National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Microsoft Windows Server 2003, Microsoft Windows XP Professional, and Microsoft Windows XP embedded

Report Number: **CCEVS-VR-VID10184-2008**
Dated: **February 07, 2008**
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
Dawn Campbell
Jean Petty
Quang Trinh
.

Validation Personnel:
Santosh Chokhani, Orion Security Solutions
Scott Shorter, Orion Security Solutions
Shaun Gilmore, National Security Agency

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Microsoft Windows Server 2003, Microsoft Windows XP, and Microsoft Windows XP Embedded. 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 Microsoft Windows Server 2003, Microsoft Windows XP, and Microsoft Windows XP Embedded was performed by the SAIC Common Criteria Testing Laboratory in the United States and was completed during December 2007. 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) have been met.

Windows 2003/XP is an operating system that supports both workstation and server installations. The TOE includes fourteen product variants of Windows 2003/XP:

- Microsoft Windows XP Professional; Service Pack (SP) 2
- Microsoft Windows XP Professional x64; SP 2
- Microsoft Windows XP Embedded, SP 2
- Microsoft Windows Server 2003 Standard; SP 2
- Microsoft Windows Server 2003 R2 Standard; SP 2
- Microsoft Windows Server 2003 Standard x64; SP 2
- Microsoft Windows Server 2003 R2 Standard x64; SP 2
- Microsoft Windows Server 2003 Enterprise; SP 2
- Microsoft Windows Server 2003 R2 Enterprise; SP 2
- Microsoft Windows Server 2003 Enterprise x64; SP 2
- Microsoft Windows Server 2003 R2 Enterprise x64; SP 2
- Microsoft Windows Server 2003, Datacenter Edition x64; SP2
- Microsoft Windows Server 2003 R2, Datacenter Edition x64; SP2
- Microsoft Windows Server 2003 Enterprise Edition with SP2 for Itanium-based Systems

The server products additionally provide Domain Controller (DC) features including the Active Directory (AD) and Kerberos Key Distribution Center (KDC). The server products in the TOE also provide Active Directory Federation Services (ADFS), Windows Server Update Services (WSUS), content indexing and searching, RPC over HTTP proxies, Simple Service Discovery Protocol (SSDP) service, Distributed Transaction Coordinator (DTC), Certificate Server, File Replication, Directory Replication, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Distributed File System (DFS) service, Removable Storage Manager, and Virtual Disk Service. Active Directory is also used by the TOE users to store and retrieve information. The discretionary access control capability and data replication capabilities of the Active Directory Service have been evaluated as part of this evaluation. Although the evaluation had no specific requirements addressing the function of the following services, all were evaluated to ensure they did not permit violations of the specific access control, information flow, or authentication policies

of the TOE: Certificate Server, File Replication, Directory Replication, DNS, DHCP, Distributed File System service, Removable Storage Manager, and Virtual Disk Service.

The reason for this current Windows evaluation over the previous Windows XP and Server 2003 evaluation of September 2006 is the added functionality of WSUS, ADFS, content indexing and searching, Distributed Transaction Coordination (DTC), Simple Service Discovery Protocol (SSDP) service for Universal Plug and Play (UPnP), and RPC over HTTP proxies to the evaluated configuration.

The validation team monitored the activities of the evaluation team, participated in Technical Oversight Panel (TOP) meetings, 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 evaluation. 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 Common Criteria Testing Laboratories (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 evaluations.

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	Microsoft Windows Server 2003, Standard Edition (32-bit version); Service Pack (SP) 2 with security updates and patches as specified in the ST Windows Server 2003, Standard x64 Edition; SP 2 with security

Item	Identifier
	updates and patches as specified in the ST Microsoft Windows Server 2003, R2 Standard Edition (32-bit version); SP 2 with security updates and patches as specified in the ST Microsoft Windows Server 2003, R2 Standard x64 Edition; SP 2 with security updates and patches as specified in the ST Microsoft Windows Server 2003, Enterprise Edition (32-bit and 64-bit versions); SP 2 with security updates and patches as specified in the ST Microsoft Windows Server 2003, Enterprise x64 Edition; SP 2 with security updates and patches as specified in the ST Microsoft Windows Server 2003, R2 Enterprise Edition (32-bit and 64-bit versions); SP 2 with security updates and patches as specified in the ST Microsoft Windows Server 2003, R2 Enterprise x64 Edition; SP 2 with security updates and patches as specified in the ST Microsoft Windows Server 2003, Datacenter x64 Edition; SP 2 with security updates and patches as specified in the ST Microsoft Windows Server 2003, R2 Datacenter x64 Edition; SP 2 with security updates and patches as specified in the ST Microsoft Windows Server 2003 Enterprise Edition with SP2 for Itanium-based Systems Microsoft Windows XP, Professional; SP 2 with security updates and patches as specified in the ST Microsoft Windows XP Professional x64 Edition; SP 2 with security updates and patches as specified in the ST Microsoft Windows XP Embedded; SP 2 with security updates and patches as specified in the ST
Security Target	Microsoft Windows Server 2003, XP Professional and XP Embedded Security Target, Version 3.0, November 19, 2007
Evaluation Technical Report	Microsoft Windows 2003/XP and XP Embedded Delta evaluation, Version 0.4, December 03, 2007.
Conformance Result	CC Part 2 Extended, CC Part 3 augmented, EAL 4 augmented with ALC_FLR.3 Compliant with Control Access Protection Profile (CAPP), Version 1.d, National Security Agency, 8 October 1999
Sponsor	Microsoft Corporation Corporate Headquarters One Microsoft Way Redmond, WA 98052-6399

Item	Identifier
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046-2554
CCEVS Validator(s)	Santosh Chokhani Shaun Gilmore Scott Shorter

3 TOE Security Services

The security services provided by the TOE are summarized below:

- **Security Audit** – Windows 2003/XP has the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes date and time of the event, user who caused the event to be generated, computer where the event occurred, and other event specific data. Authorized administrators can review audit logs. In addition to audit data, the Windows Server Update Services creates extensive logging information. This information is stored and protected in the TOE filesystem.

- **Identification and Authentication** – Windows 2003/XP requires each user to be identified and authenticated (using password or smart card) prior to performing any functions. An interactive user invokes a trusted path in order to protect his I&A information. Windows 2003/XP maintains a database of accounts including their identities, authentication information, group associations, and privilege and logon rights associations. Windows 2003/XP includes a set of account policy functions that include the ability to define minimum password length, number of failed logon attempts, duration of lockout, and password age.

- **Security Management** – Windows 2003/XP includes a number of functions to manage policy implementation. Policy management is controlled through a combination of access control, membership in administrator groups, and privileges.

- **User Data Protection** – Windows 2003/XP protects user data by enforcing several access control policies (DAC, WEBUSER, web content provider access control, and Indexing Service access control) and several information flow policies (IPSec filter information flow control, Connection Firewall, UPnP filtering, and RPC over HTTP); and, object and subject residual information protection. Windows 2003/XP uses access control methods to allow or deny access to objects, such as files, directory entries, printers, and web content. Windows 2003/XP uses information flow control methods to control the flow of IP traffic, UPnP traffic, and RPC over HTTP traffic. It authorizes access to these resources through the use of security descriptors (which are sets of information identifying users and their specific access to resources), web permissions, IP filters, and port mapping rules. Windows 2003/XP also protects user data by ensuring that resources provided to user-mode processes do not have any residual information.

- **Cryptographic Protection -** Windows 2003/XP provides additional protection of data through the use of data encryption mechanisms. These mechanisms only allow authorized users to decrypt encrypted data.

- **Protection of TOE Security Functions** – Windows 2003/XP provides a number of features to ensure the protection of TOE security functions. Windows 2003/XP protects against unauthorized data disclosure and modification by using a suite of Internet standard protocols including IPSec and ISAKMP. The XP portion of the TSF provides the ability to restore previously archived TSF data. Windows 2003/XP provides a Windows Server Update Services that allows authorized administrators the ability to manage software updates and control the propagation of updates to individual machines of the TOE. Windows 2003/XP ensures TOE self-protection and process isolation for all processes through private virtual address spaces, execution context and security context. The Windows 2003/XP data structures defining process address space, execution context, memory protection, and security context are stored in protected kernel-mode memory.

- **Resource Utilization** – Windows 2003/XP can limit the amount of disk space that can be used by an identified user or group on a specific disk volume. Each volume has a set of properties that can be changed only by a member of the administrator group. These properties allow an authorized administrator to enable quota management, specify quota thresholds, and select actions when quotas are exceeded.

- **TOE Access** – Windows 2003/XP provides the ability for a user to lock their session immediately or after a defined interval. It constantly monitors the mouse and keyboard for activity and locks the workstation after a set period of inactivity. Windows 2003/XP allows an authorized administrator to configure the system to display a logon banner before the logon dialogue.

4 Assumptions

4.1 Physical Security Assumptions

- The processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4.2 Personnel Security Assumptions

- Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

4.3 Connectivity Assumptions

- All connections to peripheral devices reside within the controlled access facilities. The TOE only addresses security concerns related to the manipulation of the TOE through its authorized access points. Internal communication paths to access points such as terminals are assumed to be adequately protected.
- Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. The TOE is

applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements that address the need to trust external systems or the communications links to such systems.

5 Architectural Information

The diagram below depicts components and subcomponents of Windows 2003/XP that comprise the TOE. The components/subcomponents are large portions of the Windows 2003/XP OS, and generally fall along process boundaries and a few major subdivisions of the kernel mode OS.

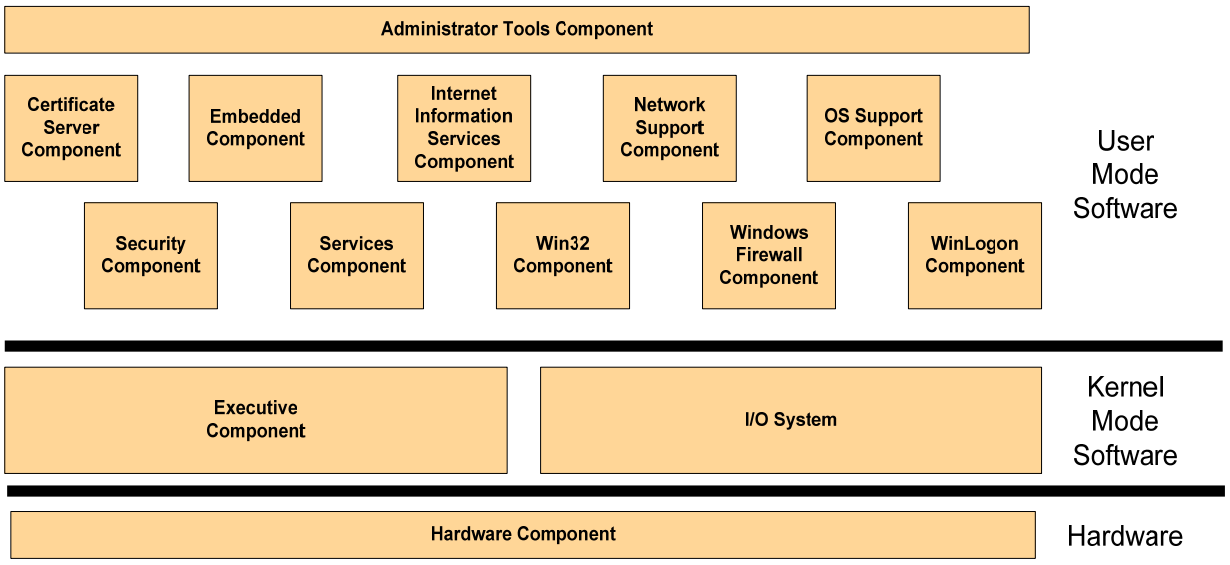

Figure 1: TOE Components

The system components are:

- Administrator Tools Module
  - Administrator Tools Component (aka GUI Component): This component represents the range of tools available to manage the security properties of the TSF.
- Certificate Services Module
  - Certificate Server Component: This component provides services related to issuing and managing public key certificates (e.g. X.509 certificates). However, no certificate server related security functions have been specified or evaluated in the TOE.
- Embedded Module
  - Embedded Component: This component provides a variety of applications that facilitate the OS functioning in devices that require an embedded OS.
- Firewall Module
  - Windows Firewall Component: This component provides services related to information flow control.

- Hardware Module
    - Hardware Component: This component includes all hardware used by the TSF to include the processor(s), motherboard and associated chip sets, controllers, and I/O devices.
- Kernel Software Module
    - Executive Component: This is the kernel-mode software that provides core OS services to include memory management, process management, and inter-process communication. This component implements all the non-I/O TSF interfaces for the kernel-mode.
    - I/O System: This is the kernel-mode software that implements all I/O related services, as well as all driver-related services. The I/O System is further divided into:
        - I/O Core Component
        - I/O File Component
        - I/O Network Component
        - I/O Devices Component
- Miscellaneous OS Support Module
    - OS Support Component: This component is a set of processes that provide various other OS support functions and services
- RPC and Network Support Module
    - Network Support Component: This component contains various support services for Remote Procedure Call (RPC), COM, and other network services.
- Security Module
    - Security Component: This component includes all security management services and functions.
- Services Module
    - Services Component: This is the component that provides many system services as well as the service controller.
- Web Services Module
    - IIS Component: This component provides services related to web/http requests.
- Win32 Module
    - Win32 Component: This component provides various support services for Win32 applications and the command console application.
- WinLogon Module
    - WinLogon Component: This component provides various interactive logon services to include interactive authentication, trusted path, session management and locking.

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor):

Assurance Class	Document Title
ASE	Microsoft Windows Server 2003, XP Professional and XP Embedded Security Target Version 3.0, November 19, 2007
ACM	Windows Server 2003 SP2 and Windows XP SP2 With ADFS and WSUS Configuration Management Manual, Version 0.2, May 23, 2007
ADO	• Windows Server 2003 SP2 and Windows XP SP2 with ADFS and WSUS Delivery Procedures, Version 0.1, July 27, 2006. • Windows Server 2003 with SP2 Security Configuration Guide, Version 3.0, May 22, 2007 • Windows XP Professional with SP2 Security Configuration Guide, Version 3.0, May 22, 2007

Assurance Class	Document Title

ADV	• System Decomposition, Rev: 2, 11/09/2006
	• Informal TOE Security Policy Model Design Specification, Rev: 4 03/05/2007
	• Functional Specification Completeness Rationale, Rev: 5, 1/27/2005
	• API Correspondence Rules, Rev 3, 2/18/2004
	• Implementation Subset Representation:
	  • Embedded: Enhanced Write Filter Driver
	  • Executive: Security Reference Monitor, Process Manager and Object Manager
	  • Internet Information Server: Internet Information Services, Indexing Service Webhits, ADFS Web Agent ISAPI Extension,
	  • IO Core: Mount Manager
	  • IO Devices: IDE/ATAPI Port Driver and FIPS Crypto Driver
	  • IO File: NPFS Driver and NT File System Driver
	  • IO Network TCP/IP Protocol Driver, Distributed File System Filter Driver,
	  • Network Support: Domain Name Service
	  • OS Support: Session Manager, Smart Card Resource Manager, Distributed File System Replication Service, License Logging Service
	  • Security: LSA Audit and Secondary Logon Service, Windows Update AutoUpdate Engine
	  • Services: Service Controller, Windows Update AutoUpdate Engine,
	  • Win32: Client Server Runtime Process
	  • Windows Firewall Application Layer Gateway Service
	  • WinLogon: WinLogon/GINA
	• Component and Subcomponent Design Specification (see Appendix A of Non-Prop ETR)

Assurance Class	Document Title
AGD	• Windows Server 2003 with SP2 Evaluated Configuration Administrator's Guide, Version 3.0, May 21, 2007 • Windows XP Professional with SP2 Evaluated Configuration Administrator's Guide, Version 3.0, May 21, 2007 • Windows XP Professional with SP2 Evaluated Configuration User's Guide, Version 3.0, February 26, 2007
ALC	• Windows Server 2003 SP2 and Windows XP SP2 With ADFS and WSUS Assurance Lifecycle, Version 0.1 July 27, 2006 • Windows Server 2003 SP2 and Windows XP SP2 With ADFS and WSUS Configuration Management Manual, Version 0.1, July 27, 2006
ATE	• Test Documents o ACL Test Suite, Rev 2.9, 08/04/2006 o ADFS Security Package Subcomponent Test Suite, Rev 1, 9/6/2006 o ADFS Web Agent Authentication Service Subcomponent Test Suite, Rev 1, 1/25/2007 o ADFS Web Agent ISAPI Extension Subcomponent Test Suite, Rev 1.0, 11/13/2006 o Admin Access Test Suite, Rev 1.5, 08/04/2006 o ASP.NET ISAPI Filter Subcomponent Test Suite, Rev 2, 10/10/2006 o Authentication Provider Test Suite, Rev 1.4, 08/02/2006 o Background Intelligent Transfer Service Subcomponent Test Suite, Rev 2, 1/26/2007 o BITS Server Extensions ISAPI Subcomponent Test Suite, Rev 2, 1/26/2007 o Certificate Server Test Suite, Rev 1.9, 08/3/2006 o COM+ Test Suite, Rev 1.6, 08/04/2006 o COM+ Event System Service Test Suite, Rev 1.3, 08/04/2006 o Content Index Service Subcomponent Test Suite, Rev: 3, 6/03/2006 o Data Execution Prevention Test Suite, Rev: 4, 4/25/2006 o DCOM Test Suite, Rev 1.8, 06/08/2006 o Devices Test Suite, Rev 1.4, 08/04/2006 o Distributed File System Filter Driver Subcomponent Test Suite, Rev 1, 11/22/2006 o Distributed File System Replication Service Subcomponent Test Suite, Rev 3, 1/25/2007 o Distributed Transaction Coordinator Subcomponent Test Suite, Rev: 2, 6/19/2006 o DS Replication Test Suite, Rev 1.6, 09/30/2005 o Federation Server and ADFS Identity Authentication Subcomponent Test Suite, Rev 18, 5/10/2007 o GDI Test Suite, Rev 1.8, 08/04/2006 o Handle Enforcement Test Suite, Rev 2.10, 08/04/2006 o Help and Support Subcomponent Test Suite, Rev: 3, 4/26/2006 o HTTP Client Test Suite, Rev 1.6, 08/03/2006 o IA32 Hardware Test Suite, Rev 1.5, 08/03/2006 o IA64 Hardware Test Suite, Rev: 3, 5/02/2006 o IMAPI Kernel Driver Subcomponent Test Suite, Rev: 3, 5/29/2006

Assurance Class	Document Title
	o Impersonation Test Suite, Rev 1.10, 08/04/2006 o Indexing Service ISAPI Extension Subcomponent Test Suite, Rev: 5, 6/06/2006 o Indexing Service Webhits Subcomponent Test Suite, Rev: 3, 6/07/2006 o IPSEC Test Suite, Rev 2.4, 08/03/2006 o KDC Test Suite, Rev 1.9, 08/04/2006 o LDAP Test Suite, Rev 1.10, 08/04/2006 o License Logging Service Subcomponent Test Suite, Rev: 6, 8/03/2006 o Managed Code Single Sign On Library Subcomponent Test Suite, Rev 3, 3/2/2007 o Managed Code SSO Claim Transforms Subcomponent Library Test Suite, Rev 99, 8/31/2006 o MAPI Test Suite, Rev 1.4, 08/04/2006 o Miscellaneous Test Suite, Rev 3.2, 08/04/2006 o Net Support Test Suite, Rev: 3, 4/03/2006 o Object Reuse Test Suite, Rev 1.4, 08/04/2006 o ODBC HTTP Server Extension Subcomponent Test Suite, Rev 2, 4/04/2007 o Privilege Test Suite, Rev 2.7, 08/04/2006 o RSoP Service Application Subcomponent Test Suite, Rev: 8, 6/22/2006 o RPC Proxy Subcomponent Test Suite, Rev: 4, 5/22/2007 o Server Driver Test Suite, Rev 0.8, 08/04/2006 o Simple Targeting Authorization Web Service Subcomponent Test Suite, Rev 1, 12/12/2006 o Special Access Test Suite, Rev: 7, 6/01/2006 o System Restore Service Subcomponent Test Suite, Rev: 7, 4/24/2006 o Task Scheduler Engine Subcomponent Test Suite Rev: 11, 5/26/2006 o Test Plan, Rev: 8, 5/29/2006 o Token Test Suite, Rev 1.8, 08/04/2006 o UPnP Device Host Subcomponent Test Suite, Rev: 6, 5/30/2006 o User Test Suite, Rev 1.13, 08/03/2006 o Windows Error Reporting Service Subcomponent Test Suite, Rev: 3, 5/26/2006 o Windows Firewall Test Suite, Rev 1.5, 08/01/2006 o Windows Update AutoUpdate Engine Subcomponent Test Suite, Rev 1, 11/8/2006 o Windows Update AutoUpdate Service Subcomponent Test Suite, Rev 1, 11/8/2006 (manual test) o WSUS Catalog Sync Agent Subcomponent Test Suite, Rev 1, 2/21/2007 o WSUS Client Web Service Subcomponent Test Suite, Rev 1, 1/24/2007 o WSUS Content Sync Agent Subcomponent Test Suite, Rev 3, 2/21/2007 o WSUS Reporting Web Service Subcomponent Test Suite, Rev 1, 12/12/2006 o WSUS Server Sync Web Service Test Suite, Rev 5, 11/13/2006

Assurance Class	Document Title
	o X64 Hardware Test Suite, Rev: 5, 5/01/2006 • GUI Tests o Active Directory Domains and Trusts GUI, Version 0.8, 09/26/05 o AT.exe Command GUI, Version 0.2, 5/10/2007 o Auditusr.exe GUI, Version 0.2, 09/09/2005 o Automatic Updates (WSUS Client), Version 0.3, 4/09/2207 o Backup and Restore GUI, Version 0.4, 03/22/2005 o Certification Authority GUI, Version 1.2, 09/23/05 o COM+ Apps Test Plan/Procedures, Rev. 1.0, 08/01/2005 o Data Execution Prevention Test Suite, April 25, 2006, Revision 4 o Date and Time GUI, Version 0.3, 09/26/2005 o Device Manager GUI, Version 0.2, 09/09/2005 o Disk Quota GUI, Version 0.2, 03/22/2005 o Event Viewer GUI, Version 1.2, 09/03/05 o Explorer GUI, Version 0.3, 09/21/2005 o IIS Mgr Test Plan/Procedures", Rev. 1.0, 9/23/2005 o Indexing Service, Version 0.2, 5/09/07 o Network ID GUI, Version 0.3, 09/12/2005 o OU Delegation GUI, 06/06/2005 o Printers GUI, Version 0.2, 09/22/2005 o Registry Editor GUI, Version 0.2, 03/22/2005 o Resultant Set of Policy and Resultant Set of Policy Provider, Version 0.1, 9/19/2006 o Services GUI, Version 0.2, 03/22/2005 o Session Locking GUI, Version 0.3, 09/26/2005 o Share a Folder Wizard, Version 0.2, 09/08/2003 o Users and Groups GUI, Version 0.8, 09/26/2005 o WinLogon/GINA, Rev. 1.6, 09/22/2005 o Scheduled Tasks, Version 0.3, 5/10/2007 o Security Policy GUI, v.1.7, 08/09/2005 o System Restore, Version 0.1, 10/10/2006 o Task Scheduler (Schtasks.exe), Version 0.2, 5/10/2007 o WSUS, Version 0.3, 4/09/2007 • Test Code for each Test Suite • Test Results as referenced by test cases
AVA	• Windows Server 2003 SP2 and Windows XP SP2 with ADFS and WSUS Misuse Analysis, Version 0.2, January 26, 2007 • Windows Server 2003 SP2 and Windows XP SP2 with ADFS and WSUS Strength of Function Analysis, Version 0.2, December 19, 2006 • Microsoft Windows Server 2003 with SP2/XP Professional with SP2 Vulnerability Analysis Version 3.0, Draft Version 0.04, May 11, 2007

7 IT Product Testing

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

7.1 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.

7.2 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. Thus the independent set of team tests was limited. The team tests were devised to focus on the added functionality in this delta evaluation, building on the team testing performed in November 2005 and September 2006 evaluations. A total of six (6) team tests were devised and covered the following areas: TSF Security Functions Management, Security Audit, User Data Protection, and TSF Protection.

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 five (5) penetration tests. The penetration tests fall in the following areas: ADFS, WSUS, access authentication credential, and extensive vulnerability search of the public domain. The penetration tests were focused on the main services evaluated in this delta evaluation.

7.3 Residual Vulnerability

The intent of the TOE design is to accept WSUS updates signed by a code signing authority from a trusted publisher or a code signer rooted in one of the two Microsoft Roots. However, due to a bug in the implementation, a WSUS update signed by any code signer who terminates into any one of the many trusted root certification authorities installed in the TOE is accepted, thus increasing the potential population of persons who can provide a Windows Update and making the TOE vulnerable to unauthorized updates.

This threat is significantly mitigated by the fact that WSUS updates and related metadata (including the hash of the updates) on the various Servers and targets are controlled by administrative DAC and the updates and related metadata (including the hash of the updates) are protected by SSL during transit.

8 Evaluated Configuration

The evaluated configuration identified in this section was also the test configuration. The evaluation results are valid for the various realizable combinations of configurations of hardware and software listed in this section. A homogeneous Windows system consisting of various Servers, Domain Controllers, and Workstations using the various hardware and software listed in this section maintains its security rating when operated using the secure usage assumptions listed in Section 4 of this validation report, including the connectivity assumptions listed in Section 4.3 of this validation report.

TOE Hardware – The evaluation results are valid for the following hardware platforms. The TOE testing was also conducted on these platforms.

Manufacturer	Model	Processor(s)	Memory
Dell	Optiplex GX620	3.0 GHz Intel Pentium D Processor 830 (1 CPU), 32-bit	2GB
Dell	PowerEdge SC1420	3.0 GHz Intel Xeon Processor (1 CPU), 32-bit	1GB
Dell	PowerEdge SC1420	3.6 GHz Intel Xeon Processor (1 CPU), 32-bit	2GB
Dell	PowerEdge 1800	3.2 GHz Intel Xeon Processor (1 CPU), 32-bit	2GB
Dell	PowerEdge 2850[1]	2.8 GHz Intel Xeon Processor (2 Dual-Core CPUs), 64-bit	4GB
HP	Proliant DL385	2.6 GHz AMD Opteron Processor 252 (2 CPUs), 64-bit	2GB
HP	rx1620 Bundle Solution Server	1.3 GHz Intel Itanium Processor (1 CPU), 64-bit	2GB
HP	xw9300 Workstation	2.2 GHz AMD Opteron Processor 248 (1 CPU), 64-bit	2GB
IBM	eServer 326m	2.0 GHz AMD Opteron Processor 270 (1 Dual-Core CPU), 64-bit	2GB
IBM	eServer 326m	2.4 GHz AMD Opteron Processor 280 (2 Dual-Core CPUs), 64-bit	2GB
Unisys	RASCAL ES7000	3.0 GHz Intel XeonMP EM64T Processor (32 CPUs), 64-bit	64GB
GemPlus	GemPC Twin USB smart cards		

TOE Software Identification – The evaluation results are valid for the following Windows Operating Systems when security updates listed in this section are applied. The TOE testing was conducted for these Operating Systems after applying the security updates listed in this section:

- Microsoft Windows XP Professional; Service Pack (SP) 2
- Microsoft Windows XP Professional x64; SP 2
- Microsoft Windows XP Embedded, SP 2
- Microsoft Windows Server 2003 Standard; SP 2
- Microsoft Windows Server 2003 R2 Standard; SP 2
- Microsoft Windows Server 2003 Standard x64; SP 2
- Microsoft Windows Server 2003 R2 Standard x64; SP 2
- Microsoft Windows Server 2003 Enterprise; SP 2
- Microsoft Windows Server 2003 R2 Enterprise; SP 2
- Microsoft Windows Server 2003 Enterprise x64; SP 2

- Microsoft Windows Server 2003 R2 Enterprise x64; SP 2
- Microsoft Windows Server 2003, Datacenter Edition x64; SP2
- Microsoft Windows Server 2003 R2, Datacenter Edition x64; SP2
- Microsoft Windows Server 2003 Enterprise Edition with SP2 for Itanium-based Systems

The following security updates and patches must be applied to the above Windows Server 2003 products:

- MS07-029: Vulnerability in Windows DNS RPC Interface Could Allow Remote Code Execution (KB935966)
- MS07-022: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (KB931784) – x86 only
- MS07-021: Vulnerabilities in CSRSS Could Allow Remote Code Execution (KB930178)
- MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution (KB925902)
- Software Update for Base Smart Card Cryptographic Service Provider: An associated Microsoft Security Bulletin for this issue is not available (KB909520)

The following security updates must be applied to the above XP products:

The following apply to all XP products:

- MS07-021: Vulnerabilities in CSRSS Could Allow Remote Code Execution (KB930178)
- MS07-017: Vulnerabilities in GDI Could Allow Remote Code Execution (KB925902)
- Software Update for Base Smart Card Cryptographic Service Provider: An associated Microsoft Security Bulletin for this issue is not available (KB909520).

The following updates are necessary for XP professional 32-bit only:

- MS07-022: Vulnerability in Windows Kernel Could Allow Elevation of Privilege (KB931784)
- MS07-006: Vulnerability in Windows Shell Could Allow Elevation of Privilege (KB928255)
- MS06-075: Vulnerability in Windows Could Allow Elevation of Privilege (KB926255)
- MS06-070: Vulnerability in Workstation Service Could Allow Remote Code Execution (KB924270)
- MS06-065: Vulnerability in Windows Object Packager Could Allow Remote Execution (KB924496)
- MS06-064: Vulnerabilities in TCP/IP IPv6 Could Allow Denial of Service (KB922819)
- MS06-063: Vulnerability in Server Service Could Allow Denial of Service (KB923414)
- MS06-061: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (KB924191)
- MS06-057: Vulnerability in Windows Explorer Could Allow Remote Execution (KB923191)
- MS06-056: Vulnerability in ASP.NET 2.0 Could Allow Information Disclosure (KB922770)
- Update for Windows XP (KB922582) - This update resolve an issue identified in Filter Manager that can prevent you from installing updates from Windows update.

- Update for Windows XP (KB910437) - This update resolve an issue in which Windows Update and Automatic Updates can no longer download updates after an Access Violation error occurs when using the Automatic Updates service
- MS06-053: Vulnerability in Indexing Service Could Allow Cross-Site Scripting (KB920685)
- MS06-045: Vulnerability in Windows Explorer Could Allow Remote Code Execution (KB921398)
- MS06-042: Cumulative Security Update for Internet Explorer (KB918899)
- MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution (KB920683)
- MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (KB921883)
- MS06-036: Vulnerability in DHCP Client Service Could Allow Remote Code Execution (KB914388)
- MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (KB917159)
- MS06-030: Vulnerability in Server Message Block Could Allow Elevation of Privilege (KB914389)
- MS06-018: Vulnerability in Microsoft Distributed Transaction Coordinator Could Allow Denial of Service (KB913580)
- MS06-015: Vulnerability in Windows Explorer Could Allow Remote Code Execution (KB908531)
- MS06-008: Vulnerability in Web Client Service Could Allow Remote Code Execution (KB911927)
- MS06-001: Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution (KB912919)
- MS05-053: Vulnerabilities in Graphics Rendering Engine Could Allow Code Execution (KB896424)
- MS05-051: Vulnerabilities in MSDTC and COM+ Could Allow Remote Code Execution (KB902400)
- MS05-049: Vulnerabilities in Windows Shell Could Allow Remote Code Execution (KB900725)
- MS05-047: Vulnerability in Plug and Play Could Allow Remote Code Execution and Local Elevation of Privilege (KB905749)
- IPSec Policy Agent Update: An associated Microsoft Security Bulletin for this issue is not available.(KB907865)
- MS05-043: Vulnerability in Print Spooler Service Could Allow Remote Code Execution (KB896423)
- MS05-042: Vulnerabilities in Kerberos Could Allow Denial of Service, Information Disclosure, and Spoofing (KB899587)
- MS05-027: Vulnerability in Server Message Block Could Allow Remote Code Execution (KB896422)
- MS05-018: Vulnerability in Windows Kernel Could Allow Elevation of Privilege and Denial of Service (KB890859)

- MS05-011: Vulnerability in Server Message Block Could Allow Remote Code Execution (KB885250)
- MS05-007: Vulnerability in Windows Could Allow Information Disclosure (KB888302)
- MS04-044: Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege (KB885835)

9 Validator Comments

The TOE developer and sponsor, and the Evaluation Team are commended for their effort to develop tests for such a complex system. The Evaluation Team is commended for their painstaking efforts to validate the evaluated configuration during team testing.

The security functional testing activities were limited to verifying that the security checks at each TSFI are enforced. The TSFI input parameters were not exercised for erroneous and anomalous inputs during security functional testing or during penetration testing.

While no specific security functional requirements or TSFI are listed for the following components of the TOE, the TOE was not evaluated in the following areas and is known to be not compliant with applicable standards and hence can cause security and interoperability problems:

- The Microsoft Cryptographic Applications Programming Interface (CAPI) does not perform X.509 certification path validation in accordance with applicable ISO and Internet standards.

- The Internet Information Server (IIS) Transport Layer Security (TLS) and Secure Socket Layer (SSL) do not perform X.509 certification path validation for client authentication in accordance with applicable ISO and Internet standards

Consumer should look at the Developer's vulnerability analysis for residual vulnerabilities when the TOE is connected to the Internet.

The value of WSUS in the evaluated configuration is limited. Only the updates explicitly listed in the ST can be distributed with WSUS.

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)
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
COM	Component Object Model
DEP	**Data Execution Prevention**
DHCP	Dynamic Host Control Protocol
DNS	Domain Name Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
FLR	Flaw Remediation
GUI	Graphic User Interface
HP	Hewlett Packard
I/O	Input/Output
IBM	International Business Machine
IIS	Internet Information Service
IPSEC	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standards
IT	Information Technology
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
RPC	Remote Procedure Call
SAIC	Science Application International Corporation
SSL	Secure Socket Layer

ST	Security Target
TLS	Transport Layer Security
TOE	Target Of Evaluation
TOP	Technical Oversight Panel
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 2005, Version 2.3.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, Version 2.3.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 2.3, August 2005.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated August 2005, Version 2.3.

[6] Common Evaluation Methodology for Information Technology Security, Version 2.3, August 2005.

[7] Final Evaluation Technical Report for Microsoft Windows 2003/XP and XP Embedded Delta evaluation Part 2.

[8] Microsoft Windows Server 2003, XP Professional and XP Embedded Security Target, Version 3.0, November 19, 2007

[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 2003/XP, Version 1.2, 28 November, 2007

13 Interpretations

13.1 International Interpretations

The evaluation team performed an analysis of the international interpretations and identified those that are applicable and had impact to the TOE evaluation. There no interpretations identified that impacted the evaluation.

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.