CoreStreet
Real Time Credential Validation Authority
Security Target

ST Version 1.0
September 02, 2004

Prepared for:
CoreStreet Inc.
One Alewife Center, Suite 200
Cambridge, MA. 02140

Prepared By:
Science Applications International Corporation
7125 Gateway Drive, Suite 300
Columbia, MD 21046

Table of Contents

1 Introduction 1
1.1 Identification 1
1.2 Overview 1
1.3 Common Criteria Conformance Claims 1
1.4 Conventions 1
2 TOE Description 3
2.1 Product Overview 3
2.2 Operational Concept 4
2.3 RTC VA Physical Components 6
2.3.1 RTC VA Environment 7
2.4 RTC VA Logical Components 8
2.4.1 Audit Function 8
2.4.2 User Data Protection 9
2.4.3 Identification and Authentication 9
2.4.4 Communication 9
2.4.5 Security Management 10
2.4.6 TSF Protection 10
3 TOE Security Environment 11
3.1 Secure Usage Assumptions 11
3.1.1 Personnel Assumptions 11
3.1.2 Physical Assumptions 11
3.1.3 System Assumptions 11
3.2 Threats 11
3.3 Organizational Security Policies 12
4 Security Objectives 14
4.1 Security Objectives for the Non-IT Environment 14
4.2 Security Objectives for the IT Environment 14
4.3 Security Objectives for the TOE 15
5 IT Security Requirements 16
5.1 TOE Security Functional Requirements 16
5.1.1 Security Audit 16
5.1.2 Communication 18
5.1.3 User Data Protection 18
5.1.4 Identification & Authentication 20
5.1.5 Security Management 20
5.1.6 Protection of TSF 22
5.2 Security Requirements for the IT Environment 23
5.2.1 Cryptographic Support 23
5.2.2 Protection of TSF 23
5.3 TOE Security Assurance Requirements 25
5.3.1 Configuration Management (ACM) 25
5.3.2 Delivery and operation (ADO) 26
5.3.3 Development (ADV) 27
5.3.4 Guidance documents (AGD) 29
5.3.5 Life cycle support (ALC) 30
5.3.6 Tests (ATE) 31
5.3.7 Vulnerability assessment (AVA) 33

6 TOE Summary Specification 36
6.1 TOE Security Functions 36
6.1.1 Audit Function 36
6.1.2 Communication 37
6.1.3 Identification and Authentication 37
6.1.4 User Data Protection 38
6.1.5 Security Management 38
6.1.6 TSF Protection 39
6.2 Assurance Measures 39
6.2.1 Process Assurance 39
6.2.2 Delivery and Guidance 40
6.2.3 Design Documentation 41
6.2.4 Tests 41
6.2.5 Vulnerability Assessment 42
7 Protection Profile Claims 43
8 Rationale 44
8.1 Security Objective Rationale 44
8.1.1 Threats to Security Objective Rationale 44
8.1.2 Assumptions to Security Objective Rationale 46
8.1.3 Organizational Security Policies to Security Objective Rationale 47
8.2 Security Requirements Rationale 49
8.2.1 Security Functional Requirements Rationale 49
8.2.2 IT Environment Security Functional Requirements Rationale 53
8.2.3 Security Functional Requirements Dependency Rationale 53
8.2.4 Explicitly Stated Requirements Rationale 54
8.2.5 Security Assurance Requirement Rationale 55
8.3 TOE Summary Specification Rationale 55
8.4 Strength of Function Rationale 57
8.5 Internal Consistency and Support 57
8.6 Protection Profile Claims Rationale 58
Appendix A - Acronyms 59
Appendix B - Glossary 61

List of Figures

Figure 1: Functional architecture for a simple RTC VA enabled PKI 4
Figure 2: RTC VA operational data flow between PKI components 5
Figure 3: RTC VA System physical components and RTC VA TOE boundary 7

List of Tables

Table 1 – TOE Security Functional Requirements 16
Table 2 – Security Auditable Events for the TOE 17
Table 3 – IT Environment Security Functional Requirements 23
Table 4 – Evaluation Assurance Requirements for EAL3 augmented 25
Table 5 – Threats to Security Objectives 44
Table 6 – Assumptions to Security Objectives 46
Table 7 – Organizational Security Policies to Security Objectives 47
Table 8 – Security Objective of the TOE vs. Security Functional Requirement 50

Table 9 – Security Objective of IT Environment vs. Security Functional Requirements 53
Table 10 – Security Functional Requirement Dependencies..... 54
Table 11 - Security Functional Requirements vs. Security Functions..... 55
Table 12 - Security Assurance Requirements vs. Assurance Measures 56

1 Introduction

This Security Target (ST) document specifies the functional and assurance security measures offered by the CoreStreet Real Time Credential Validation Authority (RTC VA) TOE. In addition it contains the IT security requirements for the IT environment in which the RTC VA will operate. A list of acronyms and a glossary can be found in the appendices.

1.1 Identification

ST Title - CoreStreet Real Time Credential Validation Authority Security Target
ST Version - version 1.0
ST Date – September 02, 2004
TOE Identification – CoreStreet Real Time Credential Validation Authority TOE comprises of

- CoreStreet RTC Authority (RTCA) version 4.0
- CoreStreet RTC Responder (RTCR) version 4.0

Evaluation Assurance Level (EAL) – EAL3 augmented
CC: Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408.

Keywords - Public Key Infrastructure, PKI, Certificate Status, Certificate Revocation, Dynamic Privilege Management, Real Time Credentials, Authorization, OCSP, CRL, Certificate Validation, Privilege Validation, Distributed OCSP, Attribute Validation

1.2 Overview

CoreStreet's Real Time Credential Validation Authority TOE manages and publishes certificate and attribute validity status, making it available to Public Key Enabled (PKE) applications. These applications rely on this information to make access control decisions to both physical locations and logical functions and services.

1.3 Common Criteria Conformance Claims

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, CCIMB-99-033
  - Part 2 Extended

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, CCIMB-99-033
  - Part 3 Conformant
  - Evaluation Assurance Level 3 (EAL 3 augmented with ALC_FLR.1)

- The minimum strength of function (SOF) of the ST is SOF-medium.

1.4 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.

    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter in parenthesis placed at the end of the component. For example FIA_UAU.2 and FIA_UAU.2(b` indicate that the ST includes two iterations of the FIA_UAU.2 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "…**big** ~~some~~ things …").
- Security Assurance Requirements – Modifications and additions to components based on Interpretations are annotated by using bold.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.
- In some cases additional requirements have been added. Where a new requirement was closely related to one of the existing families of security requirements in part 2 of the CC, the new requirement name consists of that family's name followed by X (e.g., FCO_NRO_X.3). Where a new requirement was not closely related to any existing family of security requirements, the most closely related class was used as the basis for the requirements name (e.g., FDP_X_OCSP.1).

2 TOE Description

A Public Key Infrastructure (PKI) is a security infrastructure that creates and manages public key certificates to facilitate the use of public key cryptography. One of the required basic tasks of any PKI is to maintain and distribute certificate status information for unexpired certificates. The CoreStreet RTC VA TOE is designed to provide a truly scalable, and trustworthy method for managing and distributing certificate status. In addition, it extends the functionality and utility of certificates by providing the capability to dynamically manage physical and logical access control attributes without requiring revoking and/or reissuing the certificate. Specifically, the two basic tasks that the CoreStreet RTC VA TOE performs are:

1. maintain and distribute certificate status information for unexpired certificates
2. maintain and distribute associated attribute status information for unexpired certificates

The CoreStreet RTC VA TOE distributes certificate and attribute status information in the form of digitally signed proofs. RTC VA TOE supports two types of validation proofs:

- Digitally signed OCSP responses
- miniCRLs

Either or both of these proofs can be used with any specific implementation of the RTC VA TOE. These validation proofs provide conclusive evidence to a relying party application of the current validity of a certificate or associated attributes.

2.1 Product Overview

The CoreStreet certificate validation solution comprises of three components; the RTC Authority (RTCA), the RTC Responder (RTCR) and the CoreStreet RTC Client toolkit, an OCSP client (relying party application),. The RTC VA TOE consists of two of the three components, the RTCA which securely houses and manages the status of certificates and attributes, and the RTCR which holds and disperses non-secret validation proofs to relying applications.

Figure 1 shows how the CoreStreet RTC VA TOE might integrate into a simple Public Key Infrastructure ("PKI"). In this PKI example the Remote User represents an entity that requests access to a service, data or physical location by presenting his/her certificate to a Relying Party (RP) application. Certificates are generated by the Certification Authority (CA) upon receipt of an authorized request from a Registration Authority (RA). The RP application grants or denies the service or access based on the integrity *and validity* of the presented certificate.

In many PKIs the CA posts certificates and Certificate Revocation Lists (CRLs) to a repository such as the LDAP directory shown in Figure 1. In this example the LDAP directory provides an interface between the CA and the RTCA from which the RTCA can retrieve newly issued certificates and CRLs. (The RTCA can accommodate alternate mechanisms to receive newly issued certificates and certificate status information.)

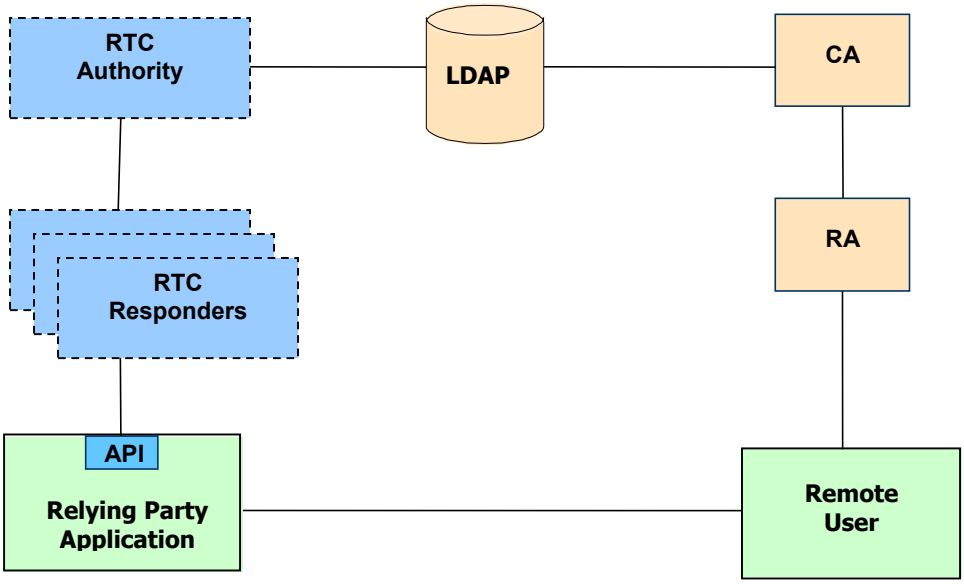

Figure 1: Functional architecture for a simple RTC VA enabled PKI

The RTCA periodically distributes validation proofs (i.e., either signed OCSP responses or miniCRLs) to one or more RTC Responders (RTCR) which then responds to queries by the RP application(s) as to the status of an individual certificate.

2.2 Operational Concept

Figure 2 illustrates the basic operational concept of a PKI system using the RTC VA technology for certificate revocation. Both imported and exported data from the RTC VA are identified and described below:

1. Prior to operation the RTC Authority must be initialized for each issuer of certificates (i.e., CA) that it will support. Issuers are registered with the RTCA which stores the issuer's public certificate along with other identifying information. The RTCA maintains a database of registered issuers, issued certificates or certificate identifiers, and associated certificate and attribute status. This registration interface is manual with issuer registration procedures determined by policy.
2. Issuers publish certificates (e.g., to a local file, LDAP directory, etc.) so the RTCA can retrieve them and manage their associated validation proofs. Certificates are not security sensitive. In configurations where the issued certificates are not available to the RTCA but where the issued certificate serial numbers are sequential, the RTCA establishes certificate identifiers based on these sequential serial numbers. The administrators can configure the RTCA upload the attribute status information from the external source (i.e. from a local file or LDAP directory) or enter the attribute information manually, mapping the attributes to the certificates.

3. Issuers will also publish Certificate Revocation Lists (or provide updated certificate status via some other appropriate means), which will be used by the RTCA to revoke or suspend certificates. CRLs are not security sensitive.

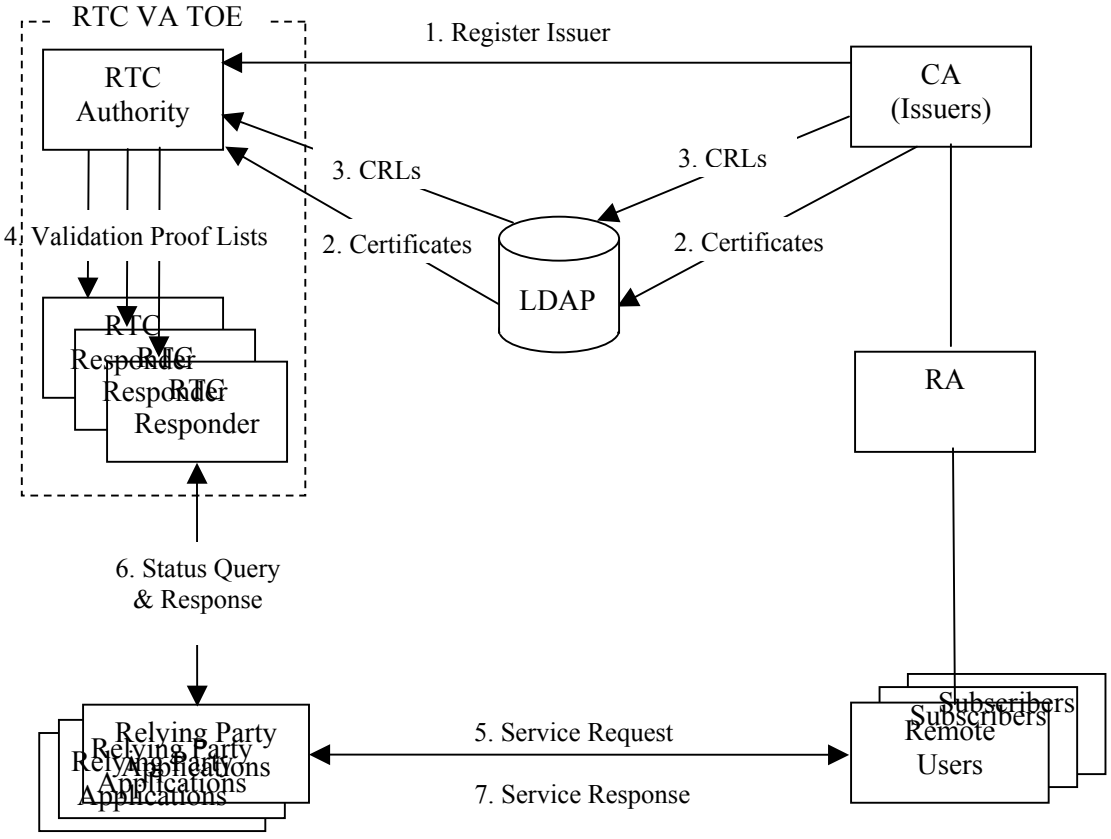

Figure 2: RTC VA operational data flow between PKI components

4. Validation Authorities periodically create and distribute lists containing current proofs for an issuer's certificates. . These validation proof lists are digitally signed and therefore not security sensitive. This digital signature also provides a level of assurance to the receiving responder as to their origin.
5. Remote users request services or access from a relying party application.
6. Relying party applications query responders for the status of a certificate. The responder returns the current certificate status. Neither the RP queries nor the responses are security sensitive.
7. Relying party application grants or denies the remote user's service request based on the status received from the responder.

The core operational tasks of the RTC VA TOE are:

- Maintain accurate certificate and attribute status information
- Distribute accurate certificate and attribute status information in a timely fashion

The RTC VA TOE security functionality is designed to ensure the accuracy of the certificate and attribute status information while RTC VA TOE architecture is designed to ensure the timely delivery and availability of the status information.

2.3 RTC VA Physical Components

Figure 3 illustrates the physical components that make up the RTC VA system as well as the TOE. Note that the TOE consists of just two components, the RTC Authority and the RTC Responders as described below and as depicted in Figure 3.

The purpose of each of the physical components of the RTC VA system is described below:

- RTC Authority (RTCA) - The RTCA periodically generates, signs and distributes public certificate validation proofs to RTC Responders.
- Security Module – provides the following cryptographic support to the RTC Authority:
    - Generating keys
    - Destruction of keys
    - Signing certificate validation proofs (OCSP responses and miniCRLs)
    - (Optionally) Signing lists of responses
    - Signing audit data
    - Establishing SSL secure communications
    - Generating random numbers
    - Verifying CRL and certificate signatures
    - Encrypting security-sensitive data for local storage (for example, passwords and keys)
    - Performing one-way hashing

  The RTCA can perform these functions in software (i.e., for use in customer evaluation of the product); however, a secure configuration requires the use of a hardware security module.
- File Distribution Hardware – serves as a repository for public certificate validation proof lists and provides a way to make the proof lists available at a URL. This mechanism can be implemented using a variety of hardware and software combinations (for example, a static web server; a file server that supports NFS, FTP, or HTTP; or a combination containing a file server that stores the proof lists and a separate HTTP server that requests these lists from the file server and distributes them to responders). The RTCA writes the certificate validation proof lists to the File Distribution Mechanism but there is no information flow from the File Distribution Mechanism to the RTCA (i.e., no upstream communication).
- RTC Responders (RTCRs)– retrieve lists of public validation proofs from one or more RTCAs and provide individual certificate validation information to relying party applications through an HTTP-based protocol.

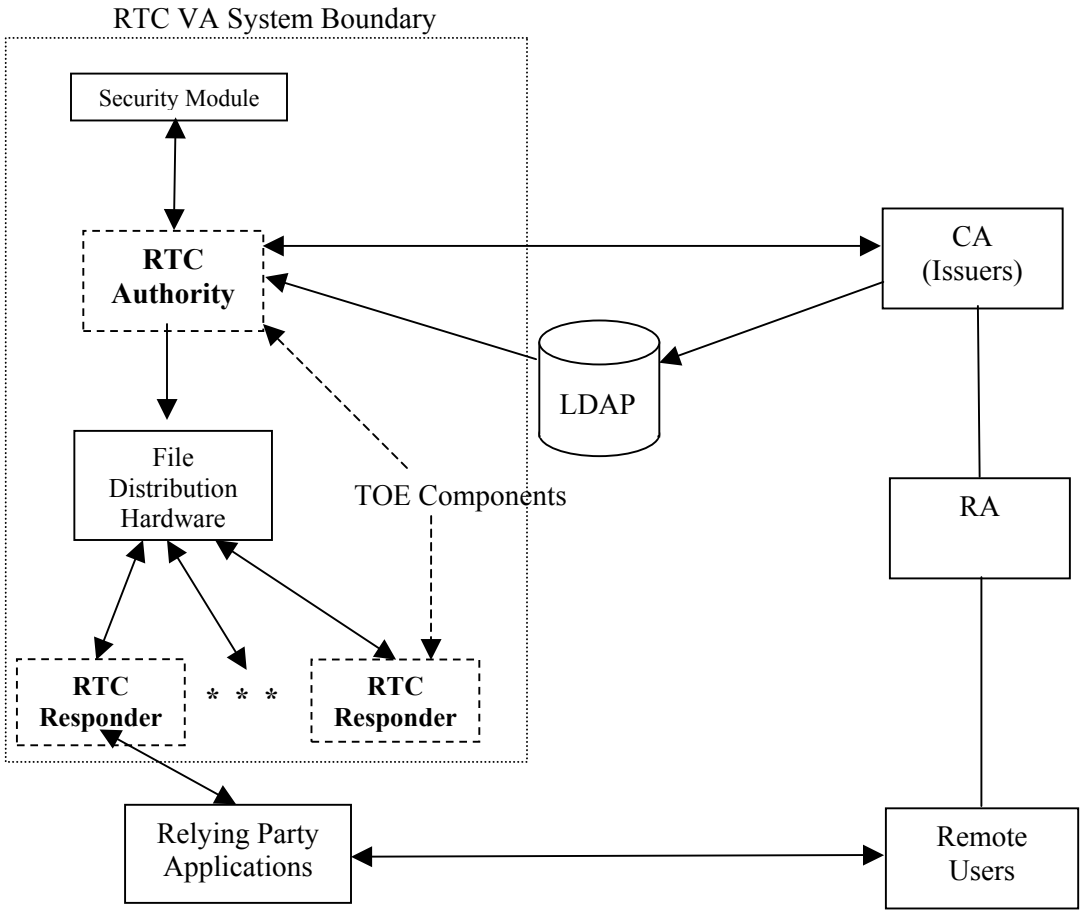

Figure 3: RTC VA System physical components and RTC VA TOE boundary

The RTCA is administered locally by the authorized administrators connected to the system locally via a workstation on the same LAN as the RTCA.

2.3.1 RTC VA Environment

The RTC VA TOE is comprised of software applications that operate in a Windows or Linux/UNIX environment. The operating environment of the RTCA includes a database for the storage, and a security module to perform all required cryptographic functions.

The TOE operates effectively with any combination of the following specific components: Operating system requirements:

Unix

- 1 GHz Intel x86 processor or 500 MHz Sparc processor
- 512 MB memory
- Sun Sparc Solaris 8/RedHat Linux 9
- Database Server (see Database Server section below)
- 100 MB available disk space

Microsoft Windows

- 1 GHz Intel x86 processor
- 512 MB memory
- Microsoft Windows 2000/Microsoft Windows 2000 Server/Microsoft Windows XP
- Professional/Microsoft Windows Server 2003
- Database Server (see Database Server section below)
- 100 MB available disk space (for database)

Database Server

- PostgreSQL 7.3 or higher (recommended for Linux deployments)
- Oracle 9i or higher (recommended for Solaris deployments)
- Microsoft SQL Server 2000 or higher (recommended for Windows deployments)
- Microsoft SQL Server Database Engine (bundled database for Windows deployments)
- McKoi (included with product; appropriate only for product evaluation purposes)

Security Modules:

- Chrysalis™ -ITS Luna SA CA3
- nCipher™ nShield
- Sun JCE (software-only, provided, recommended only for product evaluation purposes)

The TOE interacts with any of the following environment components:
Certificate Authorities:

- Netscape™ Certificate Management Server (CMS Already Certified)
- RSA Keon (Keon Ready™ Certified)
- Microsoft™ Server 2000 Certificate Authority or later
- Baltimore UniCert
- OpenSSL

Relying Party OCSP client plug-ins:

- CoreStreet RTC Client toolkit
- CoreStreet Validation Client
- Alacris™ OCSP client
- AssuredBytes™ OCSP client
- Valicert™ OCSP client toolkit
- Valicert™ Desktop Validator
- OpenSSL OCSP toolkit (open source)

2.4 RTC VA Logical Components

The logical boundaries of the TOE are defined by the security functions implemented.

2.4.1 Audit Function

The RTCA generates audit records based on the administrative actions and system actions. The audit records are stored within the environment. The administrative actions are audited and stored in a database utilized by the TOE, while system actions are stored in a system log file

defined by the TOE. The Auditor is able to view, search and sort the audit records generated based on administrator actions. The system log records are viewable by the Administrator only.

2.4.2 User Data Protection

The TOE defines the access to the TSF and user data based on the role that is assigned to the authorized user. The TOE implements an access control policy which limits the interfaces accessible to users to those associated with the defined roles of the TOE. The interfaces define what actions may be performed to the TSF and user data stored within the database.

2.4.3 Identification and Authentication

The RTCA has two authentication mechanisms that are utilized to identify the authorized users. The first mechanism is the user id and password. The RTCA provides the interface to accept and performs the verification of the user id and password against the user account information stored in the database.

The second mechanism utilizes certificate based authentication. The certificate contains the user's public key. The RTCA verifies that the user also has the associated private key by issuing a standard SSL challenge to the user who must return a response encrypted with his private key. This mechanism is used in conjunction with the password mechanism. Upon successful verification, the user is permitted access to the administrative interfaces which are allowed by the user's assigned role(s).

2.4.4 Communication

The CoreStreet RTC VA has been designed to minimize the types of imported data. The description below identifies each of these data types:

- issuer registration data – these data include the issuer's common name, assigned OID and public certificate. It contains no unprotected security sensitive data. Registration of new issuers will be a relatively infrequent event and is a manual process governed by local policy and procedures.
- newly issued certificates – the integrity and authenticity of the data is protected by digital signature
- newly issued CRLs – the integrity and authenticity of the data is protected by digital signature
- certificate attribute changes (optional) – the integrity and authenticity of the data is protected by digital signature
- certificates of the attribute managing officers (optional) – used to authenticate and verify integrity of certificate attribute change requests
- trusted root certificates – the "trust anchors" that are used to authenticate certificates from entities outside the RTC VA

Specific note is made of the fact that the relying party applications and responders do not communicate directly with the RTCA. All data imported by the RTCA is of a specific predefined type and from authenticated sources.

2.4.5 Security Management

RTCA does not support the notion of untrusted users. Rather "users" are administrative personnel operating within a supported role. CoreStreet maintains three roles within the RTCA: Administrator, Officer, and Auditor.

1. Administrators – responsible for installing, configuring and upgrading the RTC Authority and RTC Responder software. This includes managing user accounts, certificate issuers, attribute mappings, data stores, key stores and scheduling jobs.
2. Officer – responsible for managing credential lifecycles. Officers register certificates with the Authority and manage CRLs.
3. Auditors – responsible for reviewing audit logs and security breaches.

2.4.6 TSF Protection

The RTCA ensures that security functions are not bypassed by the enforcement of the authentication mechanisms and limiting the access capability based on the administrative role assigned to the user interface.

The TSF information stored in the database is stored with a digital signature to ensure that any tampering of the information can be verified by the comparison of the stored digital signature with the generated signature.

3 TOE Security Environment

3.1 Secure Usage Assumptions

This section describes the security aspects of the environment in which the TOE will be utilized. This includes information about the physical, personnel, and system aspects of the environment.

3.1.1 Personnel Assumptions

A.Admin_competent	The administrative personnel are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the administrative guidance to competently administer the TOE.
A.User_policy_procedures	Authenticated users are familiar with the policy and procedures under which the TOE operates and notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
A.Env_admin	Access to the TOE operating environment will be limited to trusted environment System Administrators (superusers) only.

3.1.2 Physical Assumptions

A.Physical_protection	The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

3.1.3 System Assumptions

A.Time_source	A reliable time source is provided by the IT environment for use by the TOE.

3.2 Threats

This section lists security threats that the TOE and the TOE environment mitigates.

T.Access_masquerade	A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality or availability.
T.Audit_corrupt	Audit trail records of security events may be subjected to unauthorized modification or destruction by an unauthorized user.
T.Entry_unauthorized	An individual, other than an authenticated user, may

	gain unauthorized, malicious access to processing resources or information via an unsophisticated technical attack.
T.Message_denied	The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.
T.Physical	Security-critical parts of the system may be subjected to physical attack by a malicious user that may compromise security.

3.3 Organizational Security Policies

The organizational security policies discussed below are those associated with the mission of the TOE. The phrase "IT system", as used in this section, refers to both the IT environment and the TOE.

P.Access	The TOE restricts access of the administrative functions to the authorized users as defined security policy.
P.Accountability	Users must be held accountable for their security-relevant actions on the TOE.
P.Authorized_use	Organization's IT resources and information shall be used only for its authorized purpose(s).
P.Cryptography	FIPS-approved or NIST-recommended cryptographic functions shall be used to perform all cryptographic operations.
P.Known	Users of the TOE must be identified and authenticated before TOE access can be granted.
P.Manage	The TOE must provide authorized administrators with utilities to effectively manage the security-related functions of the system.
P.Mission	The TOE shall operate in a manner that meets its mission goals: • Maintain and distribute valid certificate status information for unexpired certificates. • Maintain and distribute valid certificate attribute status information for unexpired certificates.
P.Physical	The processing resources of the TOE that must be physically protected in order to ensure that security objectives are met, will be located within controlled access facilities that mitigate unauthorized, physical access.
P.Training	Authenticated users of the TOE must be adequately trained, enabling them to effectively implement

	organizational security policies with respect to their discretionary actions.

4 Security Objectives

4.1 Security Objectives for the Non-IT Environment

This section lists the security objectives for the non-IT environment that are not addressed by technical measures.

OE.Documentation	The TOE environment must deter authorized administrator's errors by providing adequate documentation and training on securely installing, configuring and operating the TOE.
OE.Env_admin	Access to the TOE operating environment will be limited to trusted environment System Administrators (superusers) only.
OE.Person	The TOE environment must ensure that the TOE is managed and administered in a manner that maintains IT security and is consistent with the organizational security policies by assigning competent authorized users.
OE.Physical	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security.
OE.Users_authorized_knowledgeable	The TOE environment must ensure that all system authorized users are familiar with the policy and procedures under which the TOE is operated and notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.

4.2 Security Objectives for the IT Environment

This section identifies the security objectives that are addressed by the IT environment in which the TOE will operate.

OE.Crypto_functions	The TOE environment must provide approved cryptographic algorithms for encryption/decryption, authentication, signature generation/verification, hashing and approved key generation and destruction techniques through the use of FIPS 140-1/FIPS 140-2 Level 3 validated or compliant cryptographic modules..
OE.Operating_environment	The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with and provides a time stamp to ensure that the sequencing of events can be verified.

4.3 Security Objectives for the TOE

This section identifies the security objectives for the TOE.

O.Access_limitation	The TOE must limit administrative functions so that Administrators, Officers and Auditors do not automatically have access to user objects, except as authorized.
O.Access_restrict	The TOE must restrict the actions a user may perform before the system authenticates the identity of the user.
O.Accountability	The TOE must ensure, for actions under its control or knowledge, that all users can subsequently be held accountable for their security relevant actions.
O.Audit_protection	The TOE must be able to prevent unauthorized access and detect modifications made to audit records to ensure accountability of user actions.
O.Authorized_users	The TOE must provide the ability to specify and manage user and system access rights to processing resources and data elements under its control, supporting the organization's security policy for access control.
O.Manage	The TOE must provide the tools that ensure that the TOE is managed and administered in a manner that maintains IT security by Administrators, Officers and Auditors.
O.Non_repudiation	The TOE must prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message.
O.Security_roles	The TOE must maintain security-relevant roles and the association of users with those roles.
O.Status_valid	The TOE must ensure that the certificate status information and attribute status information disseminated are valid.
O.Traffic	The TOE must protect itself from communication traffic from an unknown source (e.g., reroute or discard) to prevent potential damage to the RTC VA.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

This section of the ST details the security functional requirements (SFR) for the TOE. The SFRs are a combination of SFRs drawn from the CC Part 2 and the explicitly stated requirements that are used to model the certificate validation functions that that are not available in the CC.

The following table lists the security functional requirements for the TOE.

Table 1 – TOE Security Functional Requirements

Requirement Class	Requirement Component
Security Audit(FAU)	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
Communication (FCO)	FCO_NRO.2 – Enforced proof of origin
	FCO_NRO_X.3 – Advanced verification of origin
User Data Protection (FDP)	FDP_ACC.1 – Subset access control
	FDP_ACF.1 – Security attribute based access control
	FDP_ETC_X.3 – Integrity protection of exported data
	FDP_X_OCSP.1 – Basic OCSP response validation
Identification and Authentication (FIA)	FIA_AFL.1 - Authentication failure handling
	FIA_ATD.1 - User attributes definition
	FIA_UAU.2 – User authentication before any action
	FIA_UAU.5 – Multiple authentication mechanisms
	FIA_UID.2 – User identification before any action
	FMT_MSA.1 – Management of security attributes
	FMT_MSA.3 – Static attribute initialization
	FMT_MTD.1 – Management of TSF data
	FMT_SMF.1 – Specification of Management Functions
	FMT_SMR.1 – Security roles
Protection of the TSF (FPT)	FPT_RVM.1 – Non-bypassability of the TSP
	FPT_X_TSP.1 - Audit log signing event **and detection**

5.1.1 Security Audit

This section describes the TOE security requirements for the audit class of security requirements.

FAU_GEN.1 **Audit data generation**

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 events listed in Table 2 below**.] (per International Interpretation #202)

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, 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, [**login, message, host IP, and the information specified in the Additional Details column in Table 2 below**.]

Table 2 – Security Auditable Events for the TOE

Event Type	Description	Additional Details
ET-TOE-2	The manual processing of any CRL by an authorized user	
ET-TOE-3	The processing of any request to alter an attribute associated with a certificate	The following additional data shall be logged: identity of the officer making changes to the status, identity(serial #) of the certificate whose attribute(s) is being changed, attribute(s) being changed
ET-TOE-4	Registration of an Issuer	None
ET-TOE-5	Removal of a registered Issuer	None
ET-TOE-6	Requests for a new OCSP proof list	None
ET-TOE-8	Rejection of any imported data whose proof of origin cannot be verified, when the import process is initiated by a user.	None
ET-TOE-9	All attempts to login	None
ET-TOE-10	All modification of user accounts	None

FAU_GEN.2 **User identity association**

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 **Audit review**

FAU_SAR.1.1 The TSF shall provide [**Auditor**] with the capability to read [**all applicable information; date/time, subject identity, account, event type, outcome and the message**] from the audit records **located in the database**.

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

FAU_SAR.2 **Restricted audit review**

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

FAU_SAR.3(a) **Selectable audit review (Sorting)**

FAU_SAR.3(a).1 The TSF shall provide the ability to perform [***sorting***] of audit data based on [**date/time, login, subject identity, host IP, event type, outcome**].

FAU_SAR.3(b) **Selectable audit review (Searching)**

FAU_SAR.3(b).1 The TSF shall provide the ability to perform [***searches***] of audit data based on [**login, subject identity, event type, host IP, outcome, and/or message present in the database**].

5.1.2 Communication

This section describes the TOE security requirements for the communication class of security requirements.

FCO_NRO.2 **Enforced proof of origin**

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted [**certificate status information, Issuer registration information, CRLs and Certificates received from CAs**] at all times.

FCO_NRO.2.2 The TSF shall be able to relate the [**identity**] of the originator of the information, and the [**digital signature**] 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 [***recipient***] given [**the certificate of the originator**].

FCO_NRO_X.3 **Advanced verification of origin**

FCO_NRO_X.3.1 The TSF shall only accept the electronic data identified in FCO_NRO.2 if it has been signed using a FIPS approved digital signature algorithm.

5.1.3 User Data Protection

This section describes the TOE security requirements for the user data protection class of security requirements.

FDP_ACC.1 **Subset access control**

FDP_ACC.1.1 TSF shall enforce the [**User Access Control Policy**] on [
subjects: authorized users
operations: access to the management interfaces
objects: management interfaces
].

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

FDP_ACF.1.1 The TSF shall enforce the [**User Access Control Policy**] to objects based on the following: [

Subject: authorized users

- **Role**

Object: management interfaces

- **Role**

]. (per International Interpretation #103)

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

- **User with Administrator role will be granted access to interfaces applicable to Administrator,**
- **User with Auditor role will be granted access to interfaces applicable to Auditor,**
- **User with Officer role will be granted access to interfaces applicable to Officers**

].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**no other additional rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**no explicit denial rules**].

FDP_ETC_X.3 Integrity protection of exported data

FDP_ETC_X.3.1 OCSP certificate status data shall be protected against undetected modification through the use of digital signatures when exporting from the TOE.

FDP_ETC_X.3.2 miniCRLs shall be protected against undetected modification through the use of digital signatures when exporting from the TOE.

FDP_X_OCSP.1 Basic OCSP response validation

FDP_X_OCSP.1.1 The TSF shall verify that all mandatory fields in the OCSP basic response contain values in accordance with IETF RFC 2560. At a minimum, the following items shall be validated:

1. The 'version' field shall contain a **0**.
2. 'ResponderID' shall contain the subject of the certificate or the hash of the signer's public key.
3. The 'signatureAlgorithm' field shall contain the OID for a FIPS-approved digital signature algorithm.
4. The 'thisUpdate' field shall indicate the time at which the status being indicated is known to be correct.
5. The 'producedAt' field shall indicate the time at which the OCSP responder signed the response.
6. The time specified in the 'nextUpdate' field shall not precede the time specified in the 'thisUpdate' field.

5.1.4 Identification & Authentication

This section describes the TOE security requirements for the identification and authentication class of security requirements.

FIA_AFL.1 **Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when [**3**] unsuccessful authentication attempts occur related to [**user login within a specified time period**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**disable the user account for a set amount of time (default is 60 seconds)**].

FIA_ATD.1 **User attributes definition**

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user id, password, certificate, role(s)**].

FIA_UAU.2 **User authentication before any action**

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.

FIA_UAU.5 **Multiple authentication mechanisms**

FIA_UAU.5.1 The TSF shall provide [**Password Authentication, Certificate Authentication**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [

- **Password Authentication is always used;**
- **Certificate Authentication is used if the user account is configured with the user's certificate.**

].

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

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.1.5 Security Management

This section describes the TOE security requirements for the security management class of security requirements.

FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**User Access Control Policy**] to restrict the ability to [***modify,*** **assign**] the security attributes [**roles**] to [**Administrator**].

FMT_MSA.3 – Static attribute initialization

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

FMT_MSA.3.2 The TSF shall allow the [**Administrator**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1(a) – Management of TSF data (User Attributes)

FMT_MTD.1(a).1 The TSF shall restrict the ability to [***modify***] the [**user security attributes, other than password**] to [**Administrators**].

FMT_MTD.1(b) – Management of TSF data (Password)

FMT_MTD.1(b).1 The TSF shall restrict the ability to [***modify***] the [**password**] to [**Administrators and the user associated with the password**].

FMT_MTD.1(c) – Management of TSF data (Audit Records)

FMT_MTD.1(c).1 The TSF shall restrict the ability to [***query***, **sort**] the [**audit records located in the database**] to [**Auditor**].

FMT_SMF.1 – Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

Available to all authorized users:

- **modify user password.**

Restricted to the Administrator role:

- **create, delete and update user accounts;**
- **view, delete and register certificate issuer;**
- **configure, modify, delete data source;**
- **mange the key store;**
- **configure OCSP response and MiniCRL;**
- **view the system logs.**

Restricted to the Auditor Role:

- **view, search and sort the audit records;**
- **view, sort and filter the aggregated credential statuses.**

Restricted to the Officer Role:

- **view, query and register certificates;**
- **view, delete, register revocation list,;**
- **view, modify individual credential status.**

]. (per International Interpretation #65)

FMT_SMR.1 – Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [**Administrator, Officer, and Auditor**].

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

5.1.6 Protection of TSF

This section describes the TOE security requirements for the protection of the TSF class of security requirements.

FPT_RVM.1 - Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_X_TSP.1 - Audit log signing event and detection

FPT_X_TSP.1.1 The TSF shall create an audit log signing event in which it utilizes the IT environment to compute a digital signature comprised of each entry in the audit record.

FPT_X_TSP.1.2 The digital signature from the audit log signing event shall be included in the audit record.

FPT_X_TSP.1.3 The TSF shall be able to detect unauthorised modifications to the audit records in the audit trail.

5.2 Security Requirements for the IT Environment

This section lists the security functional requirements that the IT Environment must provide in order for the TOE to function properly and meet its security objectives. The SFRs are drawn CC Part 2

The following table lists the SFRs for the IT Environment. The SFRs address the dependency of the TOE requirements on the environment.

Table 3 – IT Environment Security Functional Requirements

Requirement Class	Requirement Component
Cryptographic Support (FCS)	FCS_CKM.1 – Cryptographic key generation
	FCS_CKM.4 – Cryptographic key destruction
	FCS_COP.1 – Cryptographic operation
Protection of the TSF (FPT)	FPT_SEP.1 – TSF domain separation
	FPT_STM.1 – Reliable time stamps

5.2.1 Cryptographic Support

This section describes the IT environment security requirements for the cryptographic support class of security requirements.

FCS_CKM.1 **Cryptographic key generation**

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**FIPS Compliant cryptographic key generation algorithm**] and specified cryptographic key sizes [**applicable FIPS compliant cryptographic key sizes**] that meet the following: [**FIPS 140-1 or FIPS 140-2 Level 3**].

FCS_CKM.4 **Cryptographic key destruction**

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**cryptographic key zeroization method**] that meets the following: [**FIPS 140-1 or FIPS 140-2 Level** 3].

FCS_COP.1 **Cryptographic operation**

FCS_COP.1.1 The TSF shall perform [**encryption, digital signature generation, digital signature verification**] in accordance with a specified cryptographic algorithm [**FIPS compliant cryptographic algorithm**] and cryptographic key sizes [**applicable FIPS compliant cryptographic key sizes**] that meet the following: [**FIPS 140-1 or FIPS 140-2 Level 3**].

5.2.2 Protection of TSF

This section describes the IT environment security requirements for the protection of the TSF class of security requirements.

FPT_SEP.1 **TSF domain separation**

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 (EAL3) augmented with ALC_FLR.1 components as specified in Part 3 of the Common Criteria and are shown in Table 4.

Table 4 – Evaluation Assurance Requirements for EAL3 augmented

Assurance Class	Component ID	Component Title
Configuration Management (ACM)	ACM_CAP.3	Authorization controls
	ACM_SCP.1	TOE CM coverage
Delivery & Operation (ADO)	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle Support (ALC)	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Basic flaw remediation
Tests (ATE)	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment (AVA)	AVA_MSU.1	Examination of guidance
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.3.1 Configuration Management (ACM)

ACM_CAP.3 Authorization controls

Developer action elements:

ACM_CAP.3.1D The developer shall provide a reference for the TOE.

ACM_CAP.3.2D The developer shall use a CM system.

ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labeled with its reference.

ACM_CAP.3.3C The CM documentation shall include a configurations list and a CM plan.

ACM_CAP.new **The configuration list shall uniquely identify all configuration items that comprise the TOE.** (per International Interpretation #3)

ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.3.7C The CM plan shall describe how the CM system is used.

ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

Evaluator action elements:

ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.1 TOE CM coverage

Developer action elements:

ACM_SCP.1.1D The developer shall provide **a list of configuration items for the TOE**. (per International Interpretation #4).

Content and presentation of evidence elements:

ACM_SCP.1.1C **The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST**. (per International Interpretation #4)

ACM_SCP.1.2C (this element has been deleted per International Interpretation #4)

Evaluator action elements:

ACM_SCP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2 Delivery and operation (ADO)

ADO_DEL.1 Delivery procedures

Developer action elements:

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation and start-up procedures

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The **installation, generation and start-up** documentation shall describe **all** the steps necessary for secure installation, generation and start-up of the TOE. (per International Interpretation #51 (rev 1))

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.3.3 Development (ADV)

ADV_FSP.1 Informal functional specification

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.2 Security enforcing high-level design

Developer action elements:

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF..

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method or use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

Evaluator action elements:

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal correspondence demonstration

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representation that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Guidance documents (AGD)

AGD_ADM.1 Administrator guidance

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User guidance

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of the user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.5 Life cycle support (ALC)

ALC_DVS.1 Identification of security measures

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ALC_FLR.1 Basic flaw remediation

Developer action elements:

ALC_FLR.1.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

Content and presentation of evidence elements:

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

Evaluator action elements:

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.6 Tests (ATE)

ATE_COV.2 Analysis of Coverage

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator action elements:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Testing: high-level design

Developer action elements:

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

Evaluator action elements:

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing _ sample

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

5.3.7 Vulnerability assessment (AVA)

AVA_MSU.1 Examination of guidance

Developer action elements:

AVA_MSU.1.1D The developer shall provide guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.1.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

Evaluator action elements:

AVA_MSU.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

AVA_SOF.1 Strength of TOE security function evaluation

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct

AVA_VLA.1 Developer vulnerability analysis

Developer action elements:

AVA_VLA.1.1D **The developer shall perform a vulnerability analysis.** (per International Interpretation #51 (rev 1))

AVA_VLA.1.2D **The developer shall provide vulnerability analysis documentation.** (per International Interpretation #51 (rev 1))

Content and presentation of evidence elements:

AVA_VLA.1.1C **The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.** (per International Interpretation #51 (rev 1))

AVA_VLA.1.2C **The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.** (per International Interpretation #51 (rev 1))

AVA_VLA.1.3C **The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. (**per International Interpretation #51 (rev 1))

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

6 TOE Summary Specification

This section defines the instantiation of the security requirements for the TOE being evaluated. It provides a description of the implemented security functions and assurance measures that are intended to meet the TOE security requirements.

6.1 TOE Security Functions

6.1.1 Audit Function

The TOE generates audit records that track the authorized users actions on the TOE and the actions of the system. The audit records of the authorized users are generated by the RTCA application, digitally signed and stored in the database. Audit records of the system are logged in system logs. The database and the system log are stored in separate locations and protected by the environment.

The audit records, stored in the database, are generated for the following actions:

- All modification to the user accounts, including the roles;
- All attempts to log into the TOE;
- The registration and removal of Issuers(CA);
- All requests to modify the attributes associated with certificates;
- All manual uploads of CRLs and manual requests for export of OCSP proof lists and miniCRLs;
- Rejection of invalid imports of data, initiated by a user.

The audit records are generate with the following attributes; timestamp (date and time of event), unique ID, OS Login, Account Login(subject identity), Target Account, Target Certificate, Target attribute, action – code (type of event), results(outcome), message (details about the action taken) and digital signature. Each audit record is associated to the user that caused the generation of the record.

The actions performed by the system and are logged in the system log are as follows:

- The startup and shutdown of the audit function occurs automatically with the startup and shutdown of the TOE. An administrator of the TOE cannot startup or shutdown the audit function independent of the entire TOE.
- Rejection of invalid imports of data, imported automatically;
- The automatic request for a new OCSP list.

(FAU_GEN.1, FAU_GEN.2)

The TOE provides a web-based interface that allows the Auditor to view the most recent audit records in a table-like format stored in the database. The Auditor is provided in a readable format the creation date (date/time), login, account (subject identity), host IP, action (event type), results (outcome) and/or message. The Auditor is able to sort the records by clicking on the header of a column. The information is sorted in either ascending or descending order. The Auditor is able to sort the records by the creation date, login, account, host IP, action and/or result. The interface allows the Auditor to search the audit records by audit records attribute and entry of a search string. Then resulting listing will only have records that contain the search string within the selected attribute. (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3(a), FAU_SAR.3(b))

The system logs are viewable by the Administrator. The TOE provides an interface that allows the Administrator to view the records in the syslog. The records list the date/time of the event, the event level, the source of the event, the message and the any exception that may have occurred.

6.1.2 Communication

The RTCA imports CRLs from the Issuers which contain certificate status information, certificates, and Issuer registration information. The RTCA verifies the originator of the imported data against the Issuer's certificate stored in the environment. The RTCA verifies that the imported data was signed by a valid CA before importing into the RTCA. If RTCA is unable to verify the signature, the imported data is rejected.
The TOE exports OCSP proof lists signed with the TOE's certificate. The miniCRL segments also include digital signatures. (FCO_NRO.2, FCO_NRO_X.3)

6.1.3 Identification and Authentication

The RTCA maintains an account for each user that includes a user id, password, and role(s) and can include the user's certificate if required. (FIA_ATD.1) The user account information is stored in the database located in the environment.

The RTCA enforces two types of authentication mechanisms; user id/password mechanism and the combination of user id/password and certificate.

The user id/password is the traditional identification and authentication mechanism. The TOE provides a login interface where the user enters their username and password. The TOE queries the database for the user's id and password and using the information provided from the database determines if the data entered matches what is stored in the database. If the verification is successful the user is granted access to the management interfaces that are associated with the assigned role(s), otherwise access is denied.

The user id/password and certificate mechanism uses the public key in the user's certificate in conjunction with the user's id and password. When user is configured with their certificate, they are required to authenticate using both their certificate and their user name and password. The mechanism verifies the public key of the user against the use's private key, in addition to the verification of the user id/ password. The certificate verification is done using a key challenge within the SSL communication with the management interfaces of the TOE. Upon successful verification of the certificate and the user name/password the TOE is accessible, otherwise access is denied.

The two mechanisms do not allow for any TSF-mediated action prior to successful verification. (FIA_UID.2, FIA_UAU.2, FIA_UAU.5)

The RTCA limits the number of times that a user can attempt to login, unsuccessfully. When the attempts threshold is reached (default is 3 attempts) within a specified window of time (the default is 60 seconds) the user account is disabled for a set amount of time (same default of 60 seconds). The user will have to wait for the set time before they can attempt to log in again. (FIA_AFL.1) The default attempts and the default lock out time are pre-set. The default values may be set to different values during the installation of the TOE.

6.1.4 User Data Protection

The TOE enforces a User Access Control Policy to control access to web-based management interfaces. Access to the management functions are restricted based on the administrative role associated to the authorized user. The management functions are only accessible via the management interfaces. (FDP_ACC.1, FDP_ACF.1)

The TOE defines security functions to protect the certification status and validation data when it is exported from the RTCA and when it is stored in the environment.

The OCSP proof lists are structured in accordance with IETF as RFC 2560, the OCSP standard, which ensures that the proof lists includes the version of the response, the names of the RTCA, the signature algorithm OID, the start and end time of the proof list, the time that list was signed, any associated attributes and the digital signature. (FDP_X_OCSP.1)

Each OCSP proof list exported from the RTCA includes a digital signature to protect the list. The digital signatures are utilized for verification by the RTCR and relying party applications that request certificate status information from the TOE. Any modification of the proof lists results in an invalid verification of the associated digital signature and a rejection of the response by the relying party application and the rejection of the list by the RTCR. (FDP_ETC_X.3)

Similarly, each miniCRL exported from the RTCA includes a digital signature to protect their integrity and to provide a means for verifying their authenticity. The structure of the miniCRLs is CoreStreet proprietary.

6.1.5 Security Management

The RTCA defines three administrative roles which can be assigned to an authorized user. The roles are Administrator, Officer and Auditor. These roles define what management interfaces are available to an authorized user. A user can be assigned to one or more roles.
The roles are associated with the following capabilities:

- Administrator – this role is capable of managing user accounts, CAs that will communicate with the RTCA (i.e., certificate issuers), the data sources, the key store, configuring the OCSP and Mini CRLs proof lists, and viewing the system logs.
- Auditor – only this role is capable of viewing, searching and sorting the audit records stored in the database, and viewing, sorting and filtering the aggregate of the credential statuses received from the CA.
- Officer – only this role is capable of viewing, querying and registering certificates for the TOE. These include the certificates of CAs, and certificates of the users of the TOE, viewing, deleting and registering the CRLs received from the CAs. Additionally, the role is able to view and modify the individual certificate and attribute statuses.

All the authorized users are capable of modifying their own passwords. (FMT_SMR.1, FMT_MTD.1(a), FMT_MTD.1(b), FMT_MTD.1(c))

The RTCA provides management interfaces to perform the indicated management functions. The interfaces are only accessible by the authorized user associated with the appropriate role. (FMT_SMF.1)

By default all new user accounts are not assigned a role, if not specified by the Administrator. The only interface accessible to an authorized user not associated to a role is the interface to modify their password. (FMT_MSA.1, FMT_MSA.3)

6.1.6 TSF Protection

The management interfaces are restricted to the authorized users with assigned role(s). The TOE enforces the User Access Control Policy by only displaying the options that are available to role associated to the user. If the user is not assigned a role, the TOE management function displayed is the option to change the user password. (FPT_RVM.1)

The TOE utilizes the associated digital signatures to detect any modifications to the audit records stored in the database. The TOE utilizes the security module to generate a digital signature that is assigns to the audit record as it is stored in the database. Upon retrieval of the audit records, the digital signature is verified by the TOE, by resending the audit record to the security module to re-generate the digital signature. Any modifications to the record will result in the creation of a different digital signature and the verification will fail. The TOE will generate an audit record to detail the modification of the record. (FPT_X_TSP.1)

6.2 Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL3 assurance requirements:

- Process Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

6.2.1 Process Assurance

6.2.1.1 Configuration Management

The configuration management measures applied by CoreStreet ensure that configuration items and the TOE are uniquely identified, and that the documented procedures are used to control and track changes to the configuration items. CoreStreet ensures changes to the configuration item are properly controlled.
The documentation includes the list of the configuration items, describes the method for uniquely identifying the configuration items and the TOE, and describes the procedures used to control and track the changes to the items.
The configuration items under CM control are the TOE implementation representation, design documentation, tests, user and administrator guidance, installation and delivery guidance, lifecycle documentation, vulnerability assessment, and the CM documentation.

The configuration management measures are documented in:

- Development Environment and Procedures, rev 1.11, 23 June 2004.

The configuration management documentation satisfies the following requirements:

- ACM_CAP.3;
- ACM_SCP.1.

6.2.1.2 Life Cycle Support

The lifecycle documentation describes the adequacy of the procedures used during the development and maintenance of the TOE through the use of a comprehensive life-cycle management plan.

The documentation describes the physical, procedural, personnel, and other development security measures that are used in the development environment to protect the TOE. It includes the physical security of the development location and any procedures used to select development staff.

CoreStreet defines and document in the lifecycle document the procedures used to track all security flaws, to identify the corrective actions and the methods for reporting the security flaw and the corrective actions to the TOE users. The lifecycle support is documented in:

- Life Cycle Support, rev 1.12

This measure satisfies the following requirements:
- ALC_DVS.1;
- ALC_FLR.1.

6.2.2 Delivery and Guidance

6.2.2.1 Delivery and Installation

CoreStreet provides documentation that explains how the TOE is delivered, the carriers utilized and the procedures that are able to maintain security when distributed. CoreStreet's installation procedures describe the steps used for the secure installation, generation, and start-up of the TOE along with configuration settings to secure the TOE privileges and functions.

The delivery process is documented in the Life Cycle Support document and the installation, start-up and generation procedures are documented in the following:

- RTC Authority Administration Guide Version 4.0;
- RTC Authority User Guide Version 4.0;
- RTC Responder Administration Guide Version 4.0;
- CoreStreet RTC Authority Version 4.0 Release Notes.

The delivery and installation documentation satisfies the following assurance requirements:
- ADO_DEL.1;
- ADO_IGS.1.

6.2.2.2 Administrative and User Guidance

CoreStreet provides administrator guidance on how to utilize the TOE security functions, and warnings to authorized administrators about actions that can compromise the security of the TOE.

The procedures included in the administrator guidance describe the steps necessary to operate TOE in accordance with the evaluated configuration, detailing how to establish and maintain the secure configuration.

The only users of the TOE are administrators, auditors and officers, thus only administrator guidance is provided. The administrator guidance is documented in:

- RTC Authority Administration Guide Version 4.0;
- RTC Authority User Guide Version 4.0;
- RTC Responder Administration Guide Version 4.0;
- CoreStreet RTC Authority Version 4.0 Release Notes.

The administrator's guide satisfies the following assurance requirements:

- AGD_ADM.1;
- AGD_USR.1.

6.2.3 Design Documentation

The design documentation, Design and Architecture CoreStreet RTC Validation Authority includes a description of the aspects of the TOE security design, architecture and interfaces. The design documentation consists of the following:

- Functional Specification – provides a description of the interfaces, detailing the purpose, effects, exceptions and error messages, as applicable, for each interface of the TOE.
- High-Level Design – provides a high level description of the TOE, its security functions provided by the subsystems, describes the interfaces to the subsystems in terms of the purpose, parameters, effects, exceptions and error messages, and identifies the underlying hardware, firmware and/or software required by the TOE.
- Representation Correspondence – provides an analysis of correspondence between the security functions and requirements to the descriptions provide in the design documentation.

The Design and Architecture document satisfies the following security assurance requirement:

- ADV_FSP.1;
- ADV_HLD.2; and,
- ADV_RCR.1.

6.2.4 Tests

The test documentation has been created to demonstrate appropriate breadth and depth of coverage. The test documentation describes how all security relevant functions are tested. The test documentation includes test cases and variations necessary to demonstrate that all security checks and effects related to the interfaces are correctly implemented. The test documentation provides correspondence between the security-relevant interfaces and applicable tests and test variations. The test documentation describes the procedures to successfully execute the tests, and expected results of the tests. The test documentation also includes results in the form of logs resulting from completely exercising all of the security test procedures.
The test documentation consists of the following:

- RTC Validation Authority Test Plan, rev 1.15;
- RTC Validation Authority Test Procedures, rev 1.17.

The test documentation satisfies the following assurance requirements:

- ATE_COV.2;
- ATE_DPT.1;
- ATE_FUN.1;
- ATE_IND.2.

6.2.5 Vulnerability Assessment

The administrator guidance documentation describes the operation of the TOE and how to maintain a secure state. The administrator guide also describes all operating assumptions and security requirements outside the scope of control of the TOE. The administrator guidance documentation has been developed to serve as a complete, clear, consistent, and reasonable administrator reference.

The strength of TOE security function analysis demonstrates that the SOF claims made in the ST for all probabilistic or permutation mechanisms are correct. CoreStreet performs vulnerability analyses of the TOE to identify weaknesses that can be exploited in the TOE. CoreStreet documents the status of identified vulnerabilities and demonstrates that for each vulnerability the vulnerability cannot be exploited in the intended environment and that the TOE is resistant to obvious penetration attacks.
The vulnerability analysis is documented in:

- CoreStreet RTC Validation Authority Vulnerability Analysis, v1.0.

The vulnerability analysis document satisfies the following assurance requirements:

- AVA_MUS.1;
- AVA_SOF.1;
- AVA_VLA.1.

7 Protection Profile Claims

A Protection Profile for this product does not exist. The TOE does not claim conformance to a Protection Profile.

8 Rationale

This section provides the following information:

1. rationale for why the identified security objectives provide effective countermeasures for the listed threats
2. rationale for why the identified security objectives provide complete coverage of the organizational security policy
3. rationale for why the identified security objectives uphold each assumption

8.1 Security Objective Rationale

8.1.1 Threats to Security Objective Rationale

This section demonstrates how the security objectives of the TOE and its environments are sufficient for countering and mitigating the threats identified in the Security Target.

Table 5 – Threats to Security Objectives

Threats	Security Objectives
T.Access_masquerade	O.Access_restrict O.Traffic OE.Physical
T.Audit_corrupt	O.Audit_protection OE.Physical
T.Entry_unauthorized	O.Access_restrict O.Traffic OE.Physical
T.Message_denied	O.Non_repudiation
T.Physical	OE.Physical

T.Access_masquerade

A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality or availability.

This threat is countered by

- **O.Access_restrict** the system restricts the actions a user may perform prior to the user being identified and authenticated. This will reduce unauthorized access to system audit functions and resources.
- **OE.Physical** which protects the system through the use of physical access control to the area where security critical parts of the system are deployed. This keeps unauthorized personnel out of areas where they could pose a threat.
- **O.Traffic** ensures that communication traffic from an unknown source is controlled (e.g., rerouted or discarded) to prevent potential damage. This threat is extremely small since the TOE environment will not allow external traffic into the TOE that is not initiated by the TOE.

T.Audit_corrupt

Audit trail records of security events may be subjected to unauthorized modification or destruction by an unauthorized user.

This threat is countered by

- **O.Audit_protection** ensures that any unauthorized access, modification or deletion to audit records are detected.
- **OE.Physical** which protects the TOE through the use of physical access control to the rea where security critical parts of the system are deployed. This keeps unauthorized personnel out of areas where they could pose a physical threat.

T.Entry_unauthorized

An individual, other than an authenticated user, may gain unauthorized, malicious access to TOE controlled processing resources or information via an unsophisticated technical attack.

The TOE has no external authorized users, only internal administrative staff. This threat is countered by restricting access both physically and logically. Specifically this threat is countered by

- **O.Access_restrict** the system restricts the actions a user may perform prior to the user being identified and authenticated. This will reduce unauthorized access to system audit functions and resources.
- **OE.Physical** which protects the system through the use of physical access control to the area where security critical parts of the system are deployed. This keeps unauthorized personnel out of areas where they could pose a threat.
- **O.Traffic** ensures that communication traffic from an unknown source is controlled (e.g., rerouted or discarded) to prevent potential damage. This threat is extremely small since the TOE environment will not allow external traffic into the TOE that is not initiated by the TOE.

T.Message_denied

The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.

This threat is countered by

- **O.Non_repudiation** ensures that all security relevant data imported into the TOE is digitally signed to provide evidence that of the originator of the data.

T.Physical

Security-critical parts of the system may be subjected to a physical attack that may compromise security.

This threat is countered by

- **OE.Physical** which protects the system through the use of physical access control to the area where security critical parts of the system are deployed. This keeps unauthorized personnel out of areas where they could pose a physical threat.

8.1.2 Assumptions to Security Objective Rationale

This section demonstrates how the security objectives for the IT Environment are sufficient to adequately address the assumptions described in this Security Target.

Table 6 – Assumptions to Security Objectives

Assumptions	Security Objectives
A.Admin_competent	OE.Person
A.Env_admin	OE.Env_admin
A.Physical_protection	OE.Physical
A.Time_source	OE.Operating_environment
A.User_policy_procedures	OE.Users_authorized_knowledgeable

A.Admin_competent

The administrative personnel are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the administrative guidance to competently administer the TOE.

This assumption establishes that the security of the system is dependent upon those who operate it.

This assumption is addressed by

- **OE.Person** which ensures that competent administrators are assigned to operate the system.

A.Env_admin

Access to the TOE operating environment will be limited to trusted environment System Administrators (superusers) only.

This assumption establishes access the operating system is restricted to the superusers.

This assumption is addressed by

- **OE.Env_admin** which ensures that operating system of the TOE is restricted to superusers.

A.Physical_protection

The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

This assumption establishes that physical modification of the TOE software will compromise the system security.

This assumption is addressed by

- **OE.Physical** ensures that TOE and its IT environment are housed in a physically protected environment to prevent access to unauthorized individuals.

A.Time_source

A reliable time source is provided by the IT environment for use by the TOE.

This assumption establishes that a reliable time-source is crucial to the success of the RTC VA mission. Without such a time source the period of validity of the published status information will be incorrect and potentially rendering the status information useless.

This assumption is addressed by

- **OE.Operating_Environment** ensures that IT environment provides a timestamp for use by the TOE.

A.User_policy_procedures

Authenticated users are familiar with the policy and procedures under which the TOE operates and notify proper authorities of a security issues that impact their systems to minimize the potential for the loss or compromise of data.

This assumption establishes that a thorough understanding by the authenticated users of the environment under which the RTC VA operates is essential to ensuring the secure operation of the system.

This assumption is addressed by

- **OE.Users_authorized_knowledgeable** which ensures that the Administrators, Officers and Auditors are familiar with the policy under which the TOE is operated and will notify the proper authorities of any security-related issues that impact the TOE to minimize the potential for the loss or compromise of data.

8.1.3 Organizational Security Policies to Security Objective Rationale

This section provides the justification of how the organizational security policies identified in the Security Target are enforced by the security objectives of the TOE and its IT Environment

Table 7 – Organizational Security Policies to Security Objectives

Organizational Security Policies	Security Objectives
P.Access	O.Access_limitation O.Access_restrict O.Security_roles
P.Accountability	O.Accountability
P.Authorized_use	O.Access_restrict O.Authorized_users O.Security_roles
P.Cryptography	OE.Crypto_functions
P.Known	O.Access_restrict
P.Manage	O.Manage
P.Mission	O.Status_valid
P.Physical	OE.Physical
P.Training	OE.Documentation

P.Access

The system restricts access to the administrative functions to the authorized user as defined security policy.

This security policy is met by

- **O.Access_limitation** limits administrative functions to those necessary for administrative users to carry out their assigned responsibilities. This reduces unauthorized access to system functions and resources.
- **O.Access_restrict** the system restricts the actions a user may perform prior to the user being identified and authenticated. This will reduce unauthorized access to system audit functions and resources.
- **O.Security_roles** maintains the association of users with security-relevant roles and responsibilities. When used in conjunction with restricted user access to system functions, this reduces unauthorized access to system audit functions and resources.

P.Accountability

Users must be held accountable for their security-relevant actions on the TOE.

This security policy is met by

- **O.Accountability** holds authorized users accountable for their actions through the auditing of security relevant events. The audit records will expose those that abuse their rights and privileges in terms of system operation.

P.Authorized_use

The organization's resources and information shall be used only for its authorized purpose(s).

This security policy is met by

- **O.Access_restrict** ensures the system restricts the actions a user may perform prior to the user being identified and authenticated. This will reduce unauthorized access to system audit functions and resources.
- **O.Security_roles** maintains the association of users with security-relevant roles and responsibilities. When used in conjunction with restricted user access to system functions, this reduces unauthorized access to system audit functions and resources.
- **O.Authorized_users** provides the assurance that the system manages and enforces users and system process access control rights and protections in accordance with the organization's security policy**.**

P.Cryptography

FIPS-approved or NIST-recommended cryptographic functions shall be used to perform all cryptographic operations.

This security policy is met by

- **OE.Crypto_functions** which ensures the use of validated FIPS 140-1 or FIPS 140-2 Level 3 security module devices to perform all security sensitive cryptographic functions. Validated security modules also ensure that cryptographic keys are adequately protected when they are stored within the security module.

P.Known

Users of the TOE must be identified and authenticated before TOE access can be granted.

This security policy is met by

- **O.Access_restrict** the system restricts the actions a user may perform prior to the user being identified and authenticated. This will reduce unauthorized access to system audit functions and resources.

P.Manage

The TOE must provide authorized administrators with utilities to effectively manage the security-related functions of the system.

This security policy is met by

- O.Manage provides the authorized administrators with the tools manage the TOE and its functions.

P.Mission

The TOE shall operate in a manner that meets its mission goals:

- *Maintain and distribute valid certificate status information for unexpired certificates.*
- *Maintain and distribute valid certificate attribute status information for unexpired certificates.*

This security policy is met by

- **O.Status_valid** ensures that certificate and attribute status information published by the RTC VA are valid at the time of publishing.

P.Physical

The processing resources of the TOE must be physically protected in order to ensure that security objectives are met.

This security policy is met by

- **OE.Physical** which protects the system through the use of physical access control to the area where security critical parts of the system are deployed. This keeps unauthorized personnel out of areas where they could pose a physical threat.

P.Training

Authenticated users of the system must be adequately trained, enabling them to effectively implement organizational security policies with respect to their discretionary actions.

This security policy is met by

- **OE.Documentation** provides administrative users with information and training on how to install, configure and operate the system in a manner that maintains the system's security, thus reducing the likelihood of errors.

8.2 Security Requirements Rationale

8.2.1 Security Functional Requirements Rationale

All security functional requirements (SFR) for the TOE identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

Table 8 – Security Objective of the TOE vs. Security Functional Requirement

Security Objectives	Security Functional Requirement
O.Access_Limitation	FDP_ACC.1 FDP_ACF.1 FPT_RVM.1
O.Access_Restrict	FIA_AFL.1 FIA_ATD.1 FIA_UAU.2 FIA_UAU.5 FIA_UID.2
O.Accountability	FAU_GEN.1 FAU_GEN.2
O.Audit_Protection	FDP_ACC.1 FDP_ACF.1 FPT_X_TSP.1
O.Authorized_Users	FMT_MTD.1(a) FMT_MTD.1(b) FMT_SMF.1 FMT_SMR.1
O.Manage	FAU_SAR.1 FAU_SAR.2 FAU_SAR.3(a) FAU_SAR.3(b) FMT_MSA.1 FMT_MSA.3 FMT_MTD.1(a) FMT_MTD.1(b) FMT_MTD.1(c) FMT_SMF.1 FMT_SMR.1
O.Non_Repudiation	FCO_NRO.2 FCO_NRO_X.3
O.Security_Roles	FMT_SMR.1
O.Status_Valid	FCO_NRO_X.3 FDP_ETC_X.3 FDP_X_OCSP.1
O.Traffic	FCO_NRO_X.3

O.Access_Limitation

The TOE must limit administrative functions so that Administrators, Officers and Auditors do not automatically have access to user objects, except as authorized.

This security objective is met by:

- FDP_ACC.1 enforces the User Access Control Policy to restrict the access to the management function interfaces.
- FDP_ACF.1 enforces the User Access Control Policy to restrict specific TOE management function interferes to specific management roles.

- FPT_RVM.1 ensures that access to the interfaces only occurs after the successful authentication into the TOE and then that only interfaces applicable to the role assigned to the user are accessible.

O.Access_Restrict

The TOE must restrict the actions a user may perform before the system authenticates the identity of the user.

This security objective is met by:

- FIA_UID.2 ensures the user is identified before any access to the TOE is permitted.
- FIA_UAU.2 and FIA_UAU.5 ensure the user is successfully authenticated before access to the TOE is permitted.
- FIA_ATD.1 maintains the security attributes which will be used to identify and authenticate the users.
- FIA_AFL.1 ensures that accounts of user who makes a number of unsuccessful attempts to logon are disabled for a set amount of time.

O.Accountability

The TOE must ensure, for actions under its control or knowledge, that all users can subsequently be held accountable for their security relevant actions.

This security objective is met by:

- FAU_GEN.1 generates audit records of the security relevant actions of the authorized users and the system.
- FAU_GEN.2 ensures the user responsible for the security-relevant action is held accountable by associating the user to the resultant audit record.

O.Audit_Protection

The TOE must be able to prevent unauthorized access and detect modifications made to audit records to ensure accountability of user actions.

This security objective is met by:

- FDP_ACC.1 and FDP_ACF.1 enforce the User Access Control Policy to restrict access to the audit records and system logs to specific roles by restricting the access the management interfaces used to access the records.
- FPT_X_TSP.1 ensures the TOE is able to detect any modification made to the audit records.

O.Authorized_Users

The TOE must provide the ability to specify and manage user and system access rights to processing resources and data elements under its control, supporting the organization's security policy for access control.

This security objective is met by:

- FMT_MTD.1(a) and FMT_MTD.1(b) restrict the management functions that modify user attributes to the Administrator.
- FMT_SMF.1 ensures the TOE provides the management interface for the Administrator to use to manage the user attributes.
- FMT_SMR.1 defines the administrative roles that will have access to the management interfaces and the associated functions.

O.Manage

The TOE must provides the tools that ensure that the TOE is managed and administered in a manner that maintains IT security by Administrators, Officers and Auditors.

This security objective is met by:

- FAU_SAR.1, FAU_SAR.2, FAU_SAR.3(a) and FAU_SAR.3(b) provide the Auditor with the ability review the audit records for any security related violations.
- FMT_MSA.1 and FMT_MSA.3 restrict the alteration of the initial user role, the assignment and the modification of a user's role(s) to the Administrator respectively
- FMT_MTD.1(a), FMT.MTD.1b, and FMT_MTD.1(c) restrict the ability to manage the user attributes and the audit records to the appropriate authorized administrative user.
- FMT_SMF.1 ensures the TOE provides the management interfaces that will be used by a specific administrative user to perform specific management functions.
- FMT_SMR.1 defines the administrative users of the TOE and ensures they are associated to a user.

O.Non_Repudiation

The TOE must prevent user from avoiding accountability for sending a message by providing evidence that the user sent the message.

This security objective is met by:

- FCO_NRO.2 ensures the originator of the information is held accountable for sending the data with the verification of the receipt with the use of the originator's certificate.
- FCO_NRO_X.3 ensures the TOE only accepts information that has been signed by the originator.

O.Security_Roles

The TOE must maintain security-relevant roles and the association of users with those roles.

This security objective is met by:

- FMT_SMR.1 defines the administrative roles of the TOE and associates each role to a user.

O.Status_Valid

The TOE must ensure that the certificate status information and attribute status information disseminated are valid.

This security objective is met by:

- FCO_NRO_X.3 ensures the TOE only accepts certificate information and attribute information that have been protected by a digital signature ensuring the information received is valid.
- FDP_ETC_X.3 ensures that OCSP proof list and the miniCRL are exported from the RTCA to the RTCR with a digital signature to protect the list from undetected modifications.
- FDP_X_OCSP.1 ensures the TOE exports valid OCSP proof by formatting the proof lists to contain values in accordance with IETF RFC 2560.

O.Traffic

The TOE must protect itself from communication traffic from an unknown source (e.g., reroute or discard) to prevent potential damage to the RTC VA.

This security objective is met by:

- FCO_NRO_X.3 ensures that only certificate information received by the TOE is digital signed with a verifiable certificate.

8.2.2 IT Environment Security Functional Requirements Rationale

All security functional requirements (SFR) applied to the IT Environment identified in this Security Target are fully addressed in this section and each SFR is mapped to the security objective of the IT Environment for which it is intended to satisfy.

Table 9 – Security Objective of IT Environment vs. Security Functional Requirements

Security Objectives	Security Functional Requirement
OE.Crypto_Functions	FCS_CKM.1 FCS_CKM.4 FCS_COP.1
OE.Operating_Environment	FPT_SEP.1 FPT_STM.1

OE.Crypto_Functions

The TOE environment must provide approved cryptographic algorithms for encryption/decryption, authentication, signature generation/verification, hashing and approved key generation and destruction techniques through the use of FIPS 140-1/FIPS 140-2 validated or compliant cryptographic modules.

This security objective is met by:

- FCS_CKM.1, FCS_CKM.4, and FCS_COP.1 ensure the TOE environment provides a security module to perform the cryptographic functions required by the TOE in accordance with FIP 140-1/FIPS 140-2 standard.

OE.Operating_Environment

The TOE operating environment shall provide mechanisms to isolate the TOE Security Functions (TSF) and assure that TSF components cannot be tampered with and provides a time stamp to ensure that the sequencing of events can be verified.

This security objective is met by:

- FPT_SEP.1 ensures the TOE environment provides mechanisms to isolate the TOE to ensure that the TOE is protected from external tampering.
- FPT_STM.1 ensures the TOE environment provides a reliable timing mechanism which will be used by the TOE to time stamp the audit records and the proof lists.

8.2.3 Security Functional Requirements Dependency Rationale

The dependencies of the TOE security functional requirements are met through the functionality of the TOE and/or by the security functionality of the IT environment.

Table 10 - Security Functional Requirements Dependencies maps the TOE security functional requirements to the corresponding requirements they are dependent on, demonstrating that all TOE security functional requirement dependencies are met within the ST.
Note: the table below assumes the requirement iterations have the same dependencies and therefore the iterations are not individually identified in the table (e.g. FMT_MTD.1(a)).

Table 10 – Security Functional Requirement Dependencies

Dependency / Functional Requirements	FAU_GEN.1	FAU_SAR.1	FCO_NRO.2	FCS_COP.1	FDP_ACC.1	FDP_ACF.1	FIA_UAU.2	FIA_UID.2	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FAU_GEN.1														X
FAU_GEN.2	X							X						
FAU_SAR.1	X													
FAU_SAR.2		X												
FAU_SAR.3		X												
FCO_NRO.2								X						
FCO_NRO_X.3			X											
FDP_ACC.1						X								
FDP_ACF.1					X					X				
FDP_ETC_X.3				X										
FDP_X_OCSP.1				X										
FIA_AFL.1								X						
FIA_UAU.2								X						
FMT_MSA.1					X							X	X	
FMT_MSA.3									X				X	
FMT_MTD.1												X	X	
FMT_SMR.1								X						
FPT_X_TSP.1				X										

The FCS requirements have a dependency on FMT_MSA.2 which is not included in this ST. FMT_MSA.2 ensures that the TSF ensures of secure attributes. This requirement is not added to the IT environment of the TOE as the cryptographic operations used by the TOE are FIPS validated and the FIPS validation process would have tested and validated that the operations only accepts secure values.

8.2.4 Explicitly Stated Requirements Rationale

This ST contains explicitly stated requirements to address the certificate status and validation functions to which the CC functional requirements are not applicable. The CC functional requirements do not define class components that address the functions illustrated by the explicitly stated requirements. Specifically, the CC does not contain requirements that address the

application of digital signatures to data. Also, the CC does not contain requirements that address PKI standards (e.., OCSP response contents). All of the explicitly stated requirements are self-contained and do not introduce any new dependencies.

8.2.5 Security Assurance Requirement Rationale

This ST contains the assurance requirements from the CC EAL3 assurance package augmented with ALC_FLR.1. The CC permits assurance packages to be augmented, which allows the addition of assurance components from the CC not already included in the EAL. Augmentation was chosen to provide the added assurance acquired by defining flaw remediation procedures and correcting security flaws. The sufficiency of the EAL chosen (EAL3) augmented with ALC_FLR.1 is justified based on those aspects of the environment that have impact upon the assurance needed in the TOE. The administrative users manage the TOE in a competent and cooperative manner, adhering to the policy and procedure under which the TOE operates (OE.Person, and OE.User_authorized_knowledgeable). The TOE is physical protected (OE.Physical). The security flaws of the TOE are corrected. Given these aspects, a TOE based on good commercial development and maintenance practices is sufficient. EAL3 augmented is an appropriate level of assurance for the TOE described in this ST.

8.3 TOE Summary Specification Rationale

This section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions and security assurance measures are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification and indicated in Table 11 - Security Functional Requirements vs. Security Functions are all necessary for the required functionalities in the TSF.
Table 12 - Security Assurance Requirements vs. Assurance Measures provides a mapping of TOE security assurance functions to those security assurance measures that have been implemented by the developer to ensure that the TOE meets the requirements specified by CC EAL3 augmented.

Table 11 - Security Functional Requirements vs. Security Functions

Security Functions / Functional Requirements	AUDIT	COMMUNCATION	IDENTIFICATION AND AUTHENTICATION	USER DATA PROTECTION	SECURITY MANAGMENT	TSF PROTECTION
FAU_GEN.1	X					
FAU_GEN.2	X					
FAU_SAR.1	X					
FAU_SAR.2	X					
FAU_SAR.3	X					
FAU_SAR.3	X					
FCO_NRO.2		X				
FCO_NRO_X.3		X				

Security Functions / Functional Requirements	AUDIT	COMMUNCATION	IDENTIFICATION AND AUTHENTICATION	USER DATA PROTECTION	SECURITY MANAGMENT	TSF PROTECTION
FDP_ACC.1				X		
FDP_ACF.1				X		
FDP_ETC_X.3				X		
FDP_X_OCSP.1				X		
FIA_AFL.1			X			
FIA_ATD.1			X			
FIA_UAU.2			X			
FIA_UAU.5			X			
FIA_UID.2			X			
FMT_MSA.1					X	
FMT_MSA.3					X	
FMT_MTD.1(a)					X	
FMT_MTD.1(b)					X	
FMT_MTD.1(c)					X	
FMT_SMF.1					X	
FMT_SMR.1					X	
FPT_RVM.1						X
FPT_X_TSP.1						X

Table 12 - Security Assurance Requirements vs. Assurance Measures

Assurance Measures / Assurance Requirements	PROCESS ASSURANCE	DELIVERY AND GUIDANCE	DEVELOPMENT	TESTS	VULNERABILITY ASSESSMENT
ACM_CAP.3	X				
ACM_SCP.1	X				
ADO_DEL.1		X			
ADO_IGS.1		X			
ADV_FSP.1			X		
ADV_HLD.2			X		
ADV_RCR.1			X		

Assurance Measures / Assurance Requirements	PROCESS ASSURANCE	DELIVERY AND GUIDANCE	DEVELOPMENT	TESTS	VULNERABILITY ASSESSMENT
AGD_ADM.1		X			
AGD_USR.1		X			
ALC_DVS.1	X				
ALC_FLR.1	X				
ATE_COV.2				X	
ATE_DPT.1				X	
ATE_FUN.1				X	
ATE_IND.2				X	
AVA_MSU.1					X
AVA_SOF.1					X
AVA_VLA.1					X

8.4 Strength of Function Rationale

A minimum strength of function claim of SOF-medium is designated for this TOE. This claim was chosen to be consistent with the risk to assets identified by the threats listed in this ST. The strength of function is associated with the password authentication mechanism used in the Identification and Authentication function to authenticate the user into the TOE. The password authentication mechanism is described in FIA_UAU.5.

The TOE also provides a certificate-based authentication mechanism identified in FIA_UAU.5. The certificate authentication is cryptography-based and as such, is outside the scope of the SOF-claims.

8.5 Internal Consistency and Support

The selected functional requirements for the TOE and IT Environment are internally consistent. All the operations performed are in accordance with the CC. The ST does not include any instances of a requirement that conflicts with or contradicts another requirement. In instances where multiple requirements apply to the same function, the requirements and their operations do not cause a conflict between each other.

The selected requirements are mutually supportive by supporting the dependencies as demonstrated in Table 10, the rationale of the suitability of the requirements to meet the objectives; the inclusion of architectural requirements, FPT_RVM.1 and FPT_SEP.1, to protect the TOE; the inclusion of audit requirements to detect security-related actions and the inclusion of management requirements to provide a means to properly configure and manage the other security requirements.

8.6 Protection Profile Claims Rationale

A Protection Profile for this product does not exist. There is no claimed PP conformance.

Appendix A - Acronyms

The following table contains acronyms used in this document.

CA	Certification Authority
CC	Common Criteria
CIMC	Certificate Issuance Management Components
CIMS	Certificate Issuing Management System
RTC VA	Certificate Status Management Components
CSPP	Guidance for COTS Security Protection Profiles
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IT	Information Technology
KEK	Key Encryption Key
KPK	Key Protection Key
LDAP	Lightweight Directory Application Protocol
NFS	Network File System Protocol
OCSP	Online Certificate Status Protocol
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration Authority
RP	Relying Party
RTC	Real Time Credentials
SF	Security Function
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions

TSFI	TOE Security Functions Interface
TSP	TOE Security Policy
URL	Uniform Resource Locator
VA	Validation authority

Appendix B - Glossary

Attributes – information associated with users, subjects, information and objects that allow the TOE to behave correctly. Examples of attributes are file names and access control information (considered a "security attribute").
Authorized user – a user who possesses the rights and/or privileges, in accordance with the TSP, to perform an operation.
MiniCRL- a reduced form of Certificate Revocation List.
Object – an entity within the TSC that contains or receives information and upon which subjects perform operations. Objects are passive entities (i.e., information containers).
Privilege – administrator-defined attribute that is mapped to a certificate. The privilege defines the accesses rights given to the certificate owner.
Role – a predefined set of rules establishing the allowed interactions between a user and the TOE. These rules establish what functions a person assuming this role may do (e.g., backup, system configuration, key generation, etc.)
Security-attribute – an attribute that contains security relevant information such as access control information.
Security target – a set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.
Signature Algorithm OID – the identifier for the FIPS approved digital signature algorithm.
Subject – an entity within the TSC that causes operations to be performed. Subjects are active entities which perform functions (e.g., UNIX processes).
TSF data – data created by and for the TOE that might affect the operations of the TOE. Information used by the TSF in making TSP decisions (e.g., authentication data, security attributes).
User – an entity (human user or external IT entity) outside the TOE that interacts with the TOE. Users are outside the TOE and therefore outside the TSC.
User data – Data created by and for the user that does not affect the operation of the TSF (.e.g., user emails). Any data that is not TSF data is considered user data.