 directory entry or other information source that is named in an X.509 v3 public-key certificate extension as a location from which to obtain a certificate revocation list.
Cross-certification	The process whereby a UniCERT CA can certify another CA and by doing so allow users certified by the UniCERT CA to trust certificates issued to the cross certified CA. Cross certification can be unilateral or bilateral.. Cross-certification is handled using the normal processes for signing any certificate, but via a slightly different message and certificate format.
Crypto module	A hardware security module (HSM) or smart card, which can be used to store keys and perform some cryptographic operations.
CSS clone	Separate instances of the CSS executable, which use the same key material and the same database.
DB	Database.
DER	Distinguished Encoding Rules.
Directory server	A directory server is typically used to store information, such as a company directory, in a central repository and to provide quick and easy access to this information. LDAP is a standard protocol for accessing directory servers.
Distinguished Name	A sequence of attributes that identifies an entity and traces its path up the directory tree. The DN provides the necessary information about the owner of a certificate. The certificate contains both the DN of the owner (subject) and the DN of the issuer of the certificate.
DN	See *Distinguished name.*
DN attribute	An element of a distinguished name, e.g., C=US or O=Verizon.
DSD	Defence Signals Directorate.
DSA	Digital Signature Algorithm.

Term	Description
ECC	Elliptical curve cryptography is a public-key encryption method based on the algebraic structure of elliptic curves over finite fields.
ECDSA	Elliptic Curve Digital Signature Algorithm, see *ECC*.
EE	See *End entity.*
Email Handler	A Protocol Handler which enables certificate requests to be received via email and the associated email responses to be returned via email. The Email Handler also sends the notifications as configured in registration policies.
End entity	An entity (e.g. end user) that is the subject of a public-key certificate and that is using, or is permitted and able to use, the matching private key only for some purpose other than signing a certificate.
End user	An end user is an external system (or a user of an external system) that communicates with the TOE (via the operational environment) in order to request a service or data.
External system	A system external to the PKI system. Note that if a TOE sub-component is hosted on an external system, then a part of that external system (the part which is relied upon to protect the sub-component) is considered to be part of the operational environment.
Face-to-face registration	The process of entering end user details at the WebRAO directly, without a remote request coming in through the protocol handler.
FIPS	Federal Information Processing Standards.
Group	See *Authorization group*.
GUI	Graphical User Interface.
Hardware security module	A hardware security module is a cryptographic device, which can generate, store and use cryptographic keys within a secure hardware device.
HSM	See *Hardware security module.*

Term	Description
HTTP(S)	Hypertext Transfer Protocol (over SSL).
I&A	Identification and Authentication.
IEC	International Electrotechnical Commission.
IETF	Internet Engineering Task Force.
ISO	International Organization for Standardization.
Issuer DN	The distinguished name (DN) that identifies the CA that has issued a certificate.
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector.
JSP	Java Server Page.
KAS	Key Archive Server - a component for securely archiving and recovering private keys for the purpose of preventing data loss in the event a key is lost or a cryptographic device containing a key is damaged.
KAS clone	Separate instances of the KAS executable, which use the same key material and the same database.
LDAP	See *Lightweight Directory Access Protocol.*
LDAPS	LDAP over SSL.
Lightweight Directory Access Protocol	A set of open protocols for accessing information directories. LDAP can make the physical network topology and protocols transparent so that a network user can access any resource without knowing where or how it is physically connected.
LTSK	Long Term Storage Key - The Key Archive Server uses the LTSK to encrypt the archived keys it stores.
Message	An object which is transmitted to or from a (sub-)component of the TOE via a *communication channel*. Different types of message contain different types of information and/or other objects.

Term	Description
Object identifier	A string of numbers that is unique worldwide, for example, 1.2.840.23452323.1.1. An OID represent a hierarchy of domains and objects within domains, using numbers instead of names. Each OID starts from an internationally defined root. For example, 1 at the first level represents the International Standards Organization (ISO). Each level of the hierarchy is represented by its own unique number (ID), which is appended to the OID of the level above it. For example, 1.2.840 represents the hierarchy: ISO (1) ISO member-body (2) United States (840). In a hierarchy like this, each country is responsible for defining the structure of the rest of the OID under the third level (country).
OCSP	See *Online Certificate Status Protocol.*
OID	See *Object identifier.*
Online Certificate Status Protocol	A protocol that allows applications to verify whether a certificate is valid or has been revoked. OCSP can be either a replacement or a supplement to checking against a CRL. It attempts to overcome some of the distribution limitations of the CRL. OCSP specifies a request-response message syntax between a client application that requires certificate revocation status information and a server application that has knowledge of the revocation status. The OCSP server (or OCSP responder) can also provide additional status information beyond that available through a CRL.
Openv (or op env)	Operational environment.
Openv user	An authorized user of the operational environment that accesses the TOE (if at all) in order to indirectly support the services it offers (e.g. to backup data).

Term	Description
Operational policy	An operational policy consists of security or PKI relevant configuration information for a PKI entity. For example, the CA's operational policy defines how often the CA generates a CRL and whether it generates a new CRL each time a certificate is revoked. The RA's operational policy defines the time period during which the RA processes certificate requests and how often it polls the database for new requests.
Owner	The owner of a certificate is the user to which the certificate was issued, and which can, if necessary provide POP of the private key that the certificate is associated with. Similarly, an owner of a (private) key is a user which can provide POP of the key (see *Proof of possession* re "provide POP"). An owner of a PSE/P12 is a user which can provide POP of the key contained within the file. An owner of a CRL is the issuer of the CRL. The Owner of an Operational Policy is the signer of the Operational Policy.
P11	A standard for accessing cryptographic hardware tokens, for example smart cards and HSMs. The standard is defined in [PKCS11].
P12	A standard for securely exchanging and storing key material as passphrase encrypted files. The standard is defined in [PKCS12].
PEM	Privacy Enhancement for Internet Electronic Mail.
Permission	A member of a set of rules for how a user may interact with the TOE.
Personal secure environment	Verizon supports the concept of a personal secure environment (PSE). This proprietary format holds certificate owners' private keys and other sensitive data securely. They can only be accessed or altered by the authorized owner of those keys. UniCERT supports only disk-based PSEs.
PH	See *Protocol Handler*.
PKCS	Public-Key Cryptography Standards.
PKCS#11 device	See *Crypto module.*

Term	Description
PKI	See *Public key infrastructure.*
PKI entity	One of the UniCERT core components that are within the PKI system.
PKI system	*A* PKI system is synonymous with PKI; *the* PKI system is defined as is the TOE and its operational environment.
POP	See *Proof of possession*.
Proof of possession	A verification process whereby it is proven that the owner of a key pair actually possesses the private key associated with the public key.
Protocol Handler	A protocol handler is a UniCERT registration component though which applications can make protocol specific request for certificates and other PKI related services. A protocol handler converts requests from protocol specific formats to the common request format that is used internal to the UniCERT system.
PSE	See *Personal secure environment.*
Public-key certificates	A set of data that uniquely identifies an entity, contains the entity's public key and optionally other information that is digitally signed by a trusted party, thereby binding the public key to the entity. The optional information may provide more information about the user and how the key should be used.
Public-key infrastructure	A PKI system provides a framework by which users and entities can communicate securely. Public-key cryptography uses a combination of public and private keys, digital signatures, digital certificates, and Certification Authorities (CAs), to meet the major requirements of security. The X.509 standard defines a PKI as "The set of hardware, software, people and procedures needed to create, manage, store, distribute and revoke certificates based on public-key cryptography." Described in [RFC] (RFC 5280 as published by the IETF).
Publisher	Distributed with the UniCERT Core components, the Publisher posts information and certificates externally to the secured PKI.

Term	Description
RA	See *Registration Authority.*
RSA	Rivest, Shamir and Adleman (who publicly described an algorithm for public key cryptography in 1978).
RA clone	Separate instances of the RA executable, which use the same key material and the same database.
RA sub-components	Combination of RA (Server), RA eXchange, Protocol Handlers, and WebRAO that, together with an RA database, provide the registration portal (interface) to the PKI system.
RAO	See *WebRAO*.
RAX	See *RA eXchange*.
RAX clone	Separate instances of the KAS executable, which use the same key material and the same database.
Registration	The process of collecting information required to generate and authorize (approve) a certificate request. Registration may be face-to-face, or may be via a protocol handler or programmatic interface (referred to as remote registration).
Registration Authority	The RA acts as a router, transferring information to and from the CA. It receives and verifies certificate requests from the registering entities, and sends back the CA's reply.
Registration Authority Operator	See *WebRAO*.
Registration policy	A registration policy provides a set of rules and criteria for certificate requests that must be met before the CA can issue a certificate. A registration policy governs what data must be collected for the certificate applicant to register, determines the content of the certificate(s) produced, and controls the life cycle of the certificate.
Registration Policy Editor	The registration policy Editor is a portion of the CAO, which is used to create registration policies.
Remote registration	The process of registration being initiated via a protocol handler or a programmatic interface rather than face-to-face.

Term	Description
Revocation	The process of invalidating a public key certificate. There are a number of reasons for revocation, including: unspecified, key compromise, CA compromise, affiliation changed, superseded and certificate hold. A certificate hold places a certificate on hold, referred to as suspension of a certificate in this document. Except for certificate hold, all other reasons for revocation are permanent, which means the certificate will no longer be or become valid.
Revocation request	Revocation requests include requests to revoke, suspend and unsuspend a certificate.
Revoke	To invalidate a certificate.
RFC	Request for Comments.
Root CA	The Certification Authority at the top of the PKI hierarchy.
Root certificate	The self-signed public-key certificate at the top of the PKI hierarchy.
SCEP Handler	A *protocol handler* (see *Protocol Handler)* that implements the *Simple Certificate Enrolment Protocol* defined by http://www.ietf.org/id/draft-nourse-scep-19.txt. SCEP is a registration protocol used primarily by routers and VPN devices.
Schema	The structure of a database system, including the layout of fields in tables, and the relationships (if any) between different tables.
Smart card	A card with an embedded integrated circuit for storing information, typically used for authenticating a computer user or banking services, providing access control, storing value applications, and/or carrying private keys in a security system.
Social engineering attack	An attack whereby a trusted person is either bribed or threatened to cause them to reveal or change something that they should not.
SQL	Structured Query Language.
SSL	Secure Socket Layer.

Term	Description
Subject DN	The distinguished name that identifies the entity to whom a certificate is issued, for example: cn=John Doe, ou=Sales, o=Acme, l=Northeast, c=US.
Subordinate CA	A Certification Authority that is below the level of the root CA. A subordinate CA's certificate is registered (certificate is signed by another CA) as part of another PKI. This is typically the case for commercial CAs, who wish to use a well-known, trusted third party CA as their root CA. UniCERT may be configured either as a root CA or a subordinate CA.
Suspension	The temporary revocation of a certificate. Once a certificate has been suspended it can be handled in one of three ways: • It may remain on the CRL with no further action, causing users to reject transactions issued during the hold period. • It may be replaced by a (final) revocation for the same certificate, in which case the reason shall be one of the standard reasons for revocation, the revocation date shall be the date the certificate was suspended. • It may be explicitly released and the entry removed from the CRL.
TOE user	An authorized (human) user of the TOE who accesses it in order to directly support the services it offer (e.g. to authorize an end user's request for a certificate).
Token	Synonymous with *Crypto module* (in this ST).
Unidbase (UniDB)	An internal component of the TOE that provides object corresponding to tables and records within the UniCERT database schema.
Unsuspension	Removing the temporary hold (suspension) of a certificate and therefore removing it from the CRL.
UPI	UniCERT Programmatic Interface. A separate software toolkit, which provides access to the authorization and registration functionality within UniCERT. (Not part of the TOE.)
VPN	Virtual Private Network.

Term	Description
Web Registration Authority Operator	See *WebRAO.*
WebRAO	A Web-based application used to review and authorize (approve) certificate requests. It may also be used to submit certificate requests on behalf of an end entity.
X.509	The ISO/ITU-T X.509 standard defines what information can be included in a certificate and a certificate revocation list and describes the data format of the information.
X.509 certificate	The ISO/ITU-T X.509 Standard defines two types of certificates, the X.509 public key certificate and the X.509 attribute certificate. In this document the X.509 certificate refers to a X.509 public key certificate. *(*See *also Public Key certificate.)*
X.509 public key certificate	A block of data containing the certificate holder's public key and basic identification details rendered unforgeable by the digital signature of the issuing CA's private key, encoded in the ISO/ITU-T X.509 format.

Annex B Audit events

The auditable events for the TOE are specified in the following tables. Each table is devoted to the sub-component of the TOE which is responsible for generating the corresponding audit records; the "Contents" column specifies the information contained in these records (see also the SFR component FAU_GEN.1.2).

Certification Authority (CA)

Table 13 – CA audit events

Auditable Event	Event Description	Contents
Signature Verification Failure	Signature verification failure	Event type, CAO User DN, time/date, identifiable description of what failed verification and where it came from.
Certificate Generation	A certificate has been generated, signed and stored	Event type, CA user DN, time/date, reference number, issuer DN, subject DN, serial number, certificate
Certificate Revoked	A revocation request has been processed and revoked (marked in the database as revoked, suspended, released from suspension)	Event type, CA user DN, identification of RA that revocation request was received from, time/date, unique identity of revocation message including certificate revoked, suspended or released from suspension and the revocation reason, unique identity of revocation requester and approver.
CRL Generated	A CRL has been generated, signed and stored. Including Success and Failure	Event type, CA user DN, time/date, unique identity of CRL.
PKI Information sent	PKI operational policy is signed and pushed	Event type, CA user DN, time/date, unique identity of PKI and identity of entity it was pushed to
User or System access initiated	A connection to the CA has been established. Including Success and Failure	Event type, CA user DN, Unique identity of user or system accessing the CA (e.g., identification of CAO User), time/date
User or System access terminated	A connection to the CA has been terminated	Event type, CA user DN, Unique identity of user or system disconnected from the CA (e.g., identification of CAO User), time/date
PKI Event	Tampered PKI detected	Event type, CA user DN Unique identity of profile that was tampered, time/date

CA Operator (CAO)

Table 14 – CA operator audit events

Auditable Event	Event Description	Contents
Certificate Revoked	A revocation request has been submitted to the CA. Including if it's successfully sent or not.	Event type, CAO User DN, time/date, unique identity of revocation message including certificate revoked, suspended or released from suspension and the revocation reason.
Certificate Revoked	A revocation request has been submitted to the CA and the CA has responded with success or fail.	Event type, CAO User DN, time/date, unique identity of revocation message including certificate revoked, suspended or released from suspension and the revocation reason.

Auditable Event	Event Description	Contents
Certificate Request Sent	A certificate request has been signed and sent to the CA.	Event type, CAO User DN, time/date, reference number, request data, identification of CA to which the request was sent
Received Certificate Request	A certificate request has been received.	Event type, CAO User DN, time/date, certificate request data uniquely identifying the certificate request, certificate request receipt method (e.g., imported from floppy,)
Policy Created	A policy was created and saved to the database.	Event type, CAO User DN, time/date, policy name
Policy Retired	A policy was retired and saved to the database.	Event type, CAO User DN, time/date, policy name
Policy Withdrawn	A policy was withdrawn and saved to the database.	Event type, CAO User DN, time/date, policy name
Policy Deleted	A policy was deleted.	Event type, CAO User DN, time/date, policy name
Processing (Authorization) Path Events	An authorization path is added.	Event type, CAO User DN, time/date, unique identity of path, group and policy and identity of entity it is to be pushed to.
Processing (Authorization) Path Events	CAO User uses the authorization group definitions to define which, a subset or all, of an authorization group is required to authorize a request. This event is added when a modification of path is committed.	Event type, CAO User DN, time/date, unique identity of path, group and policy and identity of entity it is to be pushed to.
Processing (Authorization) Path Events	CAO User uses the authorization group definitions to define which, a subset or all, of an authorization group is required to authorize a request. This event is added when a path is retired.	Event type, CAO User DN, time/date, unique identity of path, group and policy and identity of entity it is to be pushed to.
Session events	The CAO application may log onto a number of PKIs, but only one per session	Type, CAO User DN, time/date, unique identity of PKI.
Session events	The CAO application may log onto a number of PKIs, but only one per session	Type, CAO User DN, time/date, unique identity of PKI.
Audit Archive	An archive function has been performed on the audit log within the CA database and an audit log archive file has been created.	Event type, CAO User DN, time/date, identification of audit log archive file created.

Registration Authority (RA)

Table 15 – RA audit events

Auditable Event	Event Description	Contents
Signature Verification	Signature verification. Success or failure	Event type, RA User DN, Unique identity of issuer of data failing signature (e.g., RAO user), time/date, identifiable description of what failed verification.
Message Validation	Received request message validation success or failure	Event type, RA User DN, Unique identity of issuer of data failing validation (e.g., RAO user), time/date, identifiable description of the request that failed validation, a description of the validation failure (e.g., what was revoked, as well as why and when it was revoked).

Auditable Event	Event Description	Contents
Certificate Request Generated	A certificate request has been generated signed and saved.	Event type, RA User DN, time/date, certificate request data uniquely identifying the certificate request, indication of the type of request (e.g., renewed certificate request)
Certificate Request Sent	A certificate request has been signed and sent to the CA.	Event type, RA User DN, time/date, reference number, request data, identification of CA to which the request was sent
Received signed certificate	A signed certificate was received and stored in the RA database.	Event type, RA User DN, identification of CA certificate was received from, time/date, reference number, issuer DN, subject DN, serial number, certificate
Storage of received certificate failed	A signed certificate was received but its storage failed.	Event type, RA User DN, identification of CA certificate was received from, time/date, reference number, issuer DN, subject DN, serial number, certificate, reason for failure
Revocation Request Sent	A revocation request has been signed and sent to the CA.	Event type, RA User DN, time/date, request data including unique identity of revocation request message including certificate revoked or suspended and the revocation reason, identification of entity revocation request was received from (e.g., RA eXchange, RAO), identification of entity that revocation request was received from and approved by (e.g., RA eXchange)
Received signed revocation	A signed revocation message was received and stored in the RA database.	Event type, RA User DN, identification of CA revocation was received from, time/date, request data including unique identity of revocation request message including certificate revoked or suspended and the revocation reason, identification of entity revocation request was received from and approved by (e.g., RA eXchange)
Storage of received revocation message failed	A Signed revocation message was received but its storage failed.	Event type, RA User DN, identification of CA revocation was received from, time/date, request data, unique identity of revocation message including certificate revoked, reason for failure
RA has connected to a CA	A connection to the CA has been established.	Event type, RA User DN, identity of system accessing the CA (e.g., identification of RA), time/date
RA has disconnected from the CA	A connection to the CA has been terminated.	Event type, RA User DN, identity of system disconnected from the CA (e.g., identification of RA), time/date
RA is trying to connect to a CA	Announce message sent to the CA.	Event type, RA User DN, identity of the CA (e.g., identification of CA including port machine name), time/date
PKI information is received.	Event includes CRL, policies, auth groups and PKI entities	Event type, RA User DN, identity of entity the policy was received from, time/date, unique identity of policy

RA Event Viewer

Table 16 – RA event viewer audit events

Auditable Event	Event Description	Contents
Audit Archive	An archive function has been performed on the audit log in the RA database and an audit log archive file has been created.	Event type, RA Event Viewer user DN, time/date, identification of audit log archive file created.

RA eXchange (RAX)

Table 17 – RAX audit events

Auditable Event	Event Description	Contents
Signature Verification Failure	Signature verification failed.	Event type, Unique RA eXchange, or RA eXchange interface identifier, identity of issuer of data failing signature (e.g., end entity cert requester), time/date, identifiable description of what failed verification (e.g., request data)
Certificate Request Received	Certificate request is received.	Event type, Unique RA eXchange or RA eXchange interface identifier, certificate request data, time/date
Certificate Request Sent for Authentication	Certificate request sent (stored) for authentication	Event type, RA eXchange or RA eXchange interface identifier, auth ID, issuer DN, subject DN, time/date
Received signed certificate	A signed certificate was received.	Event type, RA eXchange or RA eXchange interface identifier, identification of RA certificate was received from, time/date, reference number, issuer DN, subject DN, serial number, certificate
Certificate Identity Data Modified	A certificate's identity data has been modified; the new request is also logged.	Event type, RA eXchange or RA eXchange interface identifier, identification of RA certificate was received from, time/date, reference number, issuer DN, subject DN, date time.
A notification message has been sent	A certificate rejection notice has been sent to the requestor.	Event type, RA eXchange or RA eXchange interface identifier, time/date, description of certificate, and end user, reason the request was rejected, distribution method (e.g., email), and address (e.g., email address)

Key Archive Server (KAS)

Table 18 – KAS audit events

Auditable Event	Event Description	Contents
Signature Verification	Signature verification. Success or failure	Event type, KAS identifier (e.g., DN), Unique identity of issuer of data failing signature (e.g., CA identifier), time/date, identifiable description of what failed verification.
PKI information is received.	Event includes CRL, policies, auth groups and PKI entities	Event type, KAS identifier(e.g., DN), identity of entity the policy was received from, time/date, unique identity of policy
Key archive	Key archive success or failure	Event type, KAS identifier (e.g., DN), time/date, reference number, reason for failure
Key recover and encrypt for requestor	Key recover and encrypt for requestor success or failure	Event type, KAS identifier (e.g., DN), time/date, reference number, requesting entity identifier (e.g. KAO user) , reason for failure
LTSK generated	A new LTSK has been generated	Event type, KAS identifier (e.g., DN), time/date, reference number
Switched to new LTSK	Switched to use new LTSK for archival	Event type, KAS identifier (e.g., DN), time/date, reference number

Key Archive Operator (KAO)

Table 19 – KAO audit events

Auditable Event	Event Description	Contents
Abort key archive request	Abort key archive request	Event type, KAO user (e.g., DN), time/date, reference number, subject name of certificate associated with Key, reason for failure
Key archive request sent	Key archive request sent (stored)	Event type, KAO user (e.g., DN), time/date, reference number, subject name of certificate associated with Key
Received key archive response	Key archive response received, success or failure	Event type, KAO user (e.g., DN), time/date, reference number, subject name of certificate associated with Key, reason for failure
Key recovery request sent	Key recovery request sent (stored)	Event type, KAO user (e.g., DN), time/date, reference number, subject name of certificate associated with Key to be recovered.
Received key recovery response	Key recovery response received, success or failure	Event type, KAO user (e.g., DN), time/date, reference number, subject name of certificate associated with Key, reason for failure
LTSK generation request	LTSK generation request sent (stored)	Event type, KAO user (e.g., DN), time/date, reference number
Audit Archive	An archive function has been performed on the audit log in the KAS database and an audit log archive file has been created.	Event type, KAO user (e.g., DN), time/date, identification of audit log archive file created.

Annex C Subjects, attributes, objects and operations

TOE roles

Table 20 – TOE roles

Role	May be adopted by	(Possible) permissions
CAO User	TOE user	Create Registration Policy; Modify Policy; Import Policy; Retire Policy; Withdraw Policy; Delete Policy; Create Authorization Group; Modify Authorization Group; Retire Authorization Group; Create PKI; Resume Key Generation; Create PKI Entity; Modify PKI Entity; Remove PKI Entity ; Register Entity; Export Certificate; Revoke Certificate; Renew CA/PKI Entity; Export CRL; Configure CAO; RAA and KAO Roles; Adopt the CAO Auditor role; Adopt the CAO Audit Manager role.
CAO Audit Manager	TOE user	Archive Audit Log ; Adopt the CAO Auditor role.
CAO Auditor	TOE user	View Audit Log, Verify Audit Log
RA User	TOE user	Adopt the RA Audit Manager role; Adopt the RA Auditor role.
RA Audit Manager	TOE user	Adopt the RA Auditor role.
RA Auditor	TOE user	N/A
WebRAO User	TOE user	N/A
RRO	TOE user	N/A
KRO	TOE user	N/A
KAO User	TOE user	Archive end users' private encryption keys; Recover end users' private encryption keys; Initiate re-generation of the LTSK; Adopt the KAO Auditor role; Adopt the KAO Audit Manager role.
KAO Audit Manager	TOE user	Adopt the KAO Auditor role.
KAO Auditor	TOE user	N/A
End user	End user	N/A

Subjects

For the following table, the definitions of certificate actions and cryptographic actions are as follows:

- Certificate actions – means that the user/subject can, limited by their assigned role:
  - Register certificate requests, and check the status of these requests;
  - Approve or reject a certificate request; and
  - Approve or reject a revocation request; View certificates and certificate status.
- Cryptographic actions - means that the user/subject can (subject to the limitations of the policy of the PKI system and knowledge of any required passphrase or PIN):
  - Generate, distribute, access and destroy cryptographic keys; and
  - Select cryptographic algorithms and key sizes.

Table 21 – Subjects and security attributes

User/Subject	Attributes (plus Role and subset of permissions; Means of I&A)
CAO User	Certificate actions, Cryptographic actions.
CAO Audit Manager	Can query, verify and archive CA (i.e. both CA and CAO-produced) audit records (using the CAO).
CAO Auditor	Can query and verify CA (i.e. CA and CAO-produced) audit records (using the CAO).
RA User	
RA Audit Manager	Can query, verify and archive RA audit records (i.e. RA, RAX, RA Event Viewer and WebRAO produced) (using the RA Event Viewer).
RA Auditor	Can query and verify RA audit records (i.e. RA, RAX, RA Event Viewer and WebRAO produced) (using the RA Event Viewer).
WebRAO User	Certificate actions; Cryptographic actions.
RRO	Certificate actions; Cryptographic actions.
KRO	Can recover archived keys.
KAO User	Cryptographic actions; Can archive and recover keys.
KAO Audit Manager	Can query and archive KAS (i.e. both KAS and KAO-produced) audit records (using the KAO).
KAO Auditor	Can query KAS [i.e. both KAS and KAO-produced] audit records (using the KAO).
End user	An end user cannot directly access objects controlled by the TSF. It can only send (and subsequently receive) messages to and from the TOE, and retrieve published objects.

Objects

The objects that the TSF is concerned with are specified in the following table, together with their security attributes, and the operations that may be performed upon them.

The security attributes listed for an object refer to (a representation of) a property of that object which is controlled by the TSF. Another representation of the same property may be part of the data which is contained in the object; this may be TSF data or user data.

The operations that the TSF is concerned with, i.e. those listed in the table, are those "controlled" operations which are covered by the PKI access SFP and the PKI messaging SFP. Other possible operations on an object, e.g. reading or writing a message, are, in themselves, outside the scope of those policies; however, they may be an implicit part of a controlled operation (e.g. a subject has to read a message before deciding whether to accept or reject it).

For convenience, the table also includes an "object" identified as "TOE service", which indicates a TOE sub-component that provides a TOE service, namely the CA, Publisher, RA, RAX, CSS, KAS, Email Handler, Autoenroll Handler and SCEP Handler sub-components. These have to be manually started by an authorized TOE user (typically via the Service Manager utility).

Table 22 – Objects, security attributes and operations

Object	Security Attributes	Controlled operations (and notes)
Audit record	Type, Originator, Signature	Query; Archive The type relates to the subcomponent that created the record, i.e. CA, CAO, RA, RAX or RA Event Viewer
Certificate	Owner; Issuer; Status	Create; Modify status; Query status The Status attribute indicates whether or not the certificate is revoked or suspended, and whether or not it is valid (in the RFC 5280 sense, i.e. the current time is within its validity period)
CRL	Owner; Issuer; Status	Create; Publish The Status attribute indicates whether or not the CRL is valid (in the RFC 5280 sense, i.e. the current time is within its validity period)
Private key	Owner	Generate, Distribute, Access, Destroy
PSE or P12 file	Owner	Generate, Distribute, Access, Destroy
Operational policy	Owner	Create; Modify
Registration policy	Authorization Group	Distribute; Access
PKI configuration	Creator (CAO user); Version; Signature	Create; Query

Object	Security Attributes	Controlled operations (and notes)
Message	Type; Originator; Signature	Accept; Reject An accepted message is operated on further according to its type (see below), and can lead to an info flow The Originator attribute includes a means of verifying the signature (i.e. of obtaining the relevant certificate)
Request message	Type; Originator; Signature; Status	Authorize Type indicates what is being requested, e,g, generate and issue a certificate Status is approved or rejected (or pending)
Response message	Type; Originator; Signature; Result	Type equates to that of a request message that has undergone the Authorize operation (i.e. been approved or not) Result is request approved or rejected
Announce message	Type; Originator; Signature	Accept; Reject
End user info		End user info is embedded in other objects (messages, certificates), and if a subject is able to access and operate on that object then it is implicitly able to access and operate on the end user info (to the same extent that it can access and operate on that object)
TOE service	Certificate owned by the TOE subcomponent that provides the service	Start This operation can be performed only by a user/subject that can provide POP of the private key that the certificate is associated with.

Messages

Table 23 –Receiving subjects and information flows

Receiving subject	Valid sending subjects/ message types	Message checks (and any other notes)
CA (server)	RA: Announce, Certificate/renewal/revocation request. KAS: Announce. CAO: Announce, Certificate/cross certification/revocation request, CRL generation; PKI configuration.	Verify message signature Check message has not been replayed or delayed Check that the certificate of the sending TOE subcomponent is registered in the TOE PKI system, has any necessary extensions, is neither revoked nor suspended, and is valid (in the RFC 5280 sense, i.e. the current time is within its validity period). If these checks fail the CA will reject the connection.
CAO	CA: Certificate response, cross certification response, revocation response, CRL, PKI configuration	Verify message signature Check message has not been replayed or delayed Check that the certificate of the sending TOE subcomponent is registered in the TOE PKI system, has any necessary extensions, is neither revoked nor suspended, and is valid (in the RFC 5280 sense, i.e. the current time is within its validity period).
Publisher	CA: CA certificate, CRL, EE certificate, PKIEnrollmentService information, Certificate templates for publication.	No message checks
CSS	RA: Status request. RAX: Status request. Other TOE sub-component to CSS: Certificate Status Information request.	No message checks
RA (server)	CA: Response to RA Announce to CA, Response to Certificate/renewal/revocation request. KAS: Response to Key Recovery request, Empty Response to RA Announce to KAS.	Verify message signature Check message has not been replayed or delayed Check that the certificate of the sending TOE subcomponent is registered in the TOE PKI system, has any necessary extensions, is neither revoked nor suspended, and is valid (in the RFC 5280 sense, i.e. the current time is within its validity period).
RA (server)	RAX: Certificate details/registration/renewal/revocation request, Key Recovery request.	Verify message signature
RA (server)	CSS: Status response.	No message checks

Receiving subject	Valid sending subjects/ message types	Message checks (and any other notes)
WebRAO	RAX: Certificate response, Certificate Details response, Certificate Status response, Revocation response, Key Recovery response.	No message checks
Web Handler	RAX: Certificate response, Certificate Details response, Certificate Status response, Revocation response,	No message checks
Email Handler	External system. RAX: Certificate response, Notification request.	The Email Handler will accept any appropriately formatted request from an external system.
SCEP Handler	External system. RAX: Certificate response, Certificate Status response, Certificate Details response.	The SCEP Handler will accept any appropriately formatted request from an external system.
RAX	WebRAO, Web Handler: Certificate/renewal/revocation request, request authorization, Certificate Details, Status request WebRAO: Key Recovery request Email Handler, SCEP Handler, Autoenroll Handler: Certificate/renewal request; Certificate Details request. Certificate Status request RA: PKI configuration	Check that the certificate of the sending TOE subcomponent is registered in the TOE PKI system, has any necessary extensions, is neither revoked nor suspended, and is valid (in the RFC 5280 sense, i.e. the current time is within its validity period). Verify message signature (see FCO_NRO.2) If these checks fail, the RAX will reject the connection.
RA Event Viewer		This sub component is a GUI for viewing and archiving audit records
KAS	RA: Announce, Key Archival request, Key Recovery request CA: PKI configuration KAO: Key Archival request, Key Recovery request; LTSK generation request.	Verify message signature Check message has not been replayed or delayed Check that the certificate of the sending TOE subcomponent is registered in the TOE PKI system, has any necessary extensions, is neither revoked nor suspended, and is valid (in the RFC 5280 sense, i.e. the current time is within its validity period). If these checks fail, the KAS will reject the connection.

Receiving subject	Valid sending subjects/ message types	Message checks (and any other notes)
KAO	KAS: Key Archival response, Key Recovery response.	Verify message signature Check message has not been replayed or delayed Check that the certificate of the sending TOE subcomponent is registered in the TOE PKI system, has any necessary extensions, is neither revoked nor suspended, and is valid (in the RFC 5280 sense, i.e. the current time is within its validity period).
Autoenroll Handler	External system. RAX: Certificate response, Certificate details response	The Autoenroll Handler will accept any appropriately formatted request from an external system.
Autoenroll Publisher	AutoEnroll Handler: CA certificate, CRL/ARL, EE certificate, PKIEnrollmentService information, Certificate Templates for publication	No message checks