National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Netscape Certificate Management System 6.1 Service Pack 1

Report Number: **CCEVS-VR-03-0036**
Dated: **17 March 2003**
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

Richard H. Murphy
Mitretek Systems,
Falls Church, Virginia

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

The evaluation of the Netscape Certificate Management System 6.1 Service Pack 1 (CMS 6.1) was performed by Science Applications International Corporation (SAIC) in the United States and was completed on 12 March 2003. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1) and against Certificate Issuing and Management Components (CIMC) Security Level 3 Protection Profile (Version 1.0, October 31, 2001). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the Netscape Certificate Management product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC.

1.1 Evaluation Details

Evaluation Completion: 12 March 2003

Evaluated Product: Netscape Certificate Management System 6.1 Service Pack 1

Developer: America Online, Inc.
466 Ellis Street
Mountain View, CA 94043-4042

CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Validation Team:	Richard H. Murphy Mitretek Systems, Inc. 3150 Fairview Park South Falls Church, VA 22042-4519
Evaluation Class:	EAL 4 augmented with ALC_FLR.2
Completion Date:	12 March 2003

1.2 Interpretations

The Evaluation Team determined that the following CCIMB Interpretations were applicable to this evaluation:

1. Unique Identification of Configuration Items in the Configuration List (003)
2. ACM_SCP.*.1C requirements unclear (004)
3. Use of ‘as a minimum’ in C&P elements (038)
4. Meaning of “clearly stated” in APE/ASE_OBJ.1 (043)
5. Use of Documentation Without C & P Elements (051)
6. Aspects of Objectives in TOE and Environment (084)
7. SOF Claims Additional to Overall Claim (085)
8. Indistinguishable work units for ADO_DEL (116)

The Evaluation Team determined that the following NIAP interpretations were applicable to this evaluation:

1. Empty Selection or Assignments (407)
2. Other Properties In FMT_MSA.3 Should Be Specified By Assignment (409)
3. Auditing Of Subject Identity For Unsuccessful Logins (410)
4. User Attributes To Be Bound Should Be Specified (415)
5. Association Of Access Control Attributes With Subjects And Objects (416)
6. Evaluation of the TOE Summary specification: Part 1 Vs Part 3 (418)
7. Clarification Of ``Audit Records" (422)
8. Some Modifications To The Audit Trail Are Authorized (423)
9. Settable Failure Limits Are Permitted (425)
10. Content of PP Claims Rationale (426)
11. Identification of Standards (427)
12. Selecting One Or More (429)

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.

1.3 Threats to Security

The Security Target identified the following threats that the evaluated product addresses:

Name (T = Threat)	Threat
T.Administrative errors of omission	Administrators, Operators, Officers or Auditors fail to perform some function essential to security.
T.User abuses authorization to collect and/or send data	User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data.
T.User error makes data inaccessible	User accidentally deletes user data rendering user data inaccessible.
T.Administrators, Operators, Officers and Auditors commit errors or hostile actions	An Administrator, Operator, Officer or Auditor commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur.
T.Critical system component fails	Failure of one or more system components results in the loss of system critical functionality.
T.Malicious code exploitation	An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets.
T.Message content modification	A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.
T.Flawed code	A system or applications developer delivers code that does not perform according to specifications or contains security flaws.
T.Disclosure of private and secret keys	A private or secret key is improperly disclosed.
T.Modification of private/secret keys	A secret/private key is modified.
T.Sender denies sending information	The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.
T.Hacker gains access	A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.
T.Hacker physical access	A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.
T.Social engineering	A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

2 Identification

2.1 ST and TOE Identification

ST: Netscape Certificate Management System 6.1 Service Pack 1 Security Target, Version 1.0, 12 March 2003

TOE Identification: Netscape Certificate Management System 6.1 Service Pack 1

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408.

Protection Profile (PP) Identification – Certificate Issuing and Management Components (CIMC) Security Level 3 Protection Profile, Version 1.0, October 31, 2001.

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

The CMS TOE consists of the CMS (CA, RA, KRA, OCSP) component and associated tools. The CMS component is the main component in Netscape CMS, and is a set of pure Java classes. This component can be portable to other J2EE containers such as Netscape's Application Server that provides excellent application deployment capability, reliability, and scalability.

The CMS component provides a secure application (service) platform where services (i.e. Certificate Authority Service, Registration Authority Service, OCSP Response Service, Key Archival and Recovery Service, and other Customer specific services) can be tightly integrated with a PKI infrastructure. A service that is developed on top of CMS can communicate to its users and other CMS services securely.

The following architectural diagram shows the interactions between various CMS configurations and various internal and external systems. Internally, CMS communicates with an internal LDAP database (CMS's Internal Database) where certificate records, request records, and system user records are stored. CMS also relies on the JSS and NSS libraries to access the cryptographic operations. Externally, the HTTP engine manages the presentation-level interaction between CMS and users including end-users, security officers, and administrators. CMS may optionally publish certificates to a corporate LDAP directory.

In addition to JSS library, NSS library, the HTTP Engine and Internal LDAP Database, CMS also relies on access to processing capabilities, file storage, as well as hardware cryptographic modules provided by its IT environment.

In the following Figure, the Non-TOE IT environments are similar among all CIMC boundaries. . Please refer to CIMC Boundary 1 in Figure 1 to see complete details for all other Non-TOE IT within other CIMC boundaries.

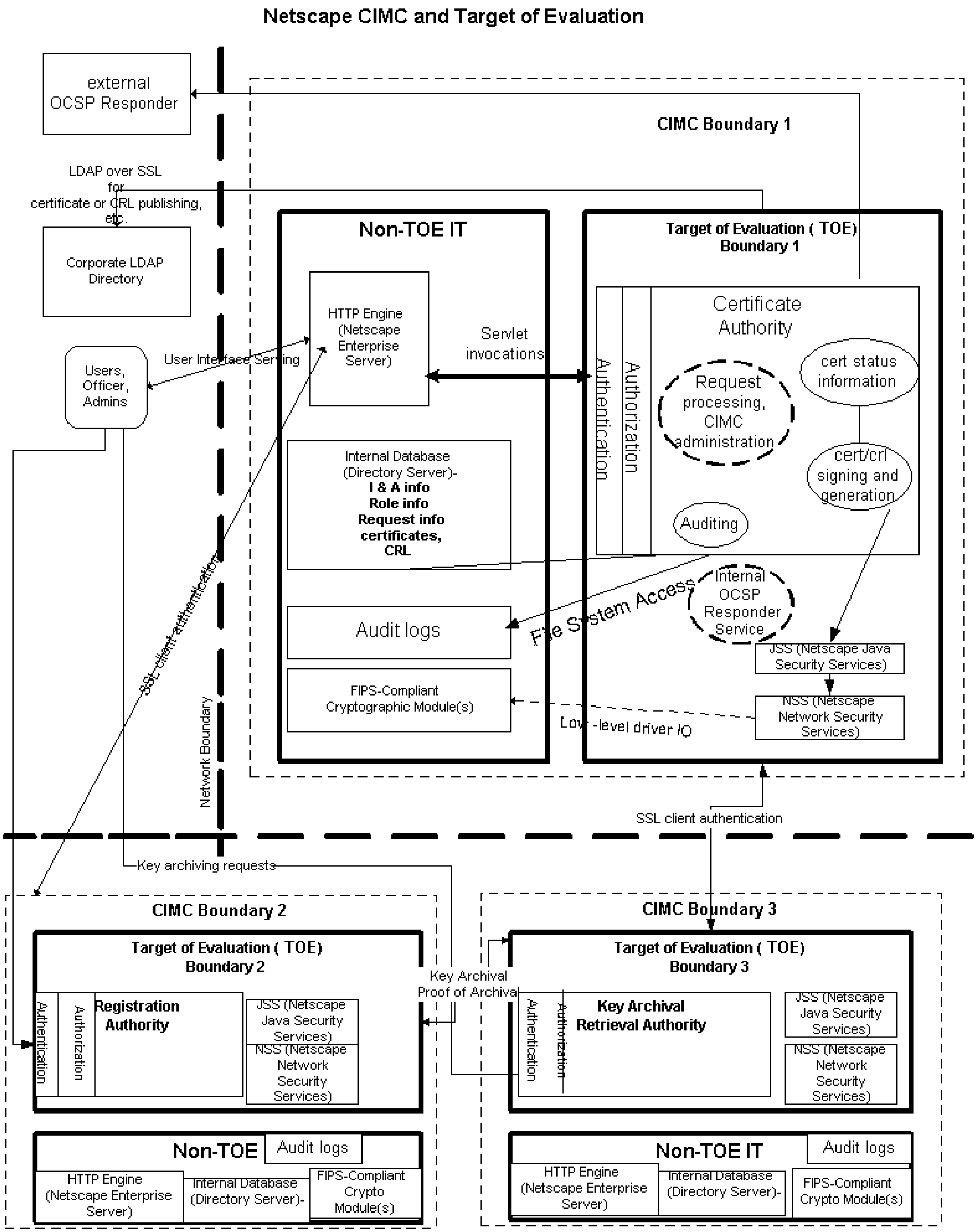
Netscape CIMC and Target of Evaluation
external OCSP Responder
CIMC Boundary 1
LDAP over SSL for certificate or CRL publishing, etc.
Corporate LDAP Directory
Non-TOE IT
Target of Evaluation (TOE) Boundary 1
HTTP Engine (Netscape Enterprise Server)
Servlet invocations
Certificate Authority
Authentication
Authorization
Request processing, CIMC administration
cert status information
cert/crl signing and generation
Auditing
Users, Officer, Admins
User Interface Serving
Internal Database (Directory Server)- I & A info Role info Request info certificates, CRL
SSL client authentication
Network Boundary
Audit logs
File System Access
Internal OCSP Responder Service
JSS (Netscape Java Security Services)
NSS (Netscape Network Security Services)
FIPS-Compliant Cryptographic Module(s)
Low -level driver IO
SSL client authentication
Key archiving requests
CIMC Boundary 2
Target of Evaluation (TOE) Boundary 2
Authentication
Authorization
Registration Authority
JSS (Netscape Java Security Services)
NSS (Netscape Network Security Services)
Non-TOE
Audit logs
HTTP Engine (Netscape Enterprise Server)
Internal Database (Directory Server)-
FIPS-Compliant Crypto Module(s)
Key Archival
Proof of Archival
CIMC Boundary 3
Target of Evaluation (TOE) Boundary 3
Authentication
Authorization
Key Archival Retrieval Authority
JSS (Netscape Java Security Services)
NSS (Netscape Network Security Services)
Non-TOE IT
Audit logs
HTTP Engine (Netscape Enterprise Server)
Internal Database (Directory Server)-
FIPS-Compliant Crypto Module(s)

Figure 1 - CMS 6.1 System Overview

2.2 IT Security Environment

The CMS 6.1 TOE is an application written in Java that is designed to integrate with a directory server such as Netscape Directory Server and a HTTP engine such as Netscape Enterprise server which provide an internal data store and a network interface, respectively. The CMS TOE utilizes NSS (Netscape Network Security Services) and JSS (Netscape Java Security Services) libraries to support the use of hardware devices that perform standards-oriented cryptographic operations. All of the components represent a CMS system. A CMS system is designed to be hosted within a secure operating system (e.g., Solaris 8.0) and to be connected to networks, including the Internet, and to offer these services using standard HTTP/SSL protocols.

CMS 6.1 is designed to be installed in one of four configurations: CA, RA, KRA (also called DRM), and OCSP Responder. The primary difference between these configurations is the set of services offered to users.

The following is a list of items in the IT security environment that the CMS TOE relies upon:

- HTTP Engine (e.g., Netscape Enterprise Server)

  The web engine provides the HTML-based UI (presentation) and HTTP-based protocol handling. It does not perform authentication and authorization other than providing and/or enforcing SSL. The web engine provides the HTML-based UI (presentation) and HTTP-based protocol handling. It performs basic certificate validation and delegates all the application-specific authentication and authorization to CMS via a callback mechanism.

- Internal Database (e.g., Netscape Directory Server)

  The internal database stores information such as certificates, requests, officers/administrator information, and other information such as access control information.

- Network Security Services (NSS)

  Network Security Services (NSS) is a set of libraries designed to support cross-platform development of security-enabled communications applications. Applications built with the NSS libraries support the SSL protocol for authentication, tamper detection, and encryption as well as the PKCS #11 interface for cryptographic token interfaces.

- JSS (a JAVA/JNI layer)

  Network Security Services for Java (JSS) provides a Java interface for security operations performed by NSS. JSS and higher levels of the Certificate Management System architecture are built with the Java Native Interface (JNI), which provides binary compatibility across different versions of the Java Virtual Machine (JVM). JSS also provides a pure Java interface for ASN.1 types and BER-DER encoding.

- JRE (Java Runtime Environment)

  JRE (Java Runtime Environment) provides the Java Virtual Machine (JVM) and supporting class libraries needed to run Netscape CMS.

- PKCS#11

  Public-Key Cryptography Standard (PKCS) #11 specifies an API used to communicate with devices that hold cryptographic information and perform cryptographic operations. Because it supports PKCS #11, Certificate Management System works with a wide range of hardware and software devices intended for such purposes. Any PKCS #11 hardware module can be used with Certificate Management System. In the Netscape CMS TOE environment, a FIPS 140-1 level 3 certified hardware module is expected to be plugged in and configured to provide higher level of security.

- Administration Server

  The Administration Server comes with all Netscape server products, including Netscape CMS. Together with the Netscape administration Console and the Configuration LDAP database (another instance of the Netscape Directory Server), it is used for managing Netscape software and users in an enterprise environment. The Configuration LDAP database stores server and application configuration settings as well as user information. This data is used by other servers in the enterprise.

- Netscape Console and Web Browser

  Netscape Console is the administration application used by the administrators to configure CMS subsystems. The Netscape Console is (very similar to browsers) capable of supporting SSL client authentication. It communicates with CMS subsystems only through SSL client authenticated channels. Web Browsers, such as the Netscape browser, are client applications used by both agents and end-entity users to access Netscape CMS. The web browsers have to support SSL. Agent interface and some functions for end-entity interface require SSL client-authentication.

- Operating System and Filesystem

  The Operating System provides execution environment for Netscape CMS. The filesystem is used to store logs, HTML forms and response templates, mail notification forms, configuration files, etc. The Operating System is expected to provide needed protection mechanism to protect the Netscape CMS TOE. Netscape CMS TOE relies on the authentication mechanism, access control mechanism (process and file protection), and audit mechanism provided by the Operating System. Because of this, Netscape CMS TOE needs to be installed on an Operating System that can provide adequate security measures.

The TOE includes both physical and logical boundaries.

2.2.1 Physical Boundaries

The TOE has two types of physical interfaces, the interface to its IT Environment and HTTP-based interfaces to access the security functions of the TOE.

As depicted in Figure 1, the TOE exists as an application program interacting with other components to implement its security functions. The TOE application runs within an IT environment consisting of a Java runtime environment and is integrated with a Netscape Enterprise Server. The java runtime environment is provided by a trusted host operating system (e.g., Solaris 8). The Netscape Enterprise Server serves to offer a HTTP-based interface to users of CMS 6.1.

The TOE application supports LDAP interfaces and also HTTP-based interfaces via Netscape Enterprise Server. The LDAP interfaces are used to connect to the internal LDAP Server (e.g., Netscape Directory Server) used by CMS 6.1 exclusively as a private data store, and also to connect to a Corporate LDAP server for publishing purposes, if configured. The HTTP-based interfaces allow users and administrators to connect to CMS 6.1 to access its security functions and to manage CMS 6.1.

2.2.2 Logical Boundaries

Since the TOE is an application, its logical and physical boundaries largely coincide. The TOE requires basic execution, data storage support, and network connectivity services from its IT environment. The external interfaces are limited to LDAP and HTTP (SSL support is provided for each type of connection.). LDAP connections are supported only when initiated by CMS 6.1. The HTTP interfaces are used to offer functions via service-oriented web pages to CMS 6.1 users, officers, and administrators.

Note that administrative functions are performed using a console application included with CMS 6.1. This application interacts with CMS using HTTP, but instead of using HTML it uses a proprietary language to better facilitate the administrator functions available.

3 Security Policy

The CMS 6.1 TOE provides several security services. Their descriptions in the following sections were taken from the ETR, Part 1 (Non-Proprietary version).

3.1 Identification and Authentication

CMS 6.1 ensures that users are identified and authenticated before they can access any other security relevant services.

3.2 Access Control

CMS provides the ability to define an access control list for each service it provides. These access control lists are used to ensure that users can only access services they have been authorized to use.

3.3 Security Management

CMS uses the access control functions to control the actions of administrative personnel. In order to accomplish this, predefined access control lists are assigned to the applicable services.

3.4 Security Audit

CMS has the ability to audit security relevant events. Audit records are generated when audit events occur, including the responsible user, date, time, and other details. Audit records are collected into audit buffers that are signed, to protect against possible tampering of the audit records, and then copied into non-volatile audit logs.

3.5 Backup and Recovery

CMS has a backup/restore utility that can be used to save a snapshot of a CMS configuration and then restore that configuration at a later date. The integrity of the backup data is protected using digital signatures.

3.6 Remote Data Entry and Export

CMS protects data import and export operations using SSL sessions.

3.7 Key Management

CMS includes a number of key management functions. In particular, CMS protects security critical keys and other information by either encrypting it or by storing it within a hardware cryptographic module. CMS also uses digital signatures when appropriate to ensure the integrity of key management related information.

3.8 Certificate Management

CMS includes a number of certificate management functions. In particular, CMS allows administrators to control, limit, or mandate values in certificates, certificate revocation lists (CRLs), and online certificate status protocol (OCSP) responses that are generated.

4 Assumptions

4.1 Personnel Assumptions

A.Auditors Review Audit Logs	Audit logs are required for security-relevant events and must be reviewed by the Auditors.
A.Authentication Data Management	An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.)
A.Competent Administrators, Operators, Officers and Auditors	Competent Administrators, Operators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.
A.CPS	All Administrators, Operators, Officers, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.
A.Disposal of Authentication Data	Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).
A.Malicious Code Not Signed	Malicious code destined for the TOE is not signed by a trusted entity.
A.Notify Authorities of Security Issues	Administrators, Operators, Officers, Auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
A.Social Engineering Training	General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks.
A.Cooperative Users	Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner.

4.2 Physical Assumptions

A.Communications Protection	The system is adequately physically protected against loss of communications i.e., availability of communications.
A.Physical Protection	The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.

4.3 Connectivity Assumptions

A.Operating System	The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats for the appropriate Security Level identified in this family of PPs.

5 Architectural Information

The high level design describes five subsystems that compose CMS 6.1:

- Certificate Authority (CA)
- Registration Authority (RA)
- Data Recovery Manager (DRM) or Key Archival and Recovery Manager (KRA)
- Online Certificate Status Protocol (OCSP) Manager
- TOE Management tools

The high level design was verified to ensure that it was internally consistent.

6 Documentation

Purchasers of CMS 6.1 receive the following documentation:

- Administrator's Guide Netscape Certificate Management System, 3/6/2003
- Agent's Guide Netscape Certificate Management System, 2/24/2003
- Command-Line Tools Guide Netscape Certificate Management System, 2/28/2003

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

7.1 Developer Testing

The vendor shipped a TOE configuration to the CCTL for installation and testing. The evaluation team installed the TOE and ran a subset of the vendor test procedures on the TOE in the evaluated configuration. The vendor provided a complete set of test results for analysis.

Some issues were noted during the set up and testing. Updates to the vendor documentation have corrected the cause of these issues.

SAIC and the developer consider the detailed test configuration to be proprietary information. However, the Evaluation Team has included a description of the vendor's test configurations in the ETR, Part 2.

The evaluation team analyzed the vendor test procedures to ensure adequate coverage and to determine if the interfaces between subsystems were behaving as expected.

The Evaluation Team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The Evaluation Team chose to run a subset all of the tests that the developer performed. The subset was chosen to ensure adequate coverage for all security functional requirements. This ensured that the Evaluation Team adequately addressed both security functions. The Evaluation Team used the developer's test configurations to perform the tests.

In addition, the Evaluation Team also tested the installation, generation, and start-up procedures to determine, in accordance with ADO_IGS.1.2E, that those procedures result in a secure configuration.

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team used a combination of vulnerability test tools, open-source vulnerability documentation, and a set of test procedures proposed by the penetration test team to identify penetration test cases based on the developer's vulnerability assessment documentation. The Evaluation Team used the developer's test configuration to successfully perform its penetration tests.

The Evaluation Team's ETR, Part 2, provides a detailed description of the tests, the results, and the effects, if any, on the information presented in the ST or other evaluation evidence.

8 Evaluated Configuration

The evaluated configuration consisted of 4 Sun Ultra 10 systems for CMS components (CA, RA, DRM, OCSP systems) and 5 nCipher Hardware Security Modules with smart card tokens. A client system running Windows 2000 was used in TOE testing. The systems were running the Solaris 2.8 operating system.

9 Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.1 and the Common Evaluation Methodology (CEM) Version 1.0 and all applicable National and International Interpretations in effect.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

> The evaluation determined the CMS 6.1 TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.2 requirements. The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report for Netscape Certificate Management Server 6.1 (CMS 6.1) Part II" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> 6.1 Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the Netscape Certificate Management System 6.1 Service Pack 1 Security Target is a CC compliant ST.
>
> 6.2 The verdicts for each CEM work unit in the ETR sections included in Section 15 are each "PASS". Therefore, when configured according to the following guidance documentation:
>
> - Netscape Certificate Management System Guidance Documentation, dated 2003/03/06.
>
> The CMS 6.1 TOE … satisfies the Netscape Certificate Management System 6.1 Service Pack 1 Security Target, Version 1.0, 12 March 2003.

The validation team followed the procedures outlined in the Common Criteria Evaluation and Validation Scheme (CCEVS) publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

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 test suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

10 Evaluator Comments/Recommendations

The evaluation team had no recommendations concerning the CMS 6.1 TOE.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as Netscape Certificate Management System 6.1 Service Pack 1 Security Target, Version 1.0, 12 March 2003.

The document identifies the security functional requirements necessary to implement Information Flow Protection and TOE Self Protection security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4 augmented with ALC_FLR.2.

13 Glossary

The following definitions are used throughout this document:

Authentication code: a cryptographic checksum, based on a FIPS-approved or recommended security method; also known as a Message Authentication Code (MAC) in ANSI standards.

CIMC: the set of hardware, software, firmware, or some combination thereof, that issues, revokes, and manages public key certificates and certificate status information, and is contained within the CIMC boundary.

CIMC boundary: an explicitly defined contiguous perimeter that establishes the physical bounds of a CIMC.

Compromise: the unauthorized disclosure, modification, substitution or use of sensitive data (including plaintext cryptographic keys and other CSPs).

Confidentiality: the property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

Critical security parameter (CSP): security-related information (e.g., secret and private cryptographic keys, authentication data such as passwords and PINs) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a CIMC or the security of the information protected by the CIMC.

Cryptographic key (key): a parameter used in conjunction with a cryptographic algorithm that determines:

- the transformation of plaintext data into ciphertext data,
- the transformation of ciphertext data into plaintext data,
- a digital signature computed from data,
- a keyed hash computed from data,
- the verification of a digital signature computed from data,
- an authentication code computed from data, or
- an exchange agreement of a shared secret.

Cryptographic key component (key component): a parameter used in conjunction with other key components in a FIPS-approved or recommended security method to form a plaintext cryptographic key or perform a cryptographic function.

Digital signature: a non-forgeable transformation of data that allows proof of the source (with non-repudiation) and verification of the integrity of that data.

Encrypted key: a cryptographic key that has been encrypted with a key encrypting key, a PIN or a password in order to disguise the value of the underlying plaintext key.

Error detection code (EDC): a code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.

FIPS-Approved or recommended mode of operation: a mode that employs only the operation of FIPS-approved or recommended security methods.

FIPS-approved or recommended security method: a security method (e.g., cryptographic algorithm, cryptographic key generation algorithm or key distribution technique, authentication technique, or evaluation criteria) that is either a) specified in a FIPS or b) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.

Firmware: the programs and data stored in hardware (e.g., ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution. *Hardware*: the physical equipment used to process programs and data in a CIMC.

Integrity: the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Key encrypting key: a cryptographic key that is used for the encryption or decryption of other keys.

Key management: the activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs, passwords) during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving.

Password: a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Personal Identification Number (PIN): a 4 or more character alphanumeric code or password used to authenticate an identity, commonly used in banking applications.

Physical protection: the safeguarding of a CIMC, cryptographic keys, or other CSPs using physical means.

Plaintext key: an unencrypted cryptographic key.

Private key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public.

Protection Profile: an implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs.

Public key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public. (Public keys are not considered CSPs.)

Public key certificate: a set of data that unambiguously identifies an entity, contains the entity's public key, is digitally signed by a trusted party, and binds the public key to the entity.

Public key (asymmetric) cryptographic algorithm: a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that, given the public key, it is computationally infeasible to derive the private key.

Secret key: a cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and which shall not be made public. The use of the term "secret" in this context does not imply a classification level rather the term implies the need to protect the key from disclosure or substitution.

Secret key (symmetric) cryptographic algorithm: a cryptographic algorithm that uses a single, secret key for both encryption and decryption.

Security policy: a precise specification of the security rules under which a CIMC shall operate, including the rules derived from the requirements of this document and additional rules imposed by the vendor.

Software: the programs and associated data that can be dynamically written and modified.

Target of Evaluation (TOE) - An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

User: an individual, or a process (subject) operating on behalf of the individual, accessing CIMC.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, Parts 1, 2, and 3

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

- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, Version 0.6, 11 January 1997.

- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 1.0, August 1999.

- Netscape Certificate Management System 6.1 Service Pack 1 Security Target, Version 1.0, 12 March 2003

- ETR Part 1 (Non-Proprietary)