National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Microsoft Windows Server 2003 Certificate Server

Report Number: CCEVS-VR-07-0022
Dated: **April 1, 2007**
Version: **1.0**

National Institute of Standards and Technology
Information Technology laboratory
100 Bureau Drive
Gaithersburg, Maryland 20899

National Security agency
Information Assurance Directorate
9600 Savage Road Suite 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements:

The TOE evaluation was sponsored by:

Microsoft Corporation
Corporate Headquarters
One Microsoft Way
Redmond, WA 98052-6399
USA

Evaluation Personnel:
Science Applications International Corporation (SAIC)
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046-2554

Shukrat Abbas
Anthony J. Apted
Dawn Campbell
Terrie L. Diaz
Quang Trinh
.

Validation Personnel:
Santosh Chokhani, Orion Security Solutions
Geoff Beier, Orion Security Solutions
Armen Galustyan, Orion Security Solutions

Table of Contents

1 Executive Summary 1
2 Identification 1
3 TOE Security Functions 2
4 Assumptions 3
4.1 Physical Security Assumptions 3
4.2 Personnel Security Assumptions 3
4.3 Connectivity Assumptions 3
4.4 Clarification of Scope 3
5 Architectural Information 4
6 Documentation 4
7 IT Product Testing 4
7.1 Test Configuration 5
7.2 Developer Testing 5
7.3 Evaluation Team Independent Testing 5
7.4 Highly Resistant Vulnerability Analysis 6
8 Evaluated Configuration 6
9 Validator Comments 7
10 Security Target 8
11 List of Acronyms 9
12 Bibliography 11
13 Interpretations 12
13.1 International Interpretations 12
13.2 NIAP Interpretations 12
13.3 Interpretations Validation 12

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Microsoft Windows Server 2003 Certificate Server. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the Microsoft Windows Server 2003 Certificate Server was performed by the SAIC Common Criteria Testing Laboratory in the United States and was completed during October 2005. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 Extended and Part 3 augmented, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.3 (Systematic Flaw Remediation) and AVA_VLA.4 (Highly Resistant Vulnerability Analysis) have been met. The evaluation team also determined that the TOE is conformant with the Certificate Issuing and Management Components (CIMC) Security Level 3 Protection Profile, Version 1.0, October 31, 2001

Windows Server 2003 Certificate Server is the Certification Authority that issues and manages public key certificates to facilitate the use of public key cryptography.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 4 augmented with ALC_FLR.3 and AVA_VLA.4 evaluation. The validation team also determined that the TOE is conformant with the Certificate Issuing and Management Components (CIMC) Security Level 3 Protection Profile, Version 1.0, October 31, 2001. Therefore the validation team concludes that the SAIC Common Criteria Testing Laboratories (CCTL) findings are accurate, and the conclusions justified.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs or candidate CCTLs using the Common Evaluation Methodology (CEM) for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs and candidate CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;

- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Windows Server 2003 Certificate Server
Security Target	Microsoft Windows Server 2003 Certificate Server Security Target, Version 1.0, 1 April 2007
Evaluation Technical Report	Evaluation Technical Report for Microsoft Windows Server 2003 Certificate Server, Version 1.0, 15 November 2005.
Conformance Result	CC Part 2 Extended, CC Part 3 augmented, EAL 4 augmented with ALC_FLR.3 and AVA.VLA.4 Conformant with Certificate Issuing and Management Components (CIMC) Security Level 3 Protection Profile, Version 1.0, October 31, 2001
Sponsor	Microsoft Corporation Corporate Headquarters One Microsoft Way Redmond, WA 98052-6399
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046-2554
CCEVS Validator(s)	Santosh Chokhani, Geoff Beier, and Armen Galustyan Orion Security Solutions 1489 Chain Bridge Road, Suite 300 Mclean, Virginia 22101

3 TOE Security Functions

The TOE, Microsoft Windows Server 2003 Certificate Server, issues and manages public key certificates to facilitate the use of public key cryptography. To achieve this goal, the Microsoft Certificate Server implements the following core functional components:

- Policy-based generating and distributing Public Key (including X.509) Certificates to bind user public keys to other information after validating the accuracy of the information provided
  - Certificate Enrollment or Request based on
    - PKCS #7 (Cryptographic Message Syntax Standard),
    - PKCS #10 (Certification Request Syntax Standard),
    - RFC 2797 CMC (Certificate Management Messages over Cryptographic Message Syntax)
  - Certificate Renewal
  - Certificate Revocation

    - Certificate Retrieval
    - Request Pending Management
- Maintaining and distributing certificate status information for unexpired certificates
    - Certification and Certificate Revocation List (CRL) Management
- Certificate database backup and restore
- Security configuration and management of Microsoft Certificate Server

4 Assumptions

4.1 Physical Security Assumptions

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

4.2 Personnel Security Assumptions

- Audit logs are required for security-relevant events and must be reviewed by the Auditors.
- 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.)
- Competent Administrators, Operators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.
- All Administrators, Operators, Officers, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.
- Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).
- Malicious code destined for the TOE is not signed by a trusted entity.
- 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.
- General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks.
- 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.

4.3 Connectivity Assumptions

- The OS has been selected to provide the functions required by the CIMC PP to counter the perceived threats for the appropriate Security Level identified in the CIMC family of PPs.

4.4 Clarification of Scope

The TOE relies on the Windows 2003 Server Operating System and its security. Windows 2003 Server Operating System is outside the TOE and hence its security properties are not covered by this evaluation. However, the Windows 2003 Server Operating System used in the evaluated configuration of the TOE has previously been successfully evaluated for the same assurance level (i.e., EAL 4 augmented with ALC_FLR.3).

5 Architectural Information

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

The TOE is composed of the executables and dynamically linked libraries (dlls) that implement certificate issuance enforcement, certificate and certificate status publication, a database manager, and several Microsoft Management Console (MMC) snap-ins (Certification Authority, Certificates, and Certificate Templates). To interact with the services of the aforementioned functional components, the TOE provides authorized users of different roles with Graphic User Interface based and command-line based tools that can be executed remotely or locally. These tools use the underlying network based programmatic interfaces implemented by the TOE. This set of programmatic interfaces is able to support automatic certificate enrollment for both user and computer accounts defined for a distributed Windows Operating System environment within the same network as the TOE.

The TOE is packaged as a component of the Microsoft Server 2003 Enterprise Edition operating system. It is installed by selecting the Certificate Services windows component from the Add/Remove Windows Components Wizard. It exists as an application program interacting with other components to implement its security functions.

The TOE has two types of physical interface: the interface to its IT Environment; and Distributed Component Object Model (DCOM)-based interfaces to access the security functions of the TOE.

The TOE requires basic program execution, data storage support, and network connectivity services from its IT environment. The TOE uses Lightweight Directory Access Protocol (LDAP) connections to the IT environment for communication to the Active Directory where the certificate database is stored. The DCOM TOE external interfaces are available for TOE users to request Microsoft Certificate Server operations to be performed.

The cryptographic capabilities required by the TOE to process certificate requests and generate certificates and certificate revocation lists (CRLs) are provided, in the evaluated configuration, by the nCipher nShield F3 PCI – nC4032P-150 hardware security module (HSM), firmware version 2.0.2.

6 Documentation

Following is a list of user documentation which was issued by the developer (and sponsor).

Document	Version	Date
Windows Server 2003 Certificate Server Evaluated Configuration Administrator's Guide	1.0	16 September 2005
Windows Server 2003 Certificate Server Security Configuration Guide	1.0	22 September 2005
Windows Server 2003 Certificate Server Evaluated Configuration User's Guide	1.0	19 August 2005

The developer (i.e., Microsoft) also makes these documents available from a Web Site (http://www.microsoft.com/downloads). The web site is under configuration control. The TOE consumers must ensure that they download the guidance documents with the titles, version numbers, and dates listed in the table above in this section.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Test Configuration

The evaluation team conducted testing on the following hardware configuration, executing Microsoft Windows Server 2003, Enterprise Edition (32-bit) software as identified in Section 8 of this document:

- HP ProLiant DL380 G3 X2.8GHz
- nCipher hardware security module (HSM):
    1. HSM Model: nShield F3 PCI – nC4032P-150
    2. HSM Firmware Version: 2.0.2
    3. nCipher Support Software Version: 7.26 for Windows

The evaluation team initially installed the TOE as an Enterprise Subordinate CA and conducted vendor automated and manual tests on this configuration. The evaluation team also executed all of the evaluation team tests on this configuration. The server hosting the Certificate Server TOE was a member of a domain. The domain controller was provided by HP Workstation ZX2000 running Microsoft Windows Server 2003 Enterprise Edition (64 bit). A separate standalone Certificate Server host acted as a root CA to sign and issue the subordinate CA certificate for the TOE.

At the conclusion of this testing, the TOE was re-installed as an Enterprise Root CA and a subset of vendor tests and a subset of team tests were executed on this configuration. The relationship of the sever hosting the Certificate Server TOE remained unchanged. In other words, the server hosting the Certificate Server TOE was a member of a domain and the domain controller was provided by HP Workstation ZX2000 running Microsoft Windows Server 2003 Enterprise Edition (64 bit).

7.2 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all TOE Security Functions and the entire TSF Interface (TSFI). Where testing was not possible, code analysis was used to verify the TSFI behavior. The evaluation team determined that the developer's actual test results matched the vendor's expected results. It should be noted that the TSFI testing was limited to testing security checks for the interface. The TSFI input parameters were not exercised for erroneous and anomalous inputs.

7.3 Evaluation Team Independent Testing

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 developer test documentation sufficiently addresses the security functions as described in the security target and the TSFI as described in the Functional Specification.

The evaluation team performed a sample of the developer's test suite and devised an independent set of team tests. The evaluation team determined that the vendor's test suite was comprehensive. The evaluation team tested about fifty (50) of the vendor tests. The evaluation team decided to test areas in each security function that may have not been tested completely by the vendor. A total of thirteen (13) team tests[1] were devised and covered the following areas: User Subject Binding, Role Separation, Certificate Request, Proof of possession of private key, Certificate and CRL formats, audit integrity, Certification Authority (CA) public key integrity, backup, request processing, audit, and access control.

[1] Some of the tests consisted of multiple test cases.

The evaluation team confirmed that the developer's vulnerability analysis was comprehensive in terms of examining the evaluation evidence and search for vulnerabilities from public domain sources. The developer's vulnerability analysis also included examination of Microsoft Knowledge base maintained based on the security flaws reported from Microsoft internal research, external consumers, and external security research and testing organizations. The evaluation team augmented the developer's vulnerability analysis by researching and analyzing the following open sources for Windows 2003/XP vulnerabilities: CVE from http://www.cve.mitre.org Web Site.

The evaluation team also conducted three (3) penetration tests. The penetration tests fall in the following areas: GUI tests, certificate request manipulation, and invalid parameter testing.

7.4 Highly Resistant Vulnerability Analysis

Additional testing to address the AVA_VLA.4 requirements was performed by the National Security Agency (NSA) and completed in March 2007. Using the results of the evaluation by the CCTL evaluation team, the NSA evaluation team installed the TOE evaluated configuration and conducted AVA_VLA.4 vulnerability testing. The NSA team utilized the same category of tools used by the CCTL for penetration testing, as well as in-house developed tools, which enabled the team to determine that the TOE was resistant to penetration attacks performed by attackers with high attack potential.

8 Evaluated Configuration

The evaluated configuration is identified in this section.

TOE Hardware – The evaluation results are valid for the following hardware platforms.

- HP ProLiant DL380 G3 X2.8GHz
- Dell Optiplex GX270
- Unisys ES7000-540-G3 (32-bit)
- IBM xSeries 346

TOE Software Identification – The evaluation results are valid for the Microsoft Server 2003 Enterprise Edition operating system. Specifically, the TOE is included in the following product:

- Microsoft Windows Server 2003, Enterprise Edition (32-bit version); Service Pack (SP) 1

  The following security updates must be applied:

  MS05-042 – Vulnerabilities in Kerberos Could Allow Denial of Service (DoS), Information Disclosure, and Spoofing (899587)

  MS05-039 – Vulnerability in Plug and Play Could Allow Remote Code Execution and Elevation of Privilege (899588)

  MS05-027 – Vulnerability in Server Message Block (SMB) Could Allow Remote Code Execution (896422)

  A hotfix that updates the Internet Protocol (IP) Security (IPSec) Policy Agent is available for Windows Server 2003 and Windows XP (907865)

9 Validator Comments

1. Noncompliance with RFC 3280 or X.509

While the TOE produces X.509 compliant certificates and complies with the CIMC PP, the CRL generated by the TOE are not compliant with RFC 3280 or X.509. Whenever a CA re-keys, CRL is partitioned based on certificate signing key without asserting the Issuing Distribution Point extension in the CRL. In order to mitigate the security threat caused due to this lack of compliance to the PKI standards, consumers are strongly urged to not re-key a CA; they should change the CA Distinguished Name also when a new CA key is required.

Customers may also consider another alternative to mitigate this threat as follows. The customers can make sure that their certificate validation applications check that the CRL used to check the status of a certificate is signed by the same CA key that signs the certificate. The certificate validation application that is built into Windows XP and Windows Server 2003 (i.e. the IT environment for this TOE) does this check. In this situation, the threat is not materialized. However, customers may not always be in the position to dictate the capabilities of the applications that consume the certificates and CRLs produced by the TOE. Thus, the first recommendation is preferred. The second recommendation can only work in a closed Enterprise PKI environment where all relying party PK enabled applications are known to require that a certificate and CRL be signed using the same key.

2. RSA Signing

The product signs RSA encryption certificate requests with the decryption private key. This is not desirable and should be removed from the future versions of the TOE.

3. Specify Version of nCipher in configuration guidelines

The certificate Server Configuration Guide specifies the Hardware Security Module (HSM) nCipher nShield as the hardware encryption device connected to the Certificate Server. The nCipher HSM version 4.2.3 was used in the analysis of Certificate Server. Even though the nCipher HSM is outside the TOE, a search for security reports on nCipher reveals a problem with versions preceding Version 4.2.3. The link http://www.ncipher.com/support also recommends obtaining the latest version of the SNMP agent supplied by nCipher for the operating system. Therefore, the configuration guidelines should specify using the latest version of nCipher and the SNMP agent.

4. Instructions to create sequential certificate serial numbers

Sequential serial numbers allow for easier administration (issuing, revoking, unrevoking) and auditing certificates by the CA managers and the CA auditors and for easier administration for other services such as Online Certificate Status Protocol (OCSP) and Standard Based Certificate Validation Protocol (SCVP). Microsoft advertises three different serial number schemes – the default(10 bytes) and two alternates (20 bytes and 14 bytes). All three of those options include a random component that does not allow a sequential serial number.

There is a fourth (unadvertised) option that allows a sequential serial number (i.e. no random component). To get this set one must either use certutil or modify the registry on the CA directly. The registry key is: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\<ca name>\HighSerial. The certutil command line is: certutil –setreg ca \HighSerial “nn” where ’nn’ is a two digit hex number where at least one of the digits is an alpha character. If the value desired is a two digit number without an alpha character, then one must modify the registry directly. To get a sequential serial number the value must be a string (SZ) with the value between 01 and at least 3f (higher values were not tested). Using the value ‘00’ will always result in the default serial number.

It should be further noted that configuring for sequential serial number is secure since SHA-1 collision attack for predictable (e.g., sequential) serial numbers do not have any known, practical exploitation scenarios.

10 Security Target

See Table 1 in this validation report.

11 List of Acronyms

ACM	Configuration Management (Assurance Class)
ADO	Delivery and Operations (Assurance Class)
ADV	TOE Development (Assurance Class)
AGD	Guidance Document (Assurance Class)
ALC	Life Cycle (Assurance Class)
API	Application Programming Interface
ASE	ST Evaluation (Assurance Class)
ATE	TOE Testing (Assurance Class)
AVA	Vulnerability Analysis (Assurance Class)
CA	Certification Authority
CAPI	Cryptographic **API**
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme (US CC Validation Scheme)
CCIMB	Common Criteria Implementation Board
CCTL	Common Criteria Testing laboratory
CEM	Common Evaluation Methodology
CIMC	Certificate Issuing and Management Components
CMC	Certificate Management Messages over Cryptographic Message Syntax
COM	Component Object Model
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DCOM	Distributed Component Object Model
DLL	Dynamically Linked Library
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
FLR	Flaw Remediation
GUI	Graphic User Interface
HP	Hewlett Packard
HSM	Hardware Security Module
I/O	Input/Output
IBM	International Business Machine
IIS	Internet Information Service
ISO	International Organization for Standards
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MMC	Microsoft Management Console
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency

NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PP	Protection Profile
RFC	Request for Comment
RPC	Remote Procedure Call
SAIC	Science Application International Corporation
SSL	Secure Socket Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	**TOE** Security Function
TSFI	**TSF** Interface
URL	Universal Resource Locator
VR	Validation Report

.

12 Bibliography

The validation team used the following documents to prepare the validation report.

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated January 1997, Version 0.6.

[6] Common Evaluation Methodology for Information Technology Security, dated August 1999, Version 1.0.

[7] Final Evaluation Technical Report for Windows Server 2003 Certificate Server, Version 1.0, November 15, 2005.

[8] Microsoft Windows Server 2003 Certificate Server Security Target, V 1.0, November 14, 2005.

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

[10] Evaluation Team Test Plan for Microsoft Windows Server 2003 Certificate Server, Version 1.0, November 15, 2005

[11] Certificate Issuing and Management Components (CIMCs) Security Level 3 Protection Profile, Version 1.0, October 31, 2001.

13 Interpretations

13.1 International Interpretations

The Evaluation Team performed an analysis of the international interpretations and identified those that are applicable and had an impact on the evaluation. The table summarizes the set of interpretations determined to have an impact on the evaluation and identifies the impact.

Interpretation ID	Impact on CC Requirements	Impact on CEM Work Units	Comment
RI-3	New element added after ACM_CAP.2.3C	2:ACM_CAP.2-new added and 2:ACM_CAP.2-7 changed	Applied
RI-4	ACM_SCP.1.1D and ACM_SCP.1.1C changed		Applied
RI-38	ASE_DES.1.1C changed	None	Applied
RI-43	ASE_OBJ.1.2C and ASE_OBJ.1.3C changed	None	Applied
RI-51	ADO_IGS.1.1C, AVA_VLA.1.1D, AVA_VLA.1.2D, AVA_VLA.1.1C changed	None	Applied
RI-84	None	ASE_REQ.1-20 changed	Applied
RI-85	ASE_REQ.1.10C changed	ASE_REQ.1-16 changed	Applied
RI-116	none	2:ADO_DEL.1-2 deleted	Applied

13.2 NIAP Interpretations

Neither the ST nor the vendor’s evidence identified any National interpretations. As a result, since National interpretations are optional, the evaluation team did not consider any National interpretations as part of its evaluation.

13.3 Interpretations Validation

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