National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

CoreStreet
Real Time Credential Validation Authority
Version 4.0

Report Number: CCEVS-VR-04-0078

Dated: 1 September 2004

Version 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Maureen Cheheyl
Sunil Trivedi
The MITRE Corporation
Bedford, Massachusetts

Common Criteria Testing Laboratory

Tony Apted
Dawn Campbell
Terrie Diaz
Colleen Glass
SAIC
Columbia, Maryland

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the CoreStreet Real Time Credential Validation Authority, Version 4.0. It presents the evaluation results, their justifications, and the conformance result. The evaluation was performed by Science Applications International Corporation (SAIC) and was completed on 1 September 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by SAIC and submitted to the validators. The evaluation determined that the product conforms to the CC Version 2.1, Part 2 and Part 3 to meet the requirements of EAL 3 with augmentation, resulting in a "pass" in accordance with CC Part 1 paragraph 175. Evaluation Assurance Level (EAL) 3 has been augmented with the Flaw Remediation (ALC_FLR.1) requirement.

The information contained in this Validation Report is not an endorsement of the product by any agency of the U.S. Government, and no warranty of the product is either expressed or implied.

Evaluation Overview

Evaluated Product	CoreStreet Real Time Credential Validation Authority Version 4.0
Developer and Sponsor	CoreStreet Inc. One Alewife Center, Suite 200 Cambridge, MA 02140
CCTL	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Completion Date	1 September 2004
Evaluation Class	EAL3 augmented by ALC_FLR.1
Security Target	CoreStreet Real Time Credential Validation Authority Security Target, Version 1.0, 2 September 2004
Evaluation Technical Report	Evaluation Technical Report for CoreStreet Real Time Credential Validation Authority, Version 2.0, 9 September 2004
CC Version	CC Version 2.1 and all applicable International Interpretations effective on 9 January 2004
CEM Version	CEM Version 1.0 and all applicable International Interpretations effective on 9 January 2004
Evaluators	SAIC: Tony Apted, Dawn Campbell, Terrie Diaz, Colleen Glass
Validators	Maureen Cheheyl and Sunil Trivedi, The MITRE Corporation

Evaluated Product

CoreStreet's Real Time Credential Validation Authority supports a Public Key Infrastructure (PKI) 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 Real Time Credential Validation Authority (RTC VA) TOE (target of evaluation) is designed to provide a 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:

- Maintaining and distributing certificate status information for unexpired certificates

- Maintaining and distributing 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:

- Basic 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.

The CoreStreet Real Time Credential Validation Authority (RTC VA) product comprises three software components, two of which have been evaluated:

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

The third component, the CoreStreet RTC Client toolkit, an OCSP client (relying party application), is not part of the TOE.

The RTC VA application operates in a Windows or Linux/UNIX environment. The operating environment of the RTCA includes a database for 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)
-

Evaluation Results

The TOE, consisting of CoreStreet RTC Authority Version 4.0 and CoreStreet RTC Responder Version 4.0, was evaluated against the requirements of EAL3 augmented by ALC_FLR.1. The evaluation was conducted based upon CC version 2.1 and CEM version 1.0 with International Interpretations valid on 9 January 2004. The evaluation determined the CoreStreet Real Time Credential Validation Authority TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 3 augmented with ALC_FLR.1) requirements. The rationale supporting each CEM work unit verdict is recorded in the *Evaluation Technical Report for CoreStreet Real Time Credential Validation Authority Part II*, which is considered proprietary to the CCTL and to the developer.

2 Identification

The CoreStreet Real Time Credential Validation Authority TOE is made up of two software components:

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

3 Security Policy

The CoreStreet 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 can rely on this information to make access control decisions to both physical locations and logical functions and services. CoreStreet Real Time Credential Validation Authority supports the following six security functions:

Audit

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.

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, which may be one or more of Administrator, Auditor, or Officer. The TOE implements an access control policy that 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.

Identification and Authentication

The RTCA has two authentication mechanisms that may be used together to identify authorized users; there are no unauthorized users of the RTC VA TOE. The first mechanism is the user id and password. The RTCA accepts and verifies the user id and password against the user account information stored in the database. If the user's account includes a certificate containing a public key, certificate-based authentication is also required. In this case, the RTCA issues a standard SSL challenge to the user, who must return a response encrypted with his private key. Upon successful verification, the user is permitted access to those administrative interfaces allowed by the user's assigned roles.

Communication

The CoreStreet RTC VA imports these data types:

- Issuer registration data: These data include the issuer's common name, assigned OID and public certificate. They contain 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 attribute-managing officers (optional): These certificates are used to authenticate and verify the integrity of certificate privilege change requests.
- Trusted root certificates: These certificates are the "trust anchors" that are used to authenticate certificates from entities outside the RTC VA

Note that the relying party applications and the RTC Responders do not communicate directly with the RTC Authority. All data imported by the RTCA is of a specific predefined type and from authenticated sources.

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 (i.e., privileges), 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.

TSF Protection

The RTCA ensures that TOE security functions (TSF) are not bypassed by enforcing the authentication mechanisms and by restricting access 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 with the information can be discovered by comparing the stored digital signature with a generated signature.

4 Assumptions and Clarification of Scope

The RTC VA TOE is made up of software applications that operate in a Windows or Linux/UNIX environment. The operating environment of the RTCA includes a database for storage, and a FIPS 140-1/FIPS 140-2 Level 3 validated or compliant cryptographic module to perform all required cryptographic functions. The product can interoperate with several different Certificate Authorities and Relying Party OCSP client plug-ins.

Usage Assumptions

All users of the TOE are authorized users in one or more of three administrative roles. It is assumed that these administrative personnel are not careless, negligent, or hostile, that they are familiar with security policy and procedures. It is also assumed that physical access to the TOE operating environment is limited to only such personnel and that TOE software is protected from physical modification.

The TOE and its environment are intended to mitigate threats of hackers masquerading as authorized users, modification or destruction of audit data by unauthorized personnel, malicious access to processing resources or information by unauthorized individuals, and physical attack by a malicious user.

Environmental Assumptions

The non-IT environment is assumed to include adequate documentation and training on secure installation, configuration, and operation of the TOE. 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. 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. The TOE environment must ensure that all authorized users are familiar with the policy and procedures under which the TOE is operated.

The TOE environment must provide approved cryptographic algorithms for encryption and decryption, authentication, signature generation and 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.

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

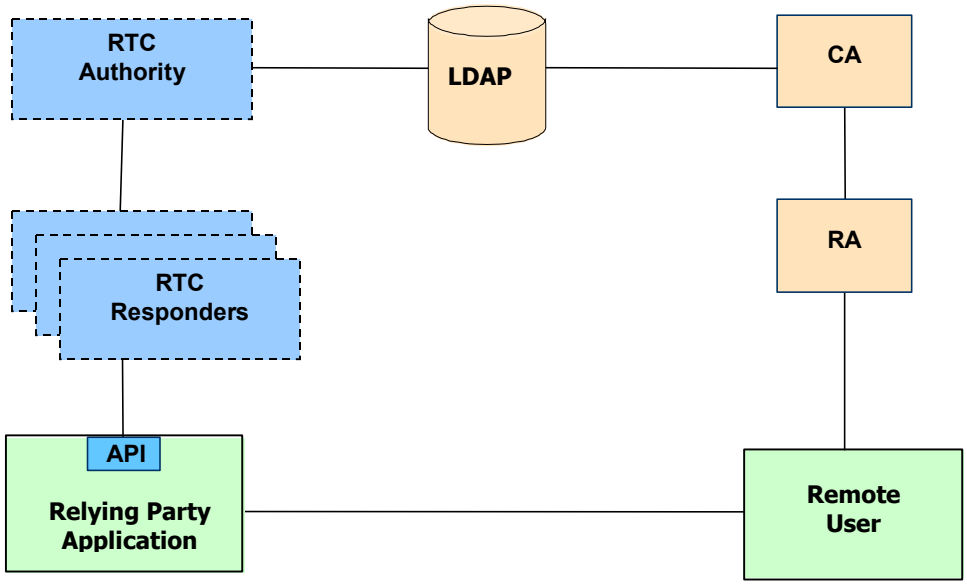
5 Architectural Information

This section provides a high level description of the TOE and its components as described in the Security Target.

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

The figure below illustrates 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 and optionally any associated attributes.

In many PKIs, the CA posts certificates and Certificate Revocation Lists (CRLs) to a repository such as the LDAP directory as illustrated in the figure below. 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.)



6 Documentation

The CoreStreet RTC Validation Authority ships with the following documents:

RTC Authority User Guide Version 4.0, Revision 3
RTC Authority Administration Guide, Version 4.0 Revision 7
RTC Responder Administration Guide, Version 4.0 Revision 7
CoreStreet RTC Validation Authority Version 4.0 Release Notes

7 IT Product Testing

The evaluation team applied each EAL 3 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The following hardware is used to create the test configurations:

Unix:
1 GHz Intel x86 processor or 500 MHz Sparc processor
512 MB memory
100 MB available disk space

Hardware Security Module - nCipher

Microsoft Windows:
1 GHz Intel x86 processor
512 MB memory
100 MB available disk space

Hardware Security Module – nCipher

Software: The following software is required for the test configuration:

Operating Systems:
Red Hat Linux 9
Microsoft Windows 2000

Supporting Software:
Red Hat Linux 9 platforms: Postgres SQL Netscape 4.7 browser
Windows platforms: Microsoft SQL Desktop Engine (MSDE); Microsoft Internet Explorer version 6.

Real Time Credential Validation Authority Software Version 3.0.2-qa005.

Java VM

Vendor Testing

The vendor developed sixteen functional test suites to test RTC VA; security function testing is integrated into these component functional tests. Security functions are mapped to specific test suites and tests, and then to subsystems, so that the tests map to subsystems. Tests were executed manually on a standard Windows configuration and on Unix configurations running on Red Hat Linux 9 and on Solaris 8. Each test suite is identified and briefly described below:

Test Suite	Description
I. Installer Tests	Verifies that the RTC VA installation program correctly installs all components.
II. RTC Authority Configuration	Verifies that the RTC Authority configuration program can be run to configure or reconfigure RTC Authority features, and that the program will not accept invalid configuration parameters.
III. RTC Responder Configuration	Verifies that the RTC Responder configuration program can be run to configure or reconfigure RTC Responder features, and that the program will not accept invalid configuration parameters.
IV. Issuer Administration	Demonstrates that the RTC Authority accepts valid certificate issuer registration data and rejects invalid registration data using the RTC Authority administration interface.
V. Certificate Administration	Demonstrates that the RTC Authority accepts valid issued certificates and rejects invalid issued certificates.
VI. Attributes	Demonstrates that the RTC Authority administrator can define and manage certificate attributes.
VII. CRLs	Demonstrates that the RTC Authority accepts valid certificate revocation lists and rejects invalid certificate revocation lists using the RTC Authority administration interface.
VIII. User Accounts	Verifies that the administrator can create and manage RTC Authority user accounts.
IX. Data Sources	Verifies that the administrator can configure the RTC Authority to obtain certificates and CRLs from bulk sources such as LDAP and URL directories.
X. Key Store	Verifies that the administrator can configure the RTC Authority to use keys and to update the key store.
XI. Basic OCSP Proof Lists	Verifies the generation and validity of OCSP responses.
XII. MiniCRL	Verifies the generation and validity of MiniCRL segments.
XIII. Trust	Verifies that the administrator can specify which certificates are to be trusted explicitly by the RTC Authority when making requests, responses, or connections, and the depth (the number of intermediate links allowed in the certification path between the certificate presented or requested in the operation and the issuer of the explicitly-trusted certificate).
XIV. Credential Status	Verifies that an auditor can search for and examine the status of individual credentials.

Test Suite	Description
XV. Last Actions	Verifies that an auditor can view the audit log, search the audit log for a selected list of entries, view individual audit log entries, sort entries based on various parameters, and examine the audit log for evidence of tampering.
XVI. Upgrade	Verifies that RTC Validation Authority components retain their version 2.6 parameters when upgraded to version 4.0.

Of these, test suites IV, V, VII, VIII, XI, XII and XV include tests of the security functions of the TOE.

Evaluator Testing

To sample the tests in the developer's test suite, the evaluation team installed the TOE on computer systems operating Windows and Linux. The team then performed a representative sample of the tests on both configurations, and they examined the test output to confirm that the actual test results were consistent with the expected results. The subset of the developer's tests that the team executed included all tests identified as demonstrating the security functionality of the TOE, based on the results of the coverage and depth analyses.

Based on a review of the product specifications and the developer's test suite, the evaluation team identified specific functionality for additional independent testing. The team tests demonstrated functionality across the security functions described in the Security Target, including the audit, communication, user data protection, identification and authentication, security management, and TSF protection functions. The evaluation team also developed penetration tests based upon their review of the vendor's vulnerability assessment, wherever needed, to confirm the non-exploitability of potential vulnerabilities that had been noted in the course of the evaluation. After each test was performed, the evaluators confirmed that the actual results matched the expected results. Because the developer's security tests included tests that anticipated one of the penetration tests devised by the evaluation team, the evaluation team did not need to execute all of their own penetration tests.

The results of the evaluation team tests and the evaluation penetration tests demonstrated that the product behaved as claimed in the Security Target. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities.

8 Evaluated Configuration

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

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)
-

9 Results of the Evaluation

The TOE, consisting of CoreStreet RTC Authority Version 4.0 and CoreStreet RTC Responder Version 4.0, was evaluated against the requirements of EAL3 augmented by ALC_FLR.1. The evaluation was conducted based upon CC version 2.1 and CEM version 1.0 with International

Interpretations valid on 9 January 2004. The evaluation determined the CoreStreet Real Time Credential Validation Authority TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 3 augmented with ALC_FLR.1) requirements. The rationale supporting each CEM work unit verdict is recorded in the *Evaluation Technical Report for CoreStreet Real Time Credential Validation Authority Part II*, which is considered proprietary to the CCTL and to the developer.

Evaluation of the CoreStreet Real Time Credential Validation Authority Security Target (ST) (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of threats, policies, and assumptions, a statement of security requirements claimed to be met by the CoreStreet Real Time Credential Validation Authority product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

Evaluation of the CM capabilities (ACM)

The evaluation team applied each EAL 3 ACM CEM work unit. The ACM evaluation ensured the TOE is labeled such that the consumer is able to identify the evaluated TOE. The evaluation team ensured that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. In addition, the evaluation team ensured changes to the implementation representation are controlled and that TOE associated configuration item modifications are properly controlled.

Evaluation of the Delivery and Operation documents (ADO)

The evaluation team applied each EAL 3 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed identification of the TOE and allows for detection of unauthorized modifications of the TOE. The evaluation team followed the CoreStreet Real Time Credential Validation Authority, RTC Authority Administration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

Evaluation of the Development (ADV)

The evaluation team applied each EAL 3 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and high-level design documents. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Evaluation of the Guidance documents (AGD)

The evaluation team applied each EAL3 AGD CEM work unit. The evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. There was not a separate user's guide since users do not directly interface with the TOE. The administrator guide was assessed during the design and testing phases of the evaluation to ensure it was complete.

Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 3 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures describe the life-cycle model and tools used to develop and maintain the TOE. To support the ALC evaluation, the evaluation team performed a Life Cycle (LC) audit. During the audit, the evaluation team witnessed the use of the security measures as described in the LC documentation and sampled records created by using the security procedures.

In addition to the EAL 3 ALC CEM work units, the evaluation team applied the ALC_FLR.1 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that systematic procedures exist for managing flaws discovered in the TOE.

Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 3 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 3 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

Assurance Requirement Results

The assurance requirements for the TOE evaluation are those required by EAL3 augmented with ALC_FLR.1.

Common Criteria Assurance Components

The CEM work units associated with EAL3 augmented with ALC_FLR.1 are distributed amongst the ETR sections in Section 15 of the ETR. Collectively, the ETR sections in Section 15 encompass all CEM work units for EAL3 augmented with ALC_FLR.1. Each ETR section includes the CEM work units associated with that ETR section title (e.g. ACM). Within each ETR section, for each CEM work unit the following is provided:

Work Unit
Analysis Approach
Conclusion and Supporting Rationale

The rationale justifies the conclusion using the CC, the CEM, and any interpretations and the evaluation evidence examined. The rationale demonstrates how the evaluation evidence meets each aspect of the criteria.

The Analysis Approach contains a description of the action performed or the method used to apply the work unit.

Testing and Vulnerability Assessment

The testing and vulnerability related detail that is described in the CEM guidance beyond the CEM work unit information is provided in the ETR Part 2 and is considered SAIC and CoreStreet proprietary. This detail is described within the CEM guidance for the testing and vulnerability assessment work units.

Assurance Components without Methodology

There are no assurance components within the ST that have no methodology associated with them. For the EAL3 augmented with ALC_FLR.1 portions of the evaluation, the CEM includes a methodology for each of the components included. In addition to the CEM work units, the evaluation team applied the CEM guidance.

The following circumstances are not applicable to this evaluation:

Common Criteria assurance components that do not contain methodology in the CEM,
Explicitly stated assurance activities, and
International Interpretations that affect a Common Criteria assurance requirement in a way that requires new methodology to satisfy the interpretation.

10 Validator Comments

The CoreStreet Real Time Credential Validation Authority TOE satisfies *CoreStreet Real Time Credential Validation Authority Security Target Version 1.0,* 2 September 2004, when configured according to the Administration Guides listed in Section 6, and the CoreStreet RTC VA ST is a CC compliant ST.

11 Security Target

The Security Target is *CoreStreet Real Time Credential Validation Authority Security Target Version 1.0,* 2 September 2004.

12 Acronyms

EAL	Evaluation Assurance Level
CA	Certification Authority
CC	*Common Criteria for Information Technology Security Evaluation*

CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	*Common Methodology for Information Technology Security Evaluation*
CRL	Certificate Revocation List
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IT	Information Technology
LDAP	Lightweight Directory Application Protocol
NIAP	National Information Assurance Program
OCSP	Online Certificate Status Protocol
PKE	Public Key Enabled
PKI	Public Key Infrastructure
RTC	Real Time Credential
RTCA	Real Time Credential Authority
RTCR	Real Time Credential Responder
RTC VA	Real Time Credential Validation Authority
SF	Security Function
SFR	Security Functional Requirement
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

13 Bibliography

CC Documents

Common Criteria for Information Technology Security Evaluation

- Part 1: Introduction and General Model, Version 2.1, August 1999, CCIMB-99-031
- Part 2: Security Functional Requirements, Version 2.1, August 1999, CCIMB-99-032
- Part 3: Security Assurance Requirements, Version 2.1, August 1999, CCIMB-99-033

With International Interpretations effective on 9 January 2004

Common Methodology for Information Technology Security Evaluation

- Part 1: Introduction and General Model, Version 0.6, 97/01/11, CEM-97/017
- Part 2: Evaluation Methodology, Version 1.0, August 1999, CEM-99/045
- Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R

With International Interpretations effective on 9 January 2004

CCEVS Documents

Common Criteria Evaluation and Validation Scheme for Information Technology Security, Guidance to Validators of IT Security Evaluations, Scheme Publication #3, Version 1.0, February 2002

Common Criteria Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Scheme Publication #4, Version 1, March 20, 2001.

Developer Documents

Design documentation

Design and Architecture CoreStreet
RTC Validation Authority, Revision 1.22, 12 August 2004

Guidance documentation

RTC Authority User Guide Version 4.0, Revision 3
RTC Authority Administration Guide, Version 4.0, Revision 7
RTC Responder Administration Guide, Version 4.0, Revision 7
CoreStreet RTC Validation Authority, Version 4.0 Release Notes

Configuration Management

Development Environment and Procedures, Revision 1.11, June 23, 2004

Delivery and Operation documentation

Development Environment and Procedures, Revision 1.11, June 23, 2004
Life Cycle Support, Revision 1.12, June 25, 2004
RTC Authority User Guide Version 4.0, Revision 3,
RTC Authority Administration Guide, Version 4.0, Revision 7
RTC Responder Administration Guide, Version 4.0, Revision 7
CoreStreet RTC Validation Authority, Version 4.0 Release Notes

Life Cycle Support

Life Cycle Support, Revision 1.12, June 25, 2004

Test

Test Plan, Revision 1.15, 1 September 2004
Test Procedures, Revision 1.17, 13 August 2004

Vulnerability Assessment

CoreStreet RTC Validation Authority Vulnerability Analysis, Version 1.0

Security Target

CoreStreet Real Time Credential Validation Authority Security Target, Version 1.0, 2 September 2004