National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

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

Microsoft Windows Vista and Windows Server 2008

Report Number: **CCEVS-VR-VID10291-2009**
Dated: **15 August 2009**
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 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

James Donndelinger
Aerospace Corporation
Columbia, MD

Shaun Gilmore
National Security Agency
Ft. Meade, MD

Common Criteria Testing Laboratory

Tony Apted
Tammy Compton
Terrie Diaz
Eve Pierre
Quang Trinh
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Microsoft Windows Vista and Windows Server 2008. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, as well as evaluators from the National Security Agency (NSA) and was completed in August 2009. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, written in part by SAIC and in part by NSA. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.3, AVA_VLA.3.

The Target of Evaluation (TOE) is Windows Vista and Windows Server 2008 provided by Microsoft, Corp. Windows Vista and Windows Server 2008 are preemptive multitasking, multiprocessor, and multi-user operating systems. In general, operating systems provide users with a convenient interface to manage underlying hardware. They control the allocation and manage computing resources such as processors, memory, and Input/Output (I/O) devices. Windows Vista and Windows Server 2008 expand these basic operating system capabilities to controlling the allocation and managing higher level IT resources including security principals (user and machine accounts), files, printing objects, services, windowstation, desktops, cryptographic keys, network ports/traffics, directory objects, and web content. Multi-user operating systems such as Windows Vista and Windows Server 2008, keep track of which user is using which resource, grant resource requests, account for resource usage, and mediate conflicting requests from different programs and users.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated in part at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) and in part by NSA for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). 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 NSA and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

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.

Based upon the work of the SAIC evaluation team and NSA evaluation team, the CCEVS concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.3 have been met.

The technical information included in this report was obtained from the Windows Vista and Windows Server 2008 Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the 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 evaluation. Upon successful completion of the evaluation, the product is added to 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 Protection Profile to which the product is conformant.
- 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
TOE:	Windows Vista and Windows Server 2008
Protection Profile	Controlled Access Protection Profile, Version 1.d, National Security Agency, 8 October 1999
ST:	Windows Vista and Windows Server 2008 Security Target, Version 1.0, July 24, 2009
Evaluation Technical Report	Evaluation Technical Report For Windows Vista and Windows Server 2008 (Proprietary), Version 2.0, August 3, 2009
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3
Conformance Result	CC Part 2 extended, CC Part 3 conformant

Item	Identifier
Sponsor	Microsoft Corporation
Developer	Microsoft Corporation
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	James Donndelinger, Aerospace Corporation, Columbia, MD
	Shaun Gilmore, National Security Agency, Ft. Meade, MD

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Overview

Windows Vista and Windows Server 2008 are operating systems that supports both workstation and server installations. The TOE includes four product variants of Windows Vista and Windows Server 2008: Windows Vista Enterprise, Windows Server 2008 Standard, Windows Server 2008 Enterprise, and Windows Server 2008 Datacenter. The server products additionally provide DC features including the Active Directory and Kerberos Key Distribution Center (KDC). The server products in the TOE also provide Internet Information Services (IIS), Certificate Services, RPC over HTTP Proxy, File Replication, Directory Replication, Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Distributed File System (DFS) service, and Removable Storage Manager. All variants include the same security features. The primary difference between the variants is the number of users and types of services they are intended to support.

Windows Vista is suited for business desktops and notebook computers (note that only desktops are included in the evaluated configuration); it is the workstation product. Designed for departmental and standard workloads, Windows Server 2008 Standard delivers intelligent file and printer sharing; secure connectivity based on Internet technologies, and centralized desktop policy management. Windows Server 2008 Enterprise differs from Windows Server 2008 Standard primarily in its support for high-performance servers for greater load handling. These capabilities provide reliability that helps ensure systems remain available. Windows Server 2008 Datacenter provides the necessary scalable and reliable foundation to support mission-critical solutions for databases, enterprise resource planning software, high-volume, real-time transaction processing, and server consolidation.

The security features addressed by this security target are those provided by Windows Vista and Windows Server 2008 as operating systems. Microsoft provides several Window Vista and Windows Server 2008 software applications that are considered outside the scope of the defined TOE and thus not part of the evaluated configuration. Services outside this evaluation include: e-mail service, Terminal Service, Microsoft Message Queuing, Right Management Service, ReadyBoost, and support for Multiple Concurrent Users (e.g., quick

user switching). The features identified and described in this section are included in the TOE and as such are within the scope of the evaluation.

The following table summarizes the TOE configurations included in the evaluation.

	Windows Vista Enterprise (32 bit and 64 bit)	Windows Server 2008 Standard (64 bit)	Windows Server 2008 Enterprise (64 bit)	Windows Server 2008 Datacenter
Single Processor	X	X	X	N/A
Multiple Processor	X	X	X	X
Stand-alone	X	X	X	X
Domain Member	X	X	X	X
Domain Controller	N/A	N/A	X	X
Variations as a Domain Element	2	2	4	2
Total Variations	4	4	6	3

3.2 TOE Physical Boundaries

Physically, each TOE workstation or server consists of an x86 or x64 machine or equivalent processor (from the Intel Celeron, Intel Pentium, Intel Core 2, AMD Sempron, AMD Athlon, or AMD Phenom processor families) with up to four (4) CPUs for a standard Server product, up to eight (8) CPUs for the Enterprise Server product, and up to 32 CPUs for the Datacenter product. A set of devices may be attached and they are listed as follows:

- Display Monitor,
- Keyboard,
- Mouse,
- CD-ROM Drive
- Fixed Disk Drives,
- Printer,
- Audio Adaptor,
- Network Adaptor, and
- Smart Card Reader.

The TOE does not include any physical network components between network adaptors of a connection. The ST assumes that any network connections, equipment, and cables are appropriately protected in the TOE security environment.

3.3 TOE Logical Boundary

This section identifies the security functions that the TSF provides.

- Security Audit
- User data protection
- Identification and authentication
- Security management
- Cryptographic protection
- Protection of the TOE Security Functions
- Resource Utilization
- Session Locking

3.3.1 Security Audit

Windows Vista and Windows Server 2008 have 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.

3.3.2 User Data Protection

Windows Vista and Windows Server 2008 protect user data by enforcing several access control policies (Discretionary Access Control, Mandatory Integrity Control, Encrypting File System, WEBUSER and web content provider access control) and several information flow policies (IPSec filter information flow control, Windows Firewall); and, object and subject residual information protection. Windows Vista and Windows Server 2008 use access control methods to allow or deny access to objects, such as files, directory entries, printers, and web content. Windows Vista and Windows Server 2008 uses information flow control methods to control the flow of IP traffic and packets. It authorizes access to these resource objects through the use of security descriptors (SDs, which are sets of information identifying users and their specific access to resource objects), web permissions, IP filters, and port mapping rules. Windows Vista and Windows Server 2008 also protects user data by ensuring that resources exported to user-mode processes do not have any residual information.

3.3.3 Identification and Authentication

Windows Vista and Windows Server 2008 require 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 Vista and Windows Server 2008 maintain databases of accounts including their identities, authentication information, group associations, and privilege and logon rights associations. Windows Vista and Windows Server 2008 include 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.

3.3.4 Security Management

Windows Vista and Windows Server 2008 include a number of functions to manage policy implementation. Policy management is controlled through a combination of access control, membership in administrator groups, and privileges.

3.3.5 Cryptographic Protection

Windows Vista and Windows Server 2008 provide FIPS-140-2 validated cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, cryptographic key agreement, and random number generation. The TOE additionally provides support for public keys, credential management and certificate validation functions and provides support for the National Security Agency's Suite, B crypto algorithms. The TOE also provides extensive auditing support in support of crypto requirements, support for replaceable random number generators, and a key isolation service designed to limit the potential exposure of secret and private keys.

3.3.6 Protection of TOE Security Functions

Windows Vista and Windows Server 2008 provide a number of features to ensure the protection of TOE security functions. Windows Vista and Windows Server 2008 protects against unauthorized data disclosure and modification by using a suite of Internet standard protocols including IPSec and ISAKMP. Windows Vista and Windows Server 2008 ensure process isolation security for all processes through private virtual address spaces, execution context and security context. The Windows Vista and Windows Server 2008 data structures defining process address space, execution context, memory protection, and security context are stored in protected kernel-mode memory. BitLocker protects hard drive data by providing Secure Startup (integrity checking of early boot components) and Full Volume Encryption (FVE). FVE protects data by encrypting entire disk volumes; in the case of the Windows operating system volume, this includes the swap and hibernation files. Secure Startup provides integrity checking of the early boot components, ensuring that FVE decryption is performed only if those components are found to be unchanged and the encrypted drive is located in the original computer.

3.3.7 Resource Utilization

Windows Vista and Windows Server 2008 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.

3.3.8 Session Locking

Windows Vista and Windows Server 2008 provide 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 Vista and Windows Server 2008 allow an authorized administrator to configure the system to display a logon banner that describes usage policies before the logon dialog.

4 Assumptions

The following assumptions were made during the evaluation of Windows Vista and Windows Server 2008:

- 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.
- 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.
- 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.

5 Documentation

The following documentation was used as evidence for the evaluation of the Windows Vista and Windows Server 2008:

5.1 Configuration Management

1. Validated through an NSA approved evaluation process

5.2 Delivery and Operation

1. Microsoft Windows Common Criteria Evaluation Document, version 6, July 29, 2009

5.3 Design Documentation

1. See the Design Documentation List at the end of the document.

5.4 Guidance Documentation

1. Microsoft Windows Common Criteria Evaluation Document, version 6, Tuesday, July 29, 2009
2. Windows Vista Security Guide - http://technet.microsoft.com/en-us/library/cc507874.aspx
3. Windows Server 2008 Security Guide - http://technet.microsoft.com/en-us/library/cc264463.aspx

5.5 Life Cycle

1. Validated through an NSA approved evaluation process.

5.6 Testing

1. Microsoft Windows Common Criteria Evaluation Test Plan, Rev: 14, 7/29/2009
2. 64 Bit Kernel Debug Support Test Suite, Rev: 1, 11/30/2007
3. Access Control (ACL) Test Suite, Rev: 5, 07/19/2009
4. ACPI Driver Test Suite,, Rev: 3, 02/09/2009
5. Administrator Access Test Suite, Rev: 22, 07/19/2009
6. Advanced Local Process Communication Test Suite, Rev: 4, 06/25/2009
7. Application Compatibility Support Test Suite, Rev: 5, 06/13/2009
8. Application Experience Lookup Service Test Suite, Rev: 2, 05/12/2008
9. Application Information Service Test Suite, Rev: 3, 04/23/2009
10. Authentication Provider Test Suite, Rev: 1.3, 05/27/2009
11. Background Intelligent Transfer Service Test Suite, Rev: 11, 07/04/2009
12. Base Filtering Engine Service Test Suite, Rev: 2, 04/09/2009
13. Bits Server ISAPI Extensions Test Suite, Rev: 2, 04/29/2009
14. Bowser Driver Test Suite, Rev: 1, 06/23/2009
15. (OS) Certificate Server Test Suite, Rev 2.0, 06/04/2009
16. Client Side Caching Driver Test Suite, Rev: 4, 06/30/2009
17. COM+ Test Suite, Rev: 4, 07/06/2009
18. COM+ Event System Service Test Suite, Rev: 2.1, 07/03/2009

19. Computer Browser Service Test Suite, Rev: 4, 06/04/2009
20. Configuration Manager Test Suite, Rev: 4, 07/05/2009
21. Credential Manager Test Suite, Rev: 6, 06/13/2009
22. Data Execution Prevention Test Suite, Rev: 99, 04/24/2009
23. Desktop Window Manager Test Suite, Rev: 1.0, 07/04/2009
24. Devices Test Suite, Rev: 99, 04/24/2009
25. Directory Services Replication Test Suite, Rev: 2.1, 06/05/2009
26. Distributed COM Services Test Suite, Rev: 2.1, 02/06/2009
27. Distributed File System Filter Driver Test Suite, Rev: 1, 11/22/2006)
28. Distributed File System Replication Service Test Suite, Rev: 6, 02/04/2009
29. Distributed Transaction Coordinator Test Suite, Rev: 2, 06/19/2009
30. Event Tracing For Windows Test Suite, Rev: 1, 07/05/2009
31. Executive Object Services Test Suite, Rev: 6, 07/06/2009
32. Fileinfo Fs Minifilter Driver Test Suite, Rev: 2, 06/23/2008
33. GDI Test Suite, Rev 2.1, 07/19/2009
34. Goby Cryptographic Test Suite, Rev: 1.0, 06/05/2007
35. Handle Enforcement Test Suite, Rev: 5, 7/19/2009
36. Hardware Test Suite, Rev: 1, 06/12/2009, X64 Rev: 99, 04/24/2009, IA32 Rev: 99, 04/24/2009, IA64 Rev: 2, 05/01/2006)
37. HID Class Library Test Suite, Rev: 99, 02/17/2006
38. HTTP Client Test Suite, Rev: 3.1, 06/30/2009
39. IIS Coadmin DLL Test Suite, Rev: 1, 06/30/2009
40. Impersonation Test Suite, Rev: 2.2, 07/24/2009
41. Internet Key Exchange Test Suite, Rev 2, 06/13/2009
42. IP Helper Service Test Suite, Rev: 99, 06/12/2009
43. IPSEC Test Suite, Rev 2.3, 08/12/2005
44. ISAPI DLL For Web Printing Test Suite, Rev: 1, 04/27/2009
45. KDC Test Suite, Rev: 1.8, 06/02/2009
46. Kernel Debug Manager Test Suite, Rev: 5, 06/04/2009
47. Kernel Mode Driver Framework Test Suite, Rev: 1, 05/13/2009
48. Kernel Mode WMI Test Suite, Rev: 99, 06/11/2009
49. Kernel Transaction Manager Test Suite, Rev: 99, 04/07/2009
50. LDAP Test Suite, Rev: 2.0, 06/05/2009
51. Local Session Manager Test Suite, Rev: 1.0, 06/30/2009
52. MAPI Test Suite, Rev: 1.4, 06/30/2009
53. Memory Manager Test Suite, Rev: 2, 07/05/2009
54. Miscellaneous Test Suite, Rev: 3.5, 07/05/2009
55. Multiple UNC Provider And DFS Client Test Suite, Rev: 2, 12/18/2007
56. NDIS 5.1 Wrapper Driver Test Suite, Rev: 2, 12/18/2007
57. Network Store Interface Proxy Test Suite, Rev: 6, 04/21/2009
58. Network Support Test Suite, Rev: 4, 07/24/2009
59. Object Manager Test Suite, Rev: 2, 03/19/2009
60. Object Reuse Test Suite, Rev 2.1, 06/30/2009
61. Plug And Play Manager Test Suite, Rev: 4, 01/29/2009
62. Power Manager Test Suite, Rev: 5, 01/29/2009
63. Privilege Test Suite, Rev: 17, 07/19/2009

64. RPC Proxy Test Suite, Rev: 2, 05/30/2006
65. RSOP Service Application Test Suite, Rev: 9, 06/04/2009
66. Server Network Driver Test Suite, Rev 0.8, 06/12/2009
67. SMB 2.0 Server Driver Test Suite, Rev: 1, 06/03/2009
68. SMB Mini-Redirector Test Suite, Rev: 5, 06/12/2009
69. SMB Transport Driver Test SUITE, Rev: 2, 06/03/2009
70. Special Access Test Suite, Rev: 34, 07/24/2009
71. Superfetch Service Host Rev: 2, 05/15/2008
72. Task Scheduler Engine Test Suite, Rev: 9, 05/18/2006
73. Tcpip Driver Test Suite, 06/10/2009
74. TDI translation driver (TDX) test Suite, Rev: 1, 04/02/2009
75. TDI Wrapper Test Suite, Rev: 2, 04/15/2008
76. Token Test Suite, Rev: 1.8, 06/06/2009
77. TPM Base Services Test Suite, Rev: 99, 01/23/2009
78. Trusted Installer Test Suite, Rev: 4, 02/16/20009
79. USB 1.1 & 2.0 Port Driver Test Suite, Rev: 1, 06/11/2009
80. USB Mass Storage Test Suite, Rev: 4, 06/12/2009
81. User Test Suite, Rev 1.4, 07/05/2009
82. User Mode Driver Framework Reflector Test Suite, Rev: 1, 06/26/2009
83. User Profile Service Test Suite, Rev: 4, 07/04/2009
84. VDM Parallel Driver Test Suite, Rev: 99, 06/23/2009
85. Virtual Disk Service Test Suite, Rev: 1, 06/03/2009
86. Virtual Dos Machine Test Suite, Rev: 2, 02/06/2008
87. Volume Manager Driver Test Suite, Rev: 99, 04/02/2009
88. Volume Shadow Copy Driver Test Suite, Rev: 1. 6/11/2009
89. Windows Cryptographic Primitives Library Test Suite, Rev: 1, 06/10/2009
90. Windows Event Log Service Test Suite, Rev: 1, 06/10/2009
91. Windows Firewall Test Suite, Rev 1, 06/30/2009
92. Windows OS Startup Test Suite, Rev: 2, 02/24/2009
93. Windows Time Service Test Suite, Rev: 1, 05/25/2009
94. Windows Update Autoupdate Engine Test Suite, Rev: 1.1, 06/10/2009
95. Windows Update Autoupdate Service Test Suite, Rev: 1, 11/08/2006)
96. WMI Provider Host Test Suite, Rev: 1, 07/01/2009
97. Test Code
98. Actual Test Results

5.7 Vulnerability Assessment

1. Windows Vista and Windows Server 2008 Misuse Analysis Version 0.2, July 6, 2009
2. Microsoft Windows 2008/Vista Strength of Function Analysis (AVA_SOF), Version 0.1, 31 January 2009

6 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Windows Vista and Windows Server 2008, Version 1.0, July 31, 2009.

6.1 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

6.2 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. 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.

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 CCTL developed team tests was limited. A total of twenty four (24) team tests were devised and covered the following areas: Residual Information Protection, TSF Security Functions Management, TOE Security Banners, Session Locking, Identification & Authentication, TOE Access Restriction, and Access Control on Encrypted Files.

6.3 Vulnerability Analysis

Additional testing to address the AVA_VLA.3 requirements was performed by the National Security Agency (NSA) and completed in August 2009. Using the results of the evaluation by the CCTL evaluation team, the NSA evaluation team installed the TOE evaluated configuration and conducted AVA_VLA.3 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.

7 Evaluated Configuration

The evaluated configuration was tested in the configuration identified in this section. 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.

TOE Software Identification – The following Windows Operating Systems (OS'):

- Microsoft Windows Vista Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2008 Standard Edition (64-bit version)
- Microsoft Windows Server 2008 Enterprise Edition (64-bit version)
- Microsoft Windows Server 2008 Datacenter Edition

The following security updates and patches must be applied to the above Vista products:

- All security updates as of 9 June 2009, excluding the Service Pack 2 update.

The following security updates must be applied to the above Windows Server 2008 products:

- All security updates as of 9 June 2009, excluding the Service Pack 2 update.

TOE Hardware Identification – The following hardware platforms are included in the evaluated configuration:

- Dell Optiplex 755, 3.0 GHz Intel Core 2 Duo E8400, 64-bit
- Dell PowerEdge SC1420, 3.6 GHz Intel Xeon Processor (1 CPU), 32-bit
- Dell PowerEdge 1800, 3.2 GHz Intel Xeon Processor (1 CPU), 32-bit
- Dell PowerEdge 2970, 1.7 GHz quad core AMD Opteron 2344 Processor (2 CPUs), 64-bit
- HP Proliant DL385 G5, 2.1 GHz quad core AMD Opteron 2352 Processor (2 CPUs), 64-bit
- HP Proliant DL385, 2.6 GHz AMD Opteron 252 Processor (2 CPUs), 64-bit
- Unisys ES7000 Model 7600R, 2.6 GHz Intel Xeon (6-core) (8 CPUs), 64-bit
- GemPlus GemPC Twin USB smart cards

To use the product in the evaluated configuration, the product must be configured as specified in the Microsoft Windows Common Criteria Evaluation Document, version 6, July 29, 2009.

8 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL4 augmented with ALC_FLR.3 and AVA_VLA.3 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.3 and CEM version 2.3[5], [6]. The evaluation determined the Windows

Vista and Windows Server 2008 TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.3 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL as well as input from the NSA evaluators, and are augmented with the validator's observations thereof.

8.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Windows Vista and Windows Server 2008 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.2 Evaluation of the Configuration Management Capabilities (ACM)

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified

8.3 Evaluation of the Delivery and Operation Documents (ADO)

The SAIC evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.4 Evaluation of the Development (ADV)

The SAIC evaluation team applied each EAL 4 ADV CEM work unit for the functional specification and security policy model portions of the design evaluation. The evaluation team also ensured that the correspondence analysis between the functional specification and the ST was accurate. Lastly, the SAIC evaluation team sampled the source code to ensure that the functional specification was correctly represented based upon the implementation.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

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

The evaluation team applied the coverage and independent testing CEM work units. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team re-ran the entire vendor test suite,, and devised an independent set of team tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.7 Vulnerability Assessment Activity (AVA)

The SAIC evaluation team applied the AVA_MSU.2 and AVA_SOF.1 work units. The evaluation team ensured that the TOE documentation does not easily mislead an administrator and that the password mechanism meets all stated claims in the ST.

The validator reviewed the work of the evaluation team and NSA penetration testing team (AVA_VLA.3), and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

8.8 Summary of Evaluation Results

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

9 Validator Comments/Recommendations

The Evaluation Team is commended for their testing activities of such a complex system, and their efforts to validate the evaluated configuration during team testing.

The validators of this evaluation want to make it clear to those deploying these products in their systems that the analysis and testing for this evaluation was predicated on the notion of a homogeneous network. This means the analysis and security functional testing did not

address the possibility of an untrusted user from injecting a raw frame on the network, since users of the windows machines are prohibited from doing this.

.

10 Annexes

Not applicable.

11 Security Target

The Security Target is identified as Microsoft Windows Vista and Windows Server 2008 Security Target, Version 1.0, July 24, 2009.

12 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

13 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.3, August 2005.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.3, August 2005.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.3, August 2005.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security*, Version 2.3, August 2005.

[5] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 2.3, August 1999.

[6] 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.

[7] Science Applications International Corporation. *Evaluation Technical Report for the Windows Vista and Windows Server 2008 Part 2 (Proprietary)*, Version 2.0, July 31, 2009.

[8] Science Applications International Corporation. *Evaluation Team Test Report for Windows Vista and Windows Server 2008 Part 2 Supplement (SAIC and Microsoft Proprietary)*, Version 1.0, July 31, 2009.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] *Windows Vista and Windows Server 2008* Security Target, Version 1.0, July 24, 2009.

14 Design Documentation Listing

General Product Documentation	Version	Date
Security Policy Model.doc	12	2/12/2009
Functional Specification Completeness Rationale.doc	2	5/28/2009
Certificate Server Component		
(OS) Certificate Service Default Exit Module.doc	2	7/22/2009
(OS) Certificate Service Default Policy Module.doc	2	7/22/2009
(OS) Certificate Service.doc	4	7/22/2009
Cryptographic Support		
FVE Crash Dump Driver	0.03	7/22/2009
FVE Driver	0.06	7/28/2009
TPM Based Services	0.07	7/28/2009
TPM Driver	0.03	7/28/2009
Executive Component		
64 bit Kernel Debug Support.doc	9	7/22/2009
Application Compatibility Support.doc	12	7/22/2009
Cache Manager.doc	6	7/22/2009
Configuration Manager.doc	3	7/22/2009
Event Tracing for Windows.xlsm	0.08	7/22/2009
Executive Object Services.doc	3	7/22/2009
Graphics Device Interface.xlsm	0.07	7/28/2009
Hardware Abstraction Layer.doc	6	7/23/2009

Kernel Debug Manager.doc	2	7/22/2009
Kernel Mode Windows Management Instrumentation.doc	13	7/22/2009
Kernel Runtime.doc	15	7/22/2009
Kernel Runtime New Checks and Effects.xlsm	0.03	7/10/2009
Kernel Tranasction Manager.xlsm	0.09	7/22/2009
Local Process Communication.doc	9	7/22/2009
Memory Manager.doc	8	7/22/2009
Memory Manager.xlsm	0.04	7/20/2009
Microkernel.doc	15	7/22/2009
Microkernel New Checks and Effects.xlsm	0.02	7/22/2009
Object Manager.doc	3	7/22/2009
Plug and Play Manager.doc	7	7/22/2009
Plug and Play Manager New Checks and Effects.xlsm	0.07	7/22/2009
Power Manager.doc	12	7/22/2009
Process Manager.doc	2	7/22/2009
Process Manager New Checks and Effects.xlsm	0.08	7/22/2009
Security Reference Monitor.doc	16	7/22/2009
Virtual DOS Machine.doc	2	7/22/2009
Window Manager (User).xlsm	0.08	7/22/2009
Hardware Component		
AMD Hardware.doc	13	5/31/2009
Intel Hardware.doc	12	5/31/2009
Internet Information Services Component		
BITS Server Extensions ISAPI.doc	6	7/23/2009
IIS CoAdmin DLL.doc	4	7/23/2009
IIS ISAPI Handler.doc	2	7/23/2009
IIS Metadata DLL.doc	3	7/23/2009
Internet Information Services Reset Control.doc	2	7/23/2009
IIS RPC Proxy.doc	5	7/23/2009
IIS Web Admin Service.doc	6	7/23/2009
IIS Web Admin Service.xlsm	0.04	7/23/2009
IIS Web Server Core.doc	6	7/23/2009
IIS Worker Process.doc	2	7/23/2009
Internet Information Services.doc	2	7/23/2009
ISAPI DLL for Web Printing.doc	4	7/23/2009
Metadata and Admin Service.doc	2	7/23/2009
WAM Registration DLL.doc	3	7/23/2009
WinHTTP Web Proxy Auto Discovery Service.doc	2	7/23/2009
I/O Core Component		
File System Recognizer.doc	3	6/2/2009
IO Manager.doc	3	7/23/2009
IO Manager.xlsm	0.06	7/23/2009
Kernel Mode Driver Framework.xlsm	0.06	7/23/2009
Kernel Security Device Driver.doc	3	7/23/2009

Mount Manager.doc	3	7/23/2009
User Mode Driver Framework Reflector.xlsm	0.07	7/23/2009
I/O Devices Component		
ACPI Driver.doc	7	7/23/2009
Advanced Host Controller Interface Driver.xlsmdoc	0.5	7/23/2009
ALI IDE Miniport Driver	0.3	7/23/2009
AMD IDE Miniport Driver	0.3	7/23/2009
AMD K8 Processor Driver.xlsm	0.2	7/23/2009
ATAport Driver Extension.xlsm	0.6	7/23/2009
ATI ATI2MTAD Miniport Driver.doc	7	7/23/2009
AudioPortClassDriver.doc	3	7/23/2009
Beep Driver.doc	4	7/23/2009
Broadcom BCM5708C NetXtreme Gigabit NIC Miniport Driver.doc	3	7/23/2009
Composite Battery Driver.xlsm	0.4	7/23/2009
File System Filter Manager.doc	5	7/23/2009
Hardware Error Device Driver.xlsm	0.3	7/23/2009
HID Class Library.doc	5	7/23/2009
HID Keyboard Filter Driver.doc	4	7/23/2009
HID Mouse Filter Driver.doc	4	7/23/2009
HID Parsing Library.doc	4	7/23/2009
HP Proliant Smart Array.doc	4	7/23/2009
i8042 Port Driver.doc	3	7/23/2009
IDE ATAPI Port Driver.doc	2	7/23/2009
Intel Pro 1000 e1e6032e NIC Miniport Driver.doc	7	7/23/2009
Intel Pro 1000 e1g6032e NIC Miniport Driver.doc	3	7/23/2009
Intelligent IO Miniport Driver.doc	3	7/23/2009
Intelligent IO Utility Filter Driver.doc	3	7/23/2009
Intelligent Platform Management Interface Driver.xlsm	0.6	7/23/2009
ISA and EISA Class Driver.xlsm	0.4	7/23/2009
Keyboard Class Driver.doc	3	7/23/2009
LSI Serial Attached SCSI Driver.doc	3	7/23/2009
Microsoft System Management BIOS Driver.xlsm	0.2	7/23/2009
Monitor Class Function Driver.xlsm	0.4	7/23/2009
Mouse Class Driver.doc	3	7/23/2009
NULL Driver.doc	3	7/23/2009
Parallel Port Driver.doc	3	7/23/2009
Partition Manager.doc	4	7/23/2009
Plug and Play PCI Enumerator.doc	3	7/23/2009
Plug and Play Software Device Enumerator.doc	17	6/3/2009
PnP Disk Driver.doc	3	7/23/2009
PNP ISA Bus Driver.doc	3	7/23/2009
Processor Device Driver.doc	3	7/23/2009
SCSI CD-ROM Driver.doc	4	7/23/2009
SCSI Class System DLL.doc	4	7/23/2009

SCSI Port Driver.doc	17	7/23/2009
SCSI Tape Class Driver.doc	11	7/23/2009
Serial Device Driver.doc	3	7/23/2009
Serial Port Enumerator.doc	3	7/23/2009
Smart Card Driver Library.doc	3	7/23/2009
Storage Port Driver.doc	18	7/23/2009
USB1.1&2.0 Port Driver.doc	3	7/23/2009
USB CCID Driver.doc	3	7/23/2009
USB Common Class Generic Parent Driver.doc	3	7/23/2009
USB Host Controller Interface Miniport Drivers.doc	3	7/23/2009
USB Mass Storage Driver.doc	3	7/23/2009
USB Miniport Driver for Input Devices.doc	3	7/23/2009
USB Root Hub Driver.doc	3	7/23/2009
User Mode Bus Enumerator.xlsm	0.3	7/23/2009
VDM Parallel Driver	0.5	7/23/2009
VGA Super VGA Video Driver.doc	3	7/23/2009
VIA IDE Miniport Driver	0.3	7/23/2009
Video Port Driver.doc	3	7/23/2009
Volume Shadow Copy Driver.doc	4	7/23/2009
Watchdog Driver.doc	3	7/23/2009
WMI for ACPI Driver.doc	3	7/23/2009
I/O File Component		
CDROM File System.doc	5	7/24/2009
Encrypting File System.doc	2	7/24/2009
Fast Fat File System.doc	3	7/24/2009
File Information FS Mini-Filter.xlsm	0.06	7/24/2009
Mailslot Driver.doc	22	7/24/2009
NPFS Driver.doc	26	7/24/2009
NT File System Driver.doc	6	7/24/2009
UDF File System Driver.doc	2	7/24/2009
Volume Manager Driver.xlsm	0.09	7/24/2009
I/O Network Component		
Ancillary Function Driver for WinSock.doc	4	7/24/2009
Bowser Driver.doc	3	7/24/2009
Client Side Chaching Driver.xlsm	0.07	7/24/2009
Distributed File Client.xlsm	0.07	7/24/2009
Distributed File System Filter Driver.doc	5	7/24/2009
FWPkClnt Export Driver.xlsm	0.03	7/24/2009
HTTP Driver.doc	7	7/24/2009
IP Filter Driver.doc	4	7/24/2009
IP in IP Encapsulation Driver.doc	2	7/24/2009
Loopback Network Driver.doc	3	7/24/2009
Multiple UNC Provider and DFS Client.doc	4	7/24/2009
NDIS 5.1 Wrapper Driver.doc	5	7/24/2009
NDIS User Mode IO Driver.xlsm	0.04	7/24/2009
NetBT Transport Driver.doc	8	7/24/2009

Network Store Interface Proxy Driver.xlsm	0.07	7/24/2009
Qos Packet Scheduler.xlsm	0.04	7/24/2009
RDBSS.doc	23	7/24/2009
Remote NDIS Miniport.doc	3	7/24/2009
Server Driver.doc	4	7/24/2009
Server Network Driver.xlsm	0.05	7/24/2009
SMB Mini-Redirector.doc	3	7/24/2009
SMB 2.0 Sub-Redirector.xlsm	0.03	7/24/2009
SMB 2.0 Server Driver.xlsm	0.05	7/24/2009
SMB Transport Driver.doc	9	7/24/2009
TCPIP Protocol Driver.xlsm	0.06	7/24/2009
TDI Translation Driver (TDX).xlsm	0.05	7/24/2009
TDI Wrapper.doc	4	7/24/2009
WebDav Mini Redirector.doc	4	7/24/2009
Winsock2 IFS Layer Driver.doc	3	7/24/2009
Network Support Component		
COM+ Configuration Catalog Server.doc	15	7/24/2009
COM+ Event System Service.doc	7	7/24/2009
COM+ Services.doc	7	7/24/2009
DHCP Service.doc	8	7/24/2009
Distributed COM Services.doc	5	7/24/2009
Domain Name Service.doc	6	7/24/2009
Internet Extensions for Win32.doc	3	7/24/2009
Internet Key Exhange.xlsm	0.07	7/24/2009
IP Helper Service.xlsm	0.05	6/30/2009
Network Connections Manager.doc	7	6/24/2009
Network Location Awareness Service.doc	9	7/24/2009
RPC Endpoint Mapper.doc	7	7/24/2009
RPC Locator.doc	3	7/24/2009
Simple TCPIP Services Service DLL.doc	3	7/24/2009
TCPIP NetBIOS Transport Service.doc	3	7/24/2009
TCPIP Services Application.doc	3	7/24/2009
Web DAV Service DLL.doc	19	7/24/2009
OS Support Component		
BITS Service	12	7/24/2009
Distributed File System Service.doc	6	7/24/2009
Print Spooler.doc	7	7/24/2009
Removable Storage Manager.doc	5	7/24/2009
Session Manager.doc	2	7/24/2009
WMI Adapter Service.xlsm	0.04	7/24/2009
WMI Provider Host.doc	7	7/24/2009
WMI Service.doc	26	7/24/2009
Security Component		
Active Directory Replication Management.doc	5	7/24/2009
Core Directory Service.doc	3	7/24/2009
Credential Manager.doc	6	7/24/2009

Data Protection API.doc	5	7/24/2009
Directory Services Role Management.doc	5	7/24/2009
Encrypting File System Service.doc	8	7/24/2009
IFXCardM.xlsm	0.02	7/24/2009
Inter-Site Messaging.doc	4	7/24/2009
IPSecSPDServer.doc	39	6/24/2009
KDC Service.doc	4	7/24/2009
Kerberos Security Package.doc	3	7/24/2009
Key Isolation Service.xlsm	0.06	7/24/2009
LDAP.doc	4	7/24/2009
LSA Audit.doc	3	7/24/2009
LSA Authentication.doc	4	7/24/2009
LSA Policy.doc	5	7/24/2009
MAPI Based Directory Request.doc	4	7/24/2009
Microsoft Authentication Package v1.0.doc	4	7/24/2009
Microsoft Base Smart Card Crypto Provider.doc	2	7/24/2009
Microsoft Digest Access.doc	9	7/24/2009
Microsoft Smart Card Key Storage Provider.xlsm	0.03	7/24/2009
Net Logon Services DLL.doc	6	7/24/2009
NTDS Backup and Restore.doc	4	7/24/2009
PKI Trust Installation and Setup.doc	3	7/24/2009
Protected Storage Server.doc	3	7/24/2009
SAM Server.doc	7	7/24/2009
Secondary Logon Service.doc	4	7/24/2009
TLS-SSL Security Provider.doc	3	7/24/2009
Trust Signing APIs.doc	3	7/24/2009
Windows Cryptographic Primitives Library.xlsm	0.04	7/24/2009
Services Component		
Application Experience Lookup Service.doc	6	7/24/2009
Application Information Service.xlsm	0.04	7/24/2009
Computer Browser Service.doc	3	7/24/2009
Cryptographic Services.doc	6	7/24/2009
Desktop Window Manager.xlsm	0.06	7/24/2009
File Replication Service.doc	6	7/24/2009
Generic Host Process for Win32 Services.doc	2	7/24/2009
Interactive Service Detection for Session 0.xlsm	0.03	7/24/2009
Non-COM WMI Event Provision APIs.doc	5	7/24/2009
Remote Registry Service.doc	4	7/24/2009
Server Service DLL.doc	4	7/24/2009
Services and Controller App.doc	7	7/24/2009
Smart Card Resource Management Server.doc	5	7/24/2009
Superfetch.doc	5	7/24/2009
System Event Notification Service.doc	2	7/24/2009
Task Engine.xlsm	0.03	7/24/2009
UPnP Device Host.doc	2	7/24/2009
User-Mode Plug-and-Play Service.doc	28	7/24/2009

User Profile Service.xlsm	0.06	7/24/2009
Virtual Disk Service.doc	6	7/24/2009
Volume Shadow Copy Service.doc	3	7/24/2009
Windows Event Log Service.xlsm	0.06	7/24/2009
Windows Installer Service.doc	4	7/24/2009
Windows Security Center Service.doc	5	7/24/2009
Windows Security Configuration Editor Engine.doc	3	7/24/2009
Windows Shell Services DLL.doc	5	7/24/2009
Windows Time Service.doc	5	7/24/2009
Windows Update Client	4	7/24/2009
Workstation Service.doc	4	7/24/2009
Win32 Component		
Base Server.doc	2	7/24/2009
Client Server Runtime Process.doc	2	7/24/2009
Windows Server DLL.doc	4	7/24/2009
Windows Firewall Component		
Application Layer Gateway Service.doc	3	7/24/2009
Base Filtering Engine Service.xlsm	0.09	7/24/2009
Home Networking Configuration Manager.doc	3	7/24/2009
IP Network Address Translator.doc	3	7/24/2009
MAC Bridge Driver.doc	3	7/24/2009
NAT Helper.doc	3	7/24/2009
WinLogon Component		
Auto Enrollment.doc	12	7/24/2009
Group Policy Object Processing.doc	4	7/24/2009
Group Policy.doc	4	7/24/2009
Local Session Manager.xlsm	0.07	7/24/2009
Syskey.doc	3	7/24/2009
Trust Verification APIs.doc	3	7/24/2009
Trusted Installer.xlsm	0.05	7/24/2009
UserEnvironment.doc	4	7/24/2009
Windows File Protection.doc	3	7/24/2009
Windows Logon Application.doc	4	7/24/2009
Windows Loader.xlsm	0.03	7/24/2009
WinInit.xlsm	0.05	7/24/2009
Windows Smartcard Credential Provider.xlsm	0.04	7/24/2009
Admin Tools		
at exe.doc	0.4	7/24/2009
auditpol.doc	0.3	7/24/2009
Auth_Mgr_GUI.doc	1.3	7/24/2009
Backup_and_Restore.doc	0.2	7/24/2009
BitLocker	0.4	7/24/2009
Certification Authority GUI.doc	0.8	7/24/2009
cipher.exe.doc	0.2	7/24/2009
COM+ Applications.doc	0.5	7/24/2009
Computer Management.doc	0.2	7/24/2009

Data Execution Prevention for Sysdm	2	7/24/2009
Data Execution Prevention for WMIC	0.2	7/24/2009
Date_and_Time.doc	0.3	7/24/2009
DCOM Config.doc	0.2	7/24/2009
Default_Group_Policy_Object_Restore_Utility.doc	0.2	7/24/2009
Device Manager.doc	0.2	7/24/2009
DHCP Snap-in.doc	0.2	7/24/2009
Disk Management.doc	0.2	7/24/2009
Disk Quota GUI.doc	0.3	7/24/2009
DNS Snap-in.doc	0.2	7/24/2009
Domains and Trusts.doc	2	7/24/2009
Driver_Verifier_Manager.doc	0.2	7/24/2009
efsadu.doc	0.3	7/24/2009
Event Viewer.doc	0.2	7/24/2009
Explorer.doc	0.2	7/24/2009
Group Policy Refresh.doc	0.2	7/24/2009
Group Policy.doc	0.8	7/24/2009
IIS_Manager_GUI.doc	0.2	7/24/2009
Initial Configuration Tasks and Server Manager	0.2	7/24/2009
IPSec Settings GUI Spec.doc	2	7/24/2009
IPv6 Monitor DLL.doc	0.2	7/24/2009
Network.doc	0.2	7/24/2009
Network Connections Manager	8	7/24/2009
NetworkID.doc	0.2	7/24/2009
OU Delegation.doc	0.2	7/24/2009
Printers GUI.doc	0.4	7/24/2009
Registry_Editor.doc	0.2	7/24/2009
RSoP.doc	0.2	7/24/2009
SAM Lock Tool.doc	0.2	7/24/2009
Scheduled Tasks CLI Tool.doc	0.2	7/24/2009
SCWcmd.exe.doc	0.2	7/24/2009
Security Config Editor.doc	0.2	7/24/2009
Security Policy GUI.doc	1.9	7/24/2009
Security Policy UI	0.2	7/24/2009
Security_Config_Wiz.doc	0.2	7/24/2009
Services.doc	0.2	7/24/2009
Session_Locking.doc	0.2	7/24/2009
SFC.doc	2	7/24/2009
Share_a_Folder_Wizard.doc	0.2	7/24/2009
Sigverif Design Spec.doc	0.2	7/24/2009
Sites and Services.doc	0.7	7/24/2009
Task Scheduler.doc	0.2	7/24/2009
User Account Control	0.2	7/24/2009
Users and Groups.doc	0.2	7/24/2009
Virtual Disk Service	0.2	7/24/2009
Volume Shadow Copy Service Command Line.doc	0.2	7/24/2009

Windows Mngt Infra (WMI).doc	0.2	7/24/2009
Windows_Firewall_GUI.doc	3	7/24/2009