National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

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

Windows 7 and Windows Server 2008 R2

Report Number:	**CCEVS-VR-10390-2010**
Dated:	**24 March 2011**
Version:	**0.2**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Kenneth Elliott
Aerospace Corporation
Columbia, MD

Shaun Gilmore
National Security Agency
Ft. Meade, MD

Ralph Broom
MITRE Corporation
McLean, VA

Common Criteria Testing Laboratory

Tony Apted
Tammy Compton
Terrie Diaz
Chris Keenan
Eve Pierre
Michelle Rupple
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 4
3.1 Hardware Capabilities 5
3.2 Software Capabilities 5
3.3 TOE Logical Boundary 7
3.3.1 Security Audit 7
3.3.2 User Data Protection 8
3.3.3 Identification and Authentication 8
3.3.4 Security Management 8
3.3.5 Cryptographic Protection 8
3.3.6 Protection of TOE Security Functions 9
3.3.7 Resource Utilization 9
3.3.8 Session Locking 9
4 Assumptions 9
5 Documentation 10
5.1 Design Documentation 10
5.2 Guidance Documentation 17
5.3 Life Cycle 17
5.4 Testing 17
6 IT Product Testing 25
6.1 Developer Testing 25
6.2 Evaluation Team Independent Testing 25
7 Evaluated Configuration 26
8 Results of the Evaluation 27
8.1 Evaluation of the Security Target (ASE) 27
8.2 Evaluation of the Development (ADV) 27
8.3 Evaluation of the Guidance Documents (AGD) 28
8.4 Evaluation of the Life Cycle Support Activities (ALC) 28
8.5 Evaluation of the Test Documentation and the Test Activity (ATE) 28
8.6 Vulnerability Assessment Activity (AVA) 29
8.7 Summary of Evaluation Results 29
9 Validator Comments/Recommendations 29
10 Annexes 30
11 Security Target 30
12 Glossary 31
13 Bibliography 31

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Microsoft Windows 7 and Windows Server 2008 R2. 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 and was completed in March 2011. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, written by SAIC. 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.

The Target of Evaluation (TOE) is Windows 7 and Windows Server 2008 R2, configured and operated according to the guidance documents identified later in this report. The Windows 7 and Windows Server 2008 R2 TOE is a general-purpose, distributed, network OS that provides controlled access between subjects and user data objects. Windows 7 and Windows Server 2008 R2 TOE has a broad set of security capabilities including single network logon (using password or smart card); access control and data encryption; extensive security audit collection; host-based firewall and IPSec to control information flow, public key certificate service, built-in standard-based security protocols such as Kerberos , Transport Layer Security (TLS)/Secure Sockets Layer (SSL), Digest, Internet Key Exchange (IKE)/IPSec, FIPS-140 validated cryptography, web service, and Light-weight Directory Access Protocol (LDAP) Directory-based resource management. The Windows 7 and Windows Server 2008 R2 TOE provides the following security services: user data protection (WEBUSER access control, web content provider access control, discretionary access control (DAC), IPSec information flow control, connection firewall information flow control), cryptographic support, audit, Identification and Authentication (I&A) (including trusted path/channel), security management, protection of the TOE Security Functions (TSF), resource quotas, and TOE access/session control. The Windows 7 and Windows Server 2008 R2 TOE security policies provide network-wide controlled access protection (access control for user data, WEBUSER and web content provider, IPSec information flow, connection firewall information flow), encrypted data/key protection, and encrypted file protection. These policies enforce access limitations between individual users and data objects, and on in-coming and out-going traffic channels through a physically separate part of the TOE. The TOE is capable of auditing security relevant events that occur within a Windows 7 and Windows Server 2008 R2 network. All these security controls require users to identify themselves and be authenticated prior to using any node on the network.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for

IT Security Evaluation (Version 3.1 R3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1 R3). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence 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, 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 7 and Windows Server 2008 R2 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 Software	Microsoft Windows 7 Enterprise Edition (32-bit and 64-bit versions) Microsoft Windows 7 Ultimate Edition (32-bit and 64-bit versions) Microsoft Windows Server 2008 R2 Standard Edition Microsoft Windows Server 2008 R2 Enterprise Edition Microsoft Windows Server 2008 R2 Datacenter Edition Microsoft Windows Server 2008 R2 Itanium Edition
TOE Hardware	Dell Optiplex 755, 3.0 GHz Intel Core 2 Duo E8400, 64-bit Dell PowerEdge SC1420, 3.6 GHz Intel Xeon Processor (1 CPU), 3264-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 HP Integrity rx1620, 1.3 Ghz Intel Itanium Processor (1 CPU), 64-bit (Itanium) Microsoft Hyper-V Microelectronics Trusted Platform Module [SMO1200] GemPlus GemPC Twin USB smart card reader
Protection Profile	US Government Protection Profile for General-Purpose Operating Systems in a Networked environment (GPOSPP), version 1.0, 30 August 2010
ST:	Microsoft Windows 7 and Windows Server 2008 R2 Security Target, Version 1.0, March 23rd, 2011.
Evaluation Technical Report	Evaluation Technical Report For Windows 7 and Windows Server 2008 R2 (Proprietary), Version 1.0, December 3, 2010
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 R3
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Microsoft Corporation
Developer	Microsoft Corporation
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD

Item	Identifier
CCEVS Validators	Kenneth Elliott, Aerospace Corporation, Columbia, MD Shaun Gilmore, National Security Agency, Ft. Meade, MD Ralph Broom, MITRE Corporation, McLean, VA

3 Architectural Information

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

Windows 7 and Windows Server 2008 R2 are operating systems that supports both workstation and server installations. The TOE includes six product variants of Windows 7 and Windows Server 2008 R2:

- Windows 7 Enterprise
- Windows 7 Ultimate
- Windows Server 2008 R2 Standard
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Datacenter
- Windows Server 2008 R2 Itanium

Windows 7 is suited for business desktops and notebook computers; it is the workstation product and while it can be used by itself it is designed to serve as a client within Windows domains. Designed for departmental and standard workloads, Windows Server 2008 R2 Standard delivers intelligent file and printer sharing; secure connectivity based on Internet technologies, and centralized desktop policy management. Windows Server 2008 R2 Enterprise differs from Windows Server 2008 R2 Standard primarily in its support for high-performance server hardware for greater load handling. These capabilities provide reliability that helps ensure systems remain available. Windows Server 2008 R2 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. Windows Server 2008 R2 Itanium provides support for the alternate Intel Itanium CPU, but otherwise can serve where Standard or Enterprise edition products might be used.

In terms of security, Windows 7 and Server 2008 R2 share the same security characteristics. The primary difference is that the Server 2008 Server R2 products include services and capabilities that are not part of Windows 7 (for example the DNS Server, DHCP Server) or are not installed by default on Server 2008 R2 (for example the Windows Media Player, Windows Aero and desktop themes). The additional services have a bearing on the security properties of the distributed operating system (e.g., by extending the set of available interfaces and proffered services) and as such are included within the scope of the evaluation.

3.1 Hardware Capabilities

One differentiator between Windows Server editions is support for additional scalability and hardware capabilities. The following table states which hardware capabilities are supported by each edition of Windows Server 2008 R2.

Table 2: Hardware Capabilities for Windows Server 2008 R2

	Windows Server 2008 R2 Edition			
Capability	**Standard**	**Enterprise**	**Datacenter**	**Itanium**
Maximum Memory (RAM)	32 GB	2 TB	2 TB	2 TB
Maximum # of Processors	4 x 64	8 x64	64 x64	64 IA 64
Clustering	No	16-node	16-node	8-node
Hot Add/Replace Memory and Processors[1]	No	Yes	Yes	Yes
Fault-tolerant Memory Synchronization	No	Yes	Yes	Yes

3.2 Software Capabilities

Starting with Windows Server 2008, the server operating system was split into multiple server roles, with each server role providing different services and capabilities. This componentization simplifies administration and also reduces the attack surface of Windows Server by enabling the administrator to install only the specific binaries needed onto a machine to fulfill its role.

The following table indicates which roles are included in each edition of Windows Server:

Table 3: Server Roles in Windows Server 2008 R2

	Windows Server 2008 R2 Edition			
Server Role	**Standard**	**Enterprise**	**Datacenter**	**Itanium**
Active Directory Certificate Services	Yes[2]	Yes	Yes	
Active Directory Domain Services	Yes	Yes	Yes	
Active Directory Federation Services		Yes	Yes	
Active Directory Lightweight Directory Services	Yes	Yes	Yes	
Active Directory Rights Management Services	Yes	Yes	Yes	
Application Server	Yes	Yes	Yes	Yes
DHCP Server	Yes	Yes	Yes	
DNS Server	Yes	Yes	Yes	
Fax Server	Yes	Yes	Yes	

[1] Requires supporting hardware.

[2] Limited to creating non-Enterprise Certificate Authorities. Also, does not support role separation.

File Services	Yes[3]	Yes	Yes	
Hyper-V[4]	Yes	Yes	Yes	
Network Policy and Access Services	Yes[5]	Yes	Yes	
Print and Document Services	Yes	Yes	Yes	
Remote Desktop Services	Yes[6]	Yes	Yes	
Web Services (IIS 7.5)	Yes	Yes	Yes	Yes
Windows Deployment Services	Yes	Yes	Yes	
Windows Server Update Services (WSUS)	Yes	Yes	Yes	

Additionally all editions of Windows server include the Server Manager application which administrators use to add/remove roles and features from Windows Server as well as the Server Core, which a minimal server installation option for computers running on the Windows Server 2008 R2 operating system. Server Core provides a low-maintenance server environment with reduced attack surface by presenting a command-line interface to the administrator instead of the GUI-based Explorer interface.

The security features addressed by this security target are those provided by Windows 7 and Windows Server 2008 R2 as operating systems. Microsoft provides several Window 7 and Windows Server 2008 R2 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 (SMTP), Remote Desktop, Rights Management Service, Windows SharePoint Service, Microsoft Message Queuing, and ReadyBoost. These services are particularly complex or not recommended and in some cases essentially represent products in their own right. They have been excluded because they are not enabled or installed by default and are not necessary for the operation of the core security services. Also they have significant impact on the claims made in this Security Target and the ability of the TOE to conform to the intended Protection Profile.

While the Windows CC evaluation includes the IIS web server, the evaluated configuration does not allow for arbitrary server-side execution of web content (via the configuration guidance) since user subject binding would be uncertain. Similarly, the Network Access Protection (NAP) features related to 802.1X and NAP-NAC (see below) are excluded from the evaluated configuration since wireless technology and Cisco products are not included in the scope of the Microsoft Windows CC evaluation.

[3] Limited to 1 standalone DFS root.

[4] Server 2008 Hyper-V was part of a separate Common Criteria evaluation.

[5] Limited to 250 Routing and Remote Access (RRAS) connections, 50 (Internet Authentication Service) IAS connections and 2 IAS Server Groups.

[6] Limited to 250 Remote Desktop Services connections.

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

	Windows 7 Enterprise	Windows 7 Ultimate	Windows Server 2008 R2 Standard	Windows Server 2008 R2 Enterprise	Windows Server 2008 R2 Datacenter	Windows Server 2008 R2 Itanium
32-bit/64-bit	32 & 64	32 & 64	64	64	64	64
Single Core/Processor	X	X	X	X	X	X
Multiple Core/Processor	X	X	X	X	X	X
Domain Member	X	X	X	X	X	X
Domain Controller	N/A	N/A	X	X	X	N/A

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 7 and Windows Server 2008 R2 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, and other event specific data. Authorized administrators can review audit logs including the ability to search and sort audit records. Authorized Administrators can also configure the audit system to include or exclude potentially auditable events to be audited based on a wide range of characteristics.

3.3.2 User Data Protection

Windows 7 and Windows Server 2008 R2 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, Connection Firewall); and, object and subject residual information protection. Windows 7 and Windows Server 2008 R2 use access control methods to allow or deny access to objects, such as files, directory entries, printers, and web content. Windows 7 and Windows Server 2008 R2 use 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 (which are sets of information identifying users and their specific access to resource objects), web permissions, IP filters, and port mapping rules. Windows 7 and Windows Server 2008 R2 also protect user data by ensuring that resources exported to user-mode processes do not have any residual information.

3.3.3 Identification and Authentication

Windows 7 and Windows Server 2008 R2 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 7 and Windows Server 2008 R2 maintain databases of accounts including their identities, authentication information, group associations, and privilege and logon rights associations. Windows 7 and Windows Server 2008 R2 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 7 and Windows Server 2008 R2 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 7 and Windows Server 2008 R2 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 cryptographic algorithms. The TOE also provides extensive auditing support in support of cryptographic requirements, support for replaceable random number generators, and a key isolation service designed to limit the potential exposure of secret and private keys. In addition to supporting its own security functions with cryptographic support, the TOE offers access to the cryptographic support functions for user application programs.

3.3.6 Protection of TOE Security Functions

Windows 7 and Windows Server 2008 R2 provide a number of features to ensure the protection of TOE security functions. Windows 7 and Windows Server 2008 R2 protects against unauthorized data disclosure and modification by using a suite of Internet standard protocols including IPSec and ISAKMP. Windows 7 and Windows Server 2008 R2 ensure process isolation security for all processes through private virtual address spaces, execution context and security context. The Windows 7 and Windows Server 2008 R2 data structures defining process address space, execution context, memory protection, and security context are stored in protected kernel-mode memory. The Windows 7 and Windows Server 2008 R2 BitLocker features can be used to protect fixed and removable USB storage volumes. The Windows 7 and Windows Server 2008 R2 Network Access Protection feature can be used to limit access to network resources depending on the measured “health” of clients based on attributes such as security settings and installed applications. Windows 7 and Windows Server 2008 R2 also include some self-testing features that ensure the integrity of executable TSF images and its cryptographic functions.

3.3.7 Resource Utilization

Windows 7 and Windows Server 2008 R2 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 7 and Windows Server 2008 R2 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 7 and Windows Server 2008 R2 allow an authorized administrator to configure the system to display a logon banner before the logon dialogue.

4 Assumptions

The following assumption was made during the evaluation of Windows 7 and Windows Server 2008 R2:

- It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

5 Documentation

The following documentation was used as evidence for the evaluation of the Windows 7 and Windows Server 2008 R2:

5.1 Design Documentation

1. Microsoft Windows Common Criteria Evaluation Security Architecture, September 13, 2010
2. **Admin Tools**
3. Certreq.exe Command-Line Utility (August 13 2010).docx
4. Certutil.exe Command-Line Utility (August 13 2010).docx
5. Active Directory Delegation of Control Wizard (June 24 2010).docx
6. Active Directory Domains and Trusts Snap-in (June 26 2010).docx
7. Active Directory Sites and Services (June 28 2010).docx
8. Audit Policy Command Line Interface (Mar 30 2010).docx
9. Authorization Manager (June 3 2010).docx
10. BitLocker Drive Encryption Control Panel (May 6 2010).docx
11. Certificates Snap-in (Mar 30 2010).docx
12. Component Services Snap-in (June 10 2010).docx
13. Computer Management Snap-in (April 9 2010).docx
14. Control Panel (June 6 2010).docx
15. Create A Shared Folder Wizard (April 06 2010).docx
16. Date and Time Control Panel (Mar 9 2010).docx
17. Default Group Policy Object Restore Command Line Utility (Mar 18 2010).docx
18. Device and Printers Control Panel (May 13 2010).docx
19. Device Manager Snap-in (April 27 2010).docx
20. DHCP Snap-in (June 9 2010).docx
21. Disk Management Snap-In (May 4 2010).docx
22. DNS Snap-in (June 8 2010).docx
23. Driver Verifier Manager (May 3 2010).docx
24. Encrypting File System Dialog Boxes (Mar 25 2010).docx
25. Event Viewer Snap-in (July 12 2010).docx
26. Explorer (September 10 2010).docx
27. Explorer Quota Property Tab (April 30 2010).docx
28. File Encryption Command Line Utility (April 22 2010).docx
29. Group Policy Editor Snap-in (June 14 2010).docx
30. Group Policy Update Command Line Utility (April 16 2010).docx
31. Hyper-V Manager (August 11 2010).docx
32. Internet Information Service (IIS) Manager (September 14 2010).docx
33. IP Security Monitor Snap-in (May 29 2010).docx
34. IP Security Policies Snap-in (May 24 2010).docx
35. NAP Client Configuration Snap-in (June 7 2010).docx
36. Network and Sharing Control Panel (May 13 2010).docx
37. Performance Monitoring Snap-in
38. Registry Editor (April 16 2010).docx
39. Resultant Set of Policy Snap-in (May 17 2010).docx
40. Routing and Remote Access Snap-in (July 13 2010).docx
41. SAM Lock Tool (May 7 2010).docx
42. Schedule Service Command Line Utility (July 8 2010).docx
43. Scheduled Tasks Command-Line Utility (April 16 2010).docx
44. Security Configuration Wizard (July 27 2010).docx

45. Security Configuration Wizard Command Line Utility (April 26 2010).docx
46. Security Policy Snap-in (September 14 2010).docx
47. Security Templates Snap-in (May 13 2010).docx
48. Security Configuration and Analysis Snap-in (Aug 31 2010).docx
49. Server Manager (April 19 2010).docx
50. Services Snap-in (May 19 2010).docx
51. Signature Verification Command Line Utility (May 7 2010).docx
52. System Control Panel, Computer Name Tab (May 20 2010).docx
53. System Integrity Check and Repair Command Line Utility (June 28 2010).docx
54. Task Scheduler Snap-in (July 2 2010).docx
55. TPM Management (July 6 2010).docx
56. User Account Control Settings (April 23 2010).docx
57. Users and Groups Snap-in (June 28 2010).docx
58. Volume Shadow Copy Service Command Line Utility (May 10 2010).docx
59. Windows Authentication User Interface (September 10 2010).docx
60. Windows Firewall with Advanced Local Security Snap-in (June 21 2010).docx
61. WMI Control Snap-in (June 1 2010).docx
62. **Certificate Services**
63. (OS) Certificate Service (Oct 11 2010).docx
64. OS) Certificate Service Default Exit Module (May 26 2010).docx
65. OS) Certificate Service Default Policy Module (June 1 2010).docx
66. Online Responder Service (June 30 2010).docx
67. **Cryptographic Support**
68. BitLocker Drive Encryption Service (Dec 02 2009).docx
69. FVE Crash Dump Driver (Jan 22 2010).docx
70. FVE Driver (Apr 05 2010).docx
71. TPM Base Services (Jan 22 2010).docx
72. TPM Driver (Dec 02 2009).docx
73. **Executive**
74. 64 bit Kernel Debug Support (October 23 2009).docx
75. Application Compatibility Support (December 10 2009).docx
76. Cache Manager (October 26 2009).docx
77. Configuration Manager (August 24, 2010).docx
78. Event Tracing for Windows (December 17, 2009).docx
79. Executive Object Services (August 30, 2010).docx
80. Graphics Device Interface (September 16, 2010).docx
81. Hardware Abstraction Layer (HAL) (December 16, 2009).docx
82. Kernel Debug Manager (December 15, 2009).docx
83. Kernel Mode Windows Management Instrumentation (December 10 2009).docx
84. Kernel Runtime (October 23 2009).docx
85. Kernel Transaction Manager (February 2, 2009).docx
86. Advanced Local Procedure Call (ALPC) (August 27, 2010).docx
87. Memory Manager (December 18, 2009).docx
88. Microkernel (December 15, 2009).docx
89. Object Manager (August 9, 2010).docx
90. Plug and Play Manager (December 16, 2009).docx
91. Power Manager (December 16, 2009).docx
92. Process Manager\Process Manager (August 27, 2010).docx
93. Process Manager\Process Manager (August 5, 2010).docx
94. Process Manager\Process Manager (May 8, 2010).docx
95. Raw File System Library (October 23 2009).docx
96. Security Reference Monitor (March 3, 2010).docx
97. Virtual DOS Machine (December 14, 2009).docx
98. Window Manager (User) (August 25, 2010).docx

99. **Hardware**
100. AMD Hardware (7 May 2010).docx
101. Intel Hardware (7 May 2010).docx
102. Intel IA64 Hardware (7 May 2010).docx
103. **IIS**
104. Background Intelligent Transfer Service (BITS) ISAPI (Apr 01 2010).docx
105. IIS CoAdmin DLL (May 19 2010).docx
106. IIS ISAPI Handler (Mar 10 2010).docx
107. IIS Metadata DLL (Mar 10 2010).docx
108. IIS Reset Control (Mar 11 2010).docx
109. IIS RPC Proxy (Apr 01 2010).docx
110. IIS Web Admin Service (May 04 2010).docx
111. IIS Web Server Core (May 04 2010).docx
112. IIS Worker Process (Apr 01 2010).docx
113. Internet Information Services (Apr 01 2010).docx
114. ISAPI DLL for Web Printing (Mar 19 2010).docx
115. Metadata and Admin Service (Apr 05 2010).docx
116. WAM Registration DLL (Mar 19 2010).docx
117. WinHTTP Web Proxy Auto Discovery Service (Mar 19 2010).docx
118. **IO Core**
119. CNG Kernel Cryptography (September 13 2010).docx
120. File System Recognizer Driver (Jan 07 2010).docx
121. Generic Pass-through Driver (Aug 03 2010).docx
122. IO Manager (May 06 2010).docx
123. Kernel Mode Driver Framework (Jan 22 2010).docx
124. Kernel Security Device Driver (Apr 17 2010).docx
125. Kernel Security Support Provider Interface Packages (Aug 3, 2010).docx
126. Mount Manager (Apr 17 2010).docx
127. User-mode Driver Framework Reflector (Apr 17 2010).docx
128. **IO Devices**
129. ACPI Battery Miniclass Driver (May 23 2010).docx
130. ACPI Driver (June 17, 2010).docx
131. ACPI Power Meter Driver (July 6 2010).docx
132. Advanced Host Controller Interface Driver (June 28 2010).docx
133. AtaPort Driver Extension (June 28 2010.docx
134. Audio Port Class Driver (June 28, 2010).docx
135. Beep Driver (May 05 2010).docx
136. Broadcom NetXtreme 57xx Gb NIC Miniport Driver (June 15, 2010).docx
137. Composite Battery Driver (June 21, 2010).docx
138. File System Filter Manager (June 28 2010).docx
139. Hardware Error Device Driver (June 28 2010).docx
140. HID Class Library (August 6, 2010).docx
141. HID Keyboard Filter Driver (July 2, 2010).docx
142. HID Mouse Filter Driver (July 2, 2010).docx
143. HID Parsing Library (July 2, 2010).docx
144. HP ProLiant Smart Array (May 26, 2010).docx
145. i8042 Port Driver (May 24, 2010).docx
146. IDE ATAPI Port Driver (May 21 2010).docx
147. IDE Mini-Port Drivers (May 10 2010).docx
148. Intel Pro 1000 E1G60xx MT NIC Miniport Driver (June 15, 2010).docx
149. Intelligent Platform Management Interface Driver (May 26 2010).docx
150. ISA and EISA Class Driver (Aug 05 2010).docx
151. Keyboard Class Driver (May 14, 2010).docx
152. LSI Serial Attached SCSI Driver (July 3, 2010).docx

153. Microsoft System Management BIOS Driver (June 1, 2010).docx
154. Monitor Class Function Driver (June 10, 2010).docx
155. Mouse Class Driver (June 1, 2010).docx
156. Multipath Support Bus Driver (May 24 2010).docx
157. NULL Driver (May 10 2010).docx
158. NVIDIA nForce NIC Miniport Driver (July 22, 2010).docx
159. Parallel Port Driver (June 10, 2010).docx
160. Partition Manager (May 21 2010).docx
161. Plug and Play PCI Enumerator (May 26 2010).docx
162. Plug and Play Software Device Enumerator (May 24 2010).docx
163. PnP Disk Driver (May 14 2010).docx
164. PNP ISA Bus Driver (June 10, 2010).docx
165. Processor Device Driver (June 2, 2010).docx
166. SCSI CD-ROM Driver (May 14 2010).docx
167. SCSI Class System DLL (May 24 2010).docx
168. SCSI Port Driver (May 15 2010).docx
169. SCSI Tape Class Driver (May 21 2010).docx
170. SecureDigital Bus Driver (June 29 2010).docx
171. Serial Device Driver (June 10, 2010).docx
172. Serial Port Enumerator (June 10, 2010).docx
173. Smart Card Driver Library (May 21, 2010).docx
174. Smart Card Reader Filter Driver (June 13 2010).docx
175. Storage Port Driver (December 14 2009).docx
176. USB Common Class Generic Parent Driver (May 24, 2010).docx
177. USB Host Controller (June 15, 2010).docx
178. USB Host Controller Interface Miniport Drivers (June 14, 2010).docx
179. USB Mass Storage Driver (May 24, 2010).docx
180. USB Miniport Driver for Input Devices (Aug 12 2010).docx
181. USB Root Hub Driver (June 14, 2010).docx
182. User-Mode Bus Enumerator (May 26, 2010).docx
183. VDM Parallel Driver (Aug 12 2010).docx
184. VGA Super VGA Video Driver (Jun 29, 2010).docx
185. Video Port Driver (Aug 12 2010).docx
186. Volume Shadow Copy Driver (June 14 2010).docx
187. Watchdog Driver (May 12, 2010).docx
188. WMI for ACPI (August 6, 2010).docx
189. **IO File**
190. CDROM File System (April 30, 2010).docx
191. Encrypting File System (July 30, 2010).docx
192. Fast FAT File System (July 28, 2010).docx
193. File Information FS MiniFilter (7-9-2010).docx
194. Mailslot Driver (Sep 10 2010).docx
195. NPFS Driver (Sep 10 2010).docx
196. NT File System Driver (Sep 10 2010).docx
197. UDF File System Driver (May 28, 2010).docx
198. Volume Manager Driver and Extension Driver (Jun 29, 2010).docx
199. **IO Network**
200. Ancillary Function Driver for WinSock (May 19 2010).docx
201. Client Side Caching Driver (August 17, 2010).docx
202. Computer Browser Datagram Receiver (June 28 2010).docx
203. Distributed File System Client (April 27, 2010).docx
204. Distributed File System Filter Driver (May 18, 2010).docx
205. FWP IPsec Kernel-Mode API (May 18, 2010).docx
206. HTTP Driver (May 18, 2010).docx

207. IP Filter Driver (May 20 2010).docx
208. IP in IP Encapsulation Driver (May 19 2010).docx
209. Kernel RPC Provider (May 28 2010).docx
210. Loopback Network Driver (June 21, 2010).docx
211. Microsoft Tunnel Interface Driver (June 04 2010).docx
212. Multiple UNC Provider Driver (May 24, 2010).docx
213. NDIS User Mode IO Driver (June 7 2010).docx
214. NDIS Wrapper Driver (June 7, 2010).docx
215. NetBT Transport Driver (June 7, 2010).docx
216. Network Store Interface Proxy Driver (June 7 1010).docx
217. QoS Packet Scheduler (June 7 2010).docx
218. Redirected Drive Buffering SubSystem Driver (June 7 2010).docx
219. Remote NDIS Miniport (Apr 30 2010).docx
220. Server Network Driver (June 7 2010).docx
221. SMB 1.0 Server Driver (July 20, 2010).docx
222. SMB 1.0 Sub-Redirector (April 30, 2010).docx
223. SMB 2.0 Server Driver (June 23, 2010).docx
224. SMB 2.0 Sub-Redirector (June 23, 2010).docx
225. SMB Mini-Redirector (June 25, 2010).docx
226. SMB Transport Driver (April 26, 2010).docx
227. TCPIP Protocol Driver (June 21, 2010).docx
228. TDI Translation Driver (TDX) Driver (June 08 2010).docx
229. TDI Wrapper (Apr 30 2010).docx
230. WebDAV Mini Redirector (Aug 16 2010).docx
231. Winsock 2 IFS Layer Driver (May 6, 2010).docx
232. **Network Support**
233. COM+ Configuration Catalog Server (Apr 16 2010).docx
234. COM+ Event System Service (Apr 16 2010).docx
235. COM+ Services (Aug 12 2010).docx
236. DHCP Service (Aug 03 2010).docx
237. Distributed COM Services (Sep 03 2010).docx
238. Domain Name Service (Feb 04 2010).docx
239. Health Key and Certificate Management Service (Apr 16 2010).docx
240. Internet Key Exchange Service (Aug 16 2010).docx
241. IP Helper Service (Apr 16 2010).docx
242. IPSec SPD Server (Aug 03 2010).docx
243. Network Connections Manager (Aug 6 2010).docx
244. Network Location Awareness (Aug 9 2010).docx
245. Network Policy Server (Sep 17 2010).docx
246. Network Store Interface Service (May 28 2010).docx
247. NPS Host Support (Sep 07 2010).docx
248. Quarantine Agent Proxy and Service Runtime (Aug 11 2010).docx
249. Quarantine Client WMI Provider (Dec 11 2009).docx
250. RPC Endpoint Mapper (Aug 9 2010).docx
251. RPC Locator (Aug 9 2010).docx
252. Simple TCPIP Services Service DLL (Jan 27 2010).docx
253. TCPIP NetBIOS Transport Service (Jan 27 2010).docx
254. Web DAV Service DLL (Apr 16 2010).docx
255. **OS Support**
256. Background Intelligent Transfer Service (Aug 06 2010).docx
257. Distributed File System Service (Mar 17 2010).docx
258. Print Spooler (Sep 07 2010).docx
259. Session Manager (Aug 07 2010).docx
260. WMI Performance Reverse Adapter Service (Apr 05 2010).docx

261. \OS Support\WMI Provider Host\WMI Provider Host (Apr 02 2010).docx
262. WMI Provider Host (Aug 07 2010).docx
263. WMI Service (Aug 07 2010).docx
264. **Security**
265. Active Directory Replication Management (September 11, 2010).docx
266. Core Directory Service (September 9, 2010).docx
267. Credential Manager (June 3, 2010).docx
268. Credential Security Support Provider (Aug 2, 2010).docx
269. Data Protection API (May 12, 2010).docx
270. Directory Services Role Management (June 4, 2010).docx
271. Encrypting File System Service (September 10, 2010).docx
272. Inter-Site Messaging (September 10, 2010).docx
273. KDC Service (Sep 08 2010).docx
274. Kerberos Security Package (Sep 08 2010).docx
275. Key Isolation Service (June 7, 2010).docx
276. LDAP (September 11, 2010).docx
277. LSA Audit (March 17, 2010).docx
278. LSA Authentication (August 5, 2010).docx
279. LSA Policy (September 10, 2010).docx
280. MAPI Based Directory Request (September 9, 2010).docx
281. Microsoft Authentication, V1.0 (Sep 08 2010).docx
282. Microsoft Base Smart Card Crypto Provider (May 13, 2010).docx
283. Microsoft Digest Access (June 2, 2010).docx
284. Microsoft Smart Card Key Storage Provider (May 13, 2010).docx
285. Microsoft Smart Card Minidriver (July 08 2010).docx
286. Net Logon Services DLL (July 02, 2010).docx
287. NT Directory Service Backup and Restore (July 23, 2010).docx
288. PKI Trust Installation and Setup (May 3, 2010).docx
289. Protected Storage Server (May 12, 2010).docx
290. SAM Server (Sep 08 2010).docx
291. Secondary Logon Service (March 22, 2010).docx
292. TLS-SSL Security Provider (June 9, 2010).docx
293. Trust Signing APIs (May 21, 2010).docx
294. Windows Cryptographic Primitives Library (Sep 09 2010).docx
295. **Services**
296. Application Information Service (June 2, 2010).docx
297. Certificate Propagation Service (June 25 2010).docx
298. Computer Browser Service (August 24, 2010).docx
299. Cryptographic Services (Aug 24, 2010).docx
300. Desktop Window Manager (May 07, 2010).docx
301. Diagnostic Policy Service (Aug 4, 2010).docx
302. File Replication Service (September 9, 2010).docx
303. Generic Host Process for Win32 Services (April 5, 2010).docx
304. Interactive Service Detection for Session 0 (June 15, 2010).docx
305. Non-COM WMI Event Provision APIs (June 18 2010).docx
306. Offline Files Service (August 23, 2010).docx
307. Power Management Service (June 15 2010).docx
308. Program Compatibility Assistant Service (June 30, 2010).docx
309. Remote Registry Service (June 17, 2010).docx
310. Server Service DLL (August 24, 2010).docx
311. Services and Controller App (August 24, 2010).docx
312. Smart Card Resource Management Server (July 26, 2010).docx
313. SuperFetch Service Host (June 16, 2010).docx
314. System Event Notification Service (July 22 2010).docx

315. Task Scheduler Engine (June 17, 2010).docx
316. User Mode Driver Framework Service (June 10 2010).docx
317. User Profile Service (July 12, 2010).docx
318. User-Mode Plug-and-Play Service (August 26, 2010).docx
319. Virtual Disk Service (June 16 2010).docx
320. Volume Shadow Copy Service (July 16 2010).docx
321. Windows Eventlog Service (Aug 24, 2010).docx
322. Microsoft Windows Installer Service (Aug 26, 2010).docx
323. Windows Search (June 23 2010).docx
324. Windows Security Center Service (June 16, 2010).docx
325. Windows Security Configuration Editor Engine (July 26, 2010).docx
326. Windows Shell Services DLL (June 17, 2010).docx
327. Windows Time Service (August 24, 2010).docx
328. Windows Update AutoUpdate Engine (Aug 04 2010).docx
329. Workstation Service (August 26, 2010).docx
330. **Virtualization**
331. Hyper-V Image Management Service (July 19 2010).docx
332. Hyper-V Image Management Service (July 20 2010).docx
333. Hyper-V Infrastructure Driver (Aug 31 2010).docx
334. Hyper-V Virtual Machine Management (Aug 02 2010).docx
335. Hyper-V VMBus HID Miniport (September 2, 2010).docx
336. Hypervisor Top Level Functional Specification v2.0.docx
337. VHD Miniport Driver (Aug 16 2010).docx
338. Virtual Machine Bus (Aug 23 2010).docx
339. **Win32**
340. Base Server (August 4 2010).docx
341. Client Server Runtime Process (June 1 2010).docx
342. Windows Server DLL (June 22 2010).docx
343. **Windows Firewall**
344. Application Layer Gateway Service (Feb 23 2010).docx
345. Base Filtering Engine Service (May 22 2010).docx
346. Home Networking Configuration Manager (Jan 13 2010).docx
347. IP Network Address Translator (Aug 20 2010).docx
348. MAC Bridge Driver (Feb 25 2010).docx
349. NAT Helper (Feb 01 2010).docx
350. **Winlogon**
351. Auto Enrollment (May 24 2010).docx
352. Group Policy (Apr 12 2010).docx
353. Group Policy Object Processing (Apr 12 2010).docx
354. Local Session Manager (Apr 13 2010).docx
355. Secure Desktop with Credential User Interface (Apr 12 2010).docx
356. Syskey (May 24 2010).docx
357. Trust Verification APIs (Dec 22 2009).docx
358. Trusted Installer (Feb 23 2010).docx
359. User Environment (Feb 11 2010).docx
360. Windows File Protection (Dec 28 2009).docx
361. Windows Logon Application (Sep 03 2010).docx
362. Windows Logon User Interface Host (Sep 03 2010).docx
363. Windows OS Startup - WiniInit (Feb 11 2010).docx
364. Windows OS Startup - WinLoad (Apr 15 2010).docx
365. Windows OS Startup - WinResume (Jan 08 2010).docx
366. Windows Smartcard Credential Provider (Apr 14 2010).docx

5.2 Guidance Documentation

1. Windows 7 - WS08 R2 Common Criteria Supplemental Admin Guidance (January 7 2011)

5.3 Life Cycle

1. Microsoft Security Response Center EBC, January 2010
2. Windows 7 – WS08 R2 ALC Addendum, January 2010
3. Office SharePoint Server Document Management, May 2007
4. Office SharePoint Server Security, July 2008
5. Microsoft Hyper-V Server 2008 Single Evaluation Report ETR-Part ALC, v 4.0, June 6, 2009
6. Microsoft Information Security InfoSec #4 Network Standard, May 1, 2009
7. GDR Process Primer, May 1, 2009
8. Microsoft Information Security InfoSec #1.0 General Use Standard, May 1, 2009
9. How To Build Hyper-V Official Builds, May 27, 2008
10. Hyper-V CC – OEM Drivers, v 0.1, April 9, 2009
11. Hypervisor Build Tree, v 0.1, June 9, 2005
12. Hypervisor Technology Build Environment Functional Specification, v 0.1, June 6, 2005
13. Hypervisor Technology Build Environment High Level Design Specification, June 6, 2005
14. IT1525 Information Security Policy, February 21, 2008
15. Managed Source Baseline Review, January 14, 2010
16. Microsoft Security Development Lifecycle, v 3.2.4, May 4, 2007
17. BGIT Source Depot Support Overview, May 1, 2009
18. Server Setup Whitepaper, February 19, 2007
19. Threat Model Report, November 15, 2008
20. Viridian Code Review Process, May 1, 2009
21. Branch Plan for Vista, Vista SP1, and Longhorn Server, August 17, 2006
22. Windows Vista/Server 2008 Process Description, v 1.0, October 31, 2008
23. Windows Vista Server 2008 Tools Catalog, September 3, 2008
24. Windows Servicing End2End Overview, April 2007
25. WinSE Branches, November 14, 2008
26. Windows Servicing: HotfixRequest Procedures, June 2,2008
27. WinSE Security GDR Overview, May 1, 2008
28. Microsoft Source Depot Quick Start Guide, August 2, 2005
29. Windows Test Technology Quick Start Guide, September 28, 2007

5.4 Testing

1. Microsoft Windows Common Criteria Evaluation Test Plan
2. **Test Suite Mappings**
    1. (OS) Certificate Service Default Exit Module Test Mapping.docx
    2. (OS) Certificate Service Default Policy Module Test Mapping.docx
    3. (OS) Certificate Service Test Mapping.docx
    4. 64 bit Kernel Debug Support Test Mapping.docx
    5. ACPI Battery Miniclass Driver Test Mapping.docx
    6. ACPI Driver Test Mapping.docx
    7. ACPI Power Meter Driver Test Mapping.docx
    8. Active Directory Replication Management Test Mapping.docx
    9. Advanced Host Controller Interface Driver Test Mapping.docx
    10. Advanced Local Procedure Communication (ALPC) Test
    11. Advanced Local Process Communication (ALPC) Test Mapping.docx
    12. Ancillary Function Driver for WinSock Test Mapping.docx
    13. Application Compatibility Support Test Mapping.docx

14. Application Experience Lookup Service Test Mapping.docx
15. Application Information Service Test Mapping.docx
16. Application Layer Gateway Service Test Mapping.docx
17. AtaPort Driver Extension Test Mapping.docx
18. Audio Port Class Driver Test Mapping.docx
19. Auto Enrollment Test Mapping.docx
20. Background Intelligent Transfer Service (BITS) ISAPI Test
21. Background Intelligent Transfer Service Test Mapping.docx
22. Base Filtering Engine Service Test Mapping.docx
23. Base Server Test Mapping.docx
24. Beep Driver Test Mapping.docx
25. Bitlocker Drive Encryption Service Test Mapping.docx
26. Broadcom NetXtreme 57xx Gb NIC Miniport Driver Test
27. Cache Manager Test Mapping.docx
28. CDROM File System Test Mapping.docx
29. Certificate Propagation Service Test Mapping.docx
30. Certificate Service Test Mapping.docx
31. Client Server Runtime Process Test Mapping.docx
32. Client Side Caching Driver Test Mapping.docx
33. CNG Kernel Cryptography Test Mapping.docx
34. COM+ Configuration Catalog Server Test Mapping.docx
35. COM+ Event System Service Test Mapping.docx
36. COM+ Services Test Mapping.docx
37. Composite Battery Driver Test Mapping.docx
38. Computer Browser Datagram Receiver Test Mapping.docx
39. Computer Browser Service Test Mapping.docx
40. Configuration Manager Test Mapping.docx
41. Core Directory Service Test Mapping.docx
42. Credential Manager Test Mapping.docx
43. Credential Security Support Provider Test Mapping.docx
44. Cryptographic Services Test Mapping.docx
45. Data Protection API Test Mapping.docx
46. Desktop Window Manager Test Mapping.docx
47. DHCP Service Test Mapping.docx
48. Diagnostic Policy Service Test Mapping.docx
49. Digest Test Mapping.docx
50. Directory Services Role Management Test Mapping.docx
51. Distributed COM Services Test Mapping.docx
52. Distributed File System Client Test Mapping.docx
53. Distributed File System Filter Driver Test Mapping.docx
54. Distributed File System Service Test Mapping.docx
55. Domain Name Service Test Mapping.docx
56. Encrypting File System Service Test Mapping.docx
57. Encrypting File System Test Mapping.docx
58. Event Tracing for Windows Test Mapping.docx
59. Executive Object Services Test Mapping.docx
60. Fast FAT File System Test Mapping.docx
61. File Information FS MiniFilter Test Mapping.docx
62. File Replication Service Test Mapping.docx
63. File System Filter Manager Test Mapping.docx
64. File System Recognizer Driver Test Mapping.docx
65. FVE Crash Dump Driver Test Mapping.docx
66. FVE Driver Test Mapping.docx
67. FWP IPsec Kernel-Mode API Test Mapping.docx

68. Generic Host Process for Win32 Services Test Mapping.docx
69. Generic Pass-through Driver Test Mapping.docx
70. Graphics Device Interface (GDI) Test Mapping.docx
71. Group Policy Object Processing Test Mapping.docx
72. Group Policy Test Mapping.docx
73. Hardware Abstraction Layer Test Mapping.docx
74. Hardware Error Device Driver Test Mapping.docx
75. Health Key and Certificate Management Service Test Mapping.docx
76. HID Class Library Test Mapping.docx
77. HID Keyboard Filter Driver Test Mapping.docx
78. HID Mouse Filter Driver Test Mapping.docx
79. HID Parsing Library Test Mapping.docx
80. Home Networking Configuration Manager Test Mapping.docx
81. HP ProLiant Smart Array Test Mapping.docx
82. HTTP Driver Test Mapping.docx
83. HTTPS Test Mapping.docx
84. Hyper-V Image Management Service Test Mapping.docx
85. Hyper-V Infrastructure Driver Library Test Mapping.docx
86. Hyper-V Infrastructure Driver Test Mapping.docx
87. Hyper-V Networking Management Service Test Mapping.docx
88. Hyper-V Virtual Machine Management Test Mapping.docx
89. Hyper-V VMBus HID Miniport Test Mapping.docx
90. i8042 Port Driver Test Mapping.docx
91. IDE ATAPI Port Driver Test Mapping.docx
92. IDE Mini-Port Drivers Test Mapping.docx
93. IIS CoAdmin DLL Test Mapping.docx
94. IIS ISAPI Handler Test Mapping.docx
95. IIS Metadata DLL Test Mapping.docx
96. IIS Reset Control Test Mapping.docx
97. IIS RPC Proxy Test Mapping.docx
98. IIS Web Admin Service Test Mapping.docx
99. IIS Web Server Core Test Mapping.docx
100. IIS Worker Process Test Mapping.docx
101. IKE-IPSEC Test Mapping.docx
102. Intel Pro 1000 E1G60xx MT NIC Miniport Driver Test Mapping.docx
103. Intelligent Platform Management Interface Driver Test
104. Inter-Site Messaging Test Mapping.docx
105. Interactive Service Detection for Session 0 Test Mapping.docx
106. Internet Extensions for Win32 Test Mapping.docx
107. Internet Information Services Test Mapping.docx
108. Internet Key Exchange Service Test Mapping.docx
109. IO Manager Test Mapping.docx
110. IP Filter Driver Test Mapping.docx
111. IP Helper Service Test Mapping.docx
112. IP in IP Encapsulation Driver Test Mapping.docx
113. IP Network Address Translator Test Mapping.docx
114. IPSec SPD Server Test Mapping.docx
115. ISA and EISA Class Driver Test Mapping.docx
116. ISAPI DLL for Web Printing Test Mapping.docx
117. KDC Service Test Mapping.docx
118. Kerberos Security Package Test Mapping.docx
119. Kerberos Test Mapping.docx
120. Kernel Debug Manager Test Mapping.docx
121. Kernel Mode Driver Framework Loader Test Mapping.docx

122.Kernel Mode Driver Framework Test Mapping.docx
123.Kernel Mode Windows Management Instrumentation Test
124.Kernel RPC Provider Test Mapping.docx
125.Kernel Runtime Test Mapping.docx
126.Kernel Security Device Driver Test Mapping.docx
127.Kernel Security Support Provider Interface Packages Test
128.Kernel Transaction Manager Test Mapping.docx
129.Key Isolation Service Test Mapping.docx
130.Keyboard Class Driver Test Mapping.docx
131.LDAP (Protocol) Test Mapping.docx
132. LDAP Test Mapping.docx
133.Local Session Manager Test Mapping.docx
134.Loopback Network Driver Test Mapping.docx
135.LSA Audit Test Mapping.docx
136.LSA Authentication Test Mapping.docx
137. LSA Policy Test Mapping.docx
138.LSI Serial Attached SCSI Driver Test Mapping.docx
139.MAC Bridge Driver Test Mapping.docx
140.Mailslot Driver Test Mapping.docx
141.MAPI Based Directory Request Test Mapping.docx
142.ppings.txt
143.Memory Manager Test Mapping.docx
144.Metadata and Admin Service Test Mapping.docx
145.Microkernel Test Mapping.docx
146.Microsoft Authentication, V1.0 Test Mapping.docx
147.Microsoft Base Smart Card Crypto Provider Test Mapping.docx
148.Microsoft Digest Access Test Mapping.docx
149.Microsoft Smart Card Key Storage Provider Test Mapping.docx
150.Microsoft Smart Card Minidriver Test Mapping.docx
151.Microsoft System Management BIOS Driver Test Mapping.docx
152.Microsoft Tunnel Interface Driver Test Mapping.docx
153.Microsoft Windows Installer Service Test Mapping.docx
154.Monitor Class Function Driver Test Mapping.docx
155.Mount Manager Test Mapping.docx
156.Mouse Class Driver Test Mapping.docx
157.Multipath Support Bus Driver Test Mapping.docx
158.Multiple UNC Provider Driver Test Mapping.docx
159.NAT Helper Test Mapping.docx
160.NDIS User Mode IO Driver Test Mapping.docx
161.NDIS Wrapper Driver Test Mapping.docx
162.Net Logon Services DLL Test Mapping.docx
163.NetBT Transport Driver Test Mapping.docx
164.Network Connections Manager Test Mapping.docx
165.Network Location Awareness Test Mapping.docx
166.Network Policy Server Test mapping.docx
167.Network Store Interface Proxy Driver Test Mapping.docx
168.Network Store Interface Service Test Mapping.docx
169.Non-COM WMI Event Provision APIs Test Mapping.docx
170.NPFS Driver Test Mapping.docx
171.NPS Host Support Test Mapping.docx
172.NT Directory Service Backup and Restore Test Mapping.docx
173.NT File System Driver Test Mapping.docx
174.NTLM Test Mapping.docx
175.NULL Driver Test Mapping.docx

176.NVIDIA nForce NIC Miniport Driver Test Mapping.docx
177.Object Manager Test Mapping.docx
178.Offline Files Service Test Mapping.docx
179.Online Responder Service Test Mapping.docx
180.Parallel Port Driver Test Mapping.docx
181.Partition Manager Test Mapping.docx
182.PKI Test Mapping.docx
183.PKI Trust Installation and Setup Test Mapping.docx
184.Plug and Play Manager Test Mapping.docx
185.Plug and Play PCI Enumerator Test Mapping.docx
186.Plug and Play Software Device Enumerator Test Mapping.docx
187.PnP Disk Driver Test Mapping.docx
188.PNP ISA Bus Driver Test Mapping.docx
189.Power Management Service Test Mapping.docx
190.Power Manager Test Mapping.docx
191. Print Spooler Test Mapping.docx
192. Process Manager Test Mapping.docx
193.Processor Device Driver Test Mapping.docx
194.Program Compatibility Assistant Service Test Mapping.docx
195.Protected Storage Server Test Mapping.docx
196.QoS Packet Scheduler Test Mapping.docx
197.Quarantine Agent Proxy and Service Runtime Test Mapping.docx
198.Quarantine Client WMI Provider Test Mapping.docx
199.Raw File System Library Test Mapping.docx
200.Redirected Drive Buffering SubSystem Driver Test Mapping.docx
201.Remote NDIS Miniport Test Mapping.docx
202.Remote Registry Service Test Mapping.docx
203.RPC Endpoint Mapper Test Mapping.docx
204.RPC Locator Test Mapping.docx
205. SAM Server Test Mapping.docx
206.SCSI CD-ROM Driver Test Mapping.docx
207.SCSI Class System DLL Test Mapping.docx
208.SCSI Port Driver Test Mapping.docx
209.SCSI Tape Class Driver Test Mapping.docx
210.Secondary Logon Service Test Mapping.docx
211.Secure Desktop with Credential User Interface Test Mapping.docx
212.SecureDigital Bus Driver Test Mapping.docx
213.Security Reference Monitor Test Mapping.docx
214.Serial Device Driver Test Mapping.docx
215.Serial Port Enumerator Test Mapping.docx
216.Server Network Driver Test Mapping.docx
217.Server Service DLL Test Mapping.docx
218.Services and Controller App Test Mapping.docx
219.Session Manager Test Mapping.docx
220.Simple TCPIP Services Service DLL Test Mapping.docx
221.Smart Card Driver Library Test Mapping.docx
222.Smart Card Reader Filter Driver Test Mapping.docx
223.Smart Card Resource Management Server Test Mapping.docx
224.SMB 1.0 Server Driver Test Mapping.docx
225.SMB 1.0 Sub-Redirector Test Mapping.docx
226.SMB 2.0 Server Driver Test Mapping.docx
227.SMB 2.0 Sub-Redirector Test Mapping.docx
228.SMB Mini-Redirector Test Mapping.docx
229.SMB Transport Driver Test Mapping.docx

230. Storage Port Driver Test Mapping.docx
231. Superfetch Service Host Test Mapping.docx
232. Syskey Test Mapping.docx
233. System Event Notification Service Test Mapping.docx
234. Task Scheduler Engine Test Mapping.docx
235. TCPIP NetBIOS Transport Service Test Mapping.docx
236. TCPIP Protocol Driver Test Mapping.docx
237. Tcpip Services Application Test Mapping.docx
238. TDI Translation Driver (TDX) Driver Test Suite.docx
239. TDI Wrapper Test Mapping.docx
240. TLS Test Mapping.docx
241. TLS-SSL Security Provider Test Mapping.docx
242. TPM Base Services Dll Test Mapping.docx
243. TPM Base Services Test Mapping.docx
244. TPM Driver Test Mapping.docx
245. Trust Signing APIs Test Mapping.docx
246. Trust Verification APIs Test Mapping.docx
247. Trusted Installer Test Mapping.docx
248. UDF File System Driver Test Mapping.docx
249. Universal Plug and Play Device Host Test Mapping.docx
250. USB Common Class Generic Parent Driver Test Mapping.docx
251. USB Host Controller Interface Miniport Drivers Test Mapping.docx
252. USB Host Controller Test Mapping.docx
253. USB Mass Storage Driver Test Mapping.docx
254. USB Miniport Driver for Input Devices Test Mapping.docx
255. USB Root Hub Driver Test Mapping.docx
256. User Environment Test Mapping.docx
257. User Mode Driver Framework Reflector Test Mapping.docx
258. User Mode Driver Framework Service Test Mapping.docx
259. User Profile Service Test Mapping.docx
260. User-Mode Bus Enumerator Test Mapping.docx
261. User-Mode Plug-and-Play Service Test Mapping.docx
262. VDM Parallel Driver Test Mapping.docx
263. VGA Super VGA Video Driver Test Mapping.docx
264. VHD Miniport Driver Test Mapping.docx
265. Video Port Driver Test Mapping.docx
266. Virtual Disk Service Test Mapping.docx
267. Virtual DOS Machine Test Mapping.docx
268. Virtual Machine Bus Test Mapping.docx
269. Volume Manager Driver and Extension Driver Test Mapping.docx
270. Volume Shadow Copy Driver Test Mapping.docx
271. Volume Shadow Copy Service Test Mapping.docx
272. WAM Registration DLL Test Mapping.docx
273. Watchdog Driver Test Mapping.docx
274. Web DAV Service DLL Test Mapping.docx
275. WebDAV Mini Redirector Test Mapping.docx
276. Window Manager (User) Test Mapping.docx
277. Windows Cryptographic Primitives Library Test Mapping.docx
278. Windows Eventlog Service Test Mapping.docx
279. Windows File Protection Test Mapping.docx
280. Windows Logon Application Test Mapping.docx
281. Windows Logon User Interface Host Test Mapping.docx
282. Windows OS Startup - WiniInit Test Mapping.docx
283. Windows OS Startup - WinLoad Test Mapping.docx

284.Windows OS Startup - WinResume Test Mapping.docx
285.Windows Search Test Mapping.docx
286.Windows Security Center Service Test Mapping.docx
287.Windows Security Configuration Editor Engine Test Mapping.docx
288.Windows Server DLL Test Mapping.docx
289.Windows Shell Services DLL Test Mapping.docx
290.Windows Smartcard Credential Provider Test Mapping.docx
291.Windows Time Service Test Mapping.docx
292. Windows Update AutoUpdate Engine Test Mapping.docx
293.WinHTTP Web Proxy Auto Discovery Service Test Mapping.docx
294.Winsock 2 IFS Layer Driver Test Mapping.docx
295.WMI for ACPI Test Mapping.docx
296.WMI Performance Reverse Adapter Service Test Mapping.docx
297.WMI Provider Host Test Mapping.docx
298. WMI Service Test Mapping.docx
299.Workstation Service Test Mapping.docx

300.Legacy Test Suites

301. AccessControl.docx
302. AdminAccess.docx
303. AuthProvider.docx
304. CertServer.docx
305. ComPlus.docx
306. ComPlusEventSys.docx
307. DCOM.docx
308. Devices.docx
309. DS Replication.docx
310. Gdi.docx
311. HandleEnforcement.docx
312. HTTPClient.docx
313. IA32-Hardware.docx
314. IA64-Hardware.docx
315. Impersonation.docx
316.KDC.docx
317. LDAP.docx
318. MAPI.docx
319.Miscellaneous.docx
320. NetSupport.docx
321. ObjectReuse.docx
322. Privilege.docx
323. RPC Security.docx
324. ServerDriver.docx
325.SpecialAccess.docx
326.SpecialAccessBW.docx
327.Token.docx
328.User.docx
329.Windows Firewall.docx
330. X64-Hardware.docx

331.Goby Test Suites:

332. 64 bit Kernel Debug Support.docx
333. ACPI Driver.docx
334. Advanced Local Process Communication.docx
335. Application Compatibility Support.docx
336. Application Experience Lookup Service.docx
337. Application Information Service.docx

338. Background Intelligent Transfer Service.docx
339. Base Filtering Engine Service.docx
340. BITS Server Extensions ISAPI.docx
341. Client Side Caching Driver.docx
342. CNG Kernel Cryptography.docx
343. Computer Browser Service.docx
344. Configuration Manager.docx
345. Credential Manager.docx
346. Cryptographic Service Test Suite.docx
347. Desktop Window Manager.docx
348. Event Log Service.docx
349. Event Tracing for Windows.docx
350. Executive Object Services.docx
351. FileInfo Filter Driver.docx
352. Health Key and Certificate Management Service.docx
353. HID Class Library.docx
354. IIS CoAdmin.docx
355. Internet Key Exchange Service.docx
356. ISAPI DLL for Web Printing.docx
357. Kernel Debug Manager.docx
358. Kernel Mode Driver Framework.docx
359. Kernel Mode Windows Management Instrumentation.docx
360. Kernel Transaction Manager.docx
361. Key Isolation Service.docx
362. Local Session Manager.docx
363. Memory Manager.docx
364. Multiple UNC Provider driver.docx
365. NDIS 5.1 Wrapper Driver.docx
366. Network Location Awareness.docx
367. Network Policy Server.docx
368. Network Store Interface Proxy Driver.docx
369. Object Manager.docx
370. Plug and Play Manager.docx
371. Power Manager.docx
372. RPC Proxy.docx
373. Server Network Driver.docx
374. SMB 2.0 Server Driver.docx
375. SMB Mini-Redirector.docx
376. SMB Transport Driver.docx
377. SuperFetch Service Host.docx
378. TCPIP NetBIOS Transport Service.docx
379. TCPIP Protocol Driver.docx
380. TDI Translation Driver.docx
381. TPM Base Services.docx
382. Trusted Installer.docx
383. USB 1.1 and 2.0 Port Driver.docx
384. USB Mass Storage Driver.docx
385. User Profile Services.docx
386. User-mode Driver Framework Reflector.docx
387. VDM Parallel Driver.docx
388. Virtual DOS Machine.docx
389. Volume Manager Driver.docx
390. Volume Shadow Copy Driver.docx
391. Web DAV Service DLL.docx

392. Windows Cryptographic Primitives Library.docx
393. Windows OS Startup.docx
394. Windows Time Service.docx
395. Windows Update AutoUpdate Engine Test.docx
396. WMI Provider Host.docx
397. Actual Test Results

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 7 and Windows Server 2008 R2, Version 2.0, December 3, 2010.

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 team tests was limited. A total of eighteen 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.

The evaluation team also conducted thirteen penetration tests. The penetration tests fall in the following areas: cached logon, access to special accounts and resources, registry settings, erroneous IP packets, configuration settings, audit, obsolete TSFI, and invalid TSFI inputs.

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.

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

- Microsoft Windows 7 Enterprise Edition (32-bit and 64-bit versions)
- Microsoft Windows 7 Ultimate Edition (32-bit and 64-bit versions)
- Microsoft Windows Server 2008 R2 Standard Edition
- Microsoft Windows Server 2008 R2 Enterprise Edition
- Microsoft Windows Server 2008 R2 Datacenter Edition
- Microsoft Windows Server 2008 R2 Itanium Edition

The following security updates and patches must be applied to the above Windows 7 products:

- All security updates as of September 14, 2010 as well as the updates associated with security bulletins MS10-073 and MS10-085, and hotfix KB2492505.

The following security updates must be applied to the above Windows Server 2008 R2 products:

- All security updates as of September 14, 2010 as well as the updates associated with security bulletins MS10-073 and MS10-085, and hotfix KB2492505.

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), 64-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
- HP Integrity rx1620, 1.3 Ghz Intel Itanium Processor (1 CPU), 64-bit (Itanium)
- Microsoft Hyper-V
- Microelectronics Trusted Platform Module [SMO1200]
- GemPlus GemPC Twin USB smart card reader

To use the product in the evaluated configuration, the product must be configured as specified in the Windows 7 - WS08 R2 Common Criteria Supplemental Admin Guidance (January 7 2011).

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 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 3.1 and CEM version 3.1 [5], [6]. The evaluation determined the Windows 7 and Windows Server 2008 R2 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 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 7 and Windows Server 2008 R2 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 Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document.

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 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.

8.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE. The ALC evaluation also ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.3 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

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 Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The 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 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration 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 Summary of Evaluation Results

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

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

- During evaluation team testing, the team discovered that the user account name is not recorded when a standard user attempts to access the security audit log using the Event Viewer tool. Instead of recording the user account name, SYSTEM is recorded in the user field of the audit record.
- Due to the size and complexity of the product, the ST's TOE Summary Specification (TSS) contains references to MSDN and other documentation that can be used by readers to obtain further information on what was evaluated and tested in greater detail. As the underlying documents to which a URL points can change, care should be taken in ensuring that the references (when followed by the reader) actually apply to the evaluated product.
- Most named objects identified in the TSS have special access rights that are unique to each object. These access rights are not identified in the TSS, but were identified in the

evaluation evidence used by the team and tested during the evaluation. Details for many of these access rights can be found by searching the MSDN library.

10 Annexes

Not applicable.

11 Security Target

The Security Target is identified as Microsoft Windows 7 and Windows Server 2008 R2 Security Target, Version 1.0, March 23rd, 2011.

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 3.1, Revision 3, dated: July 2009.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 3, dated: July 2009.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 3, dated: July 2009.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 3, dated: July 2009.

[5] 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.

[6] Science Applications International Corporation. *Evaluation Technical Report for the Windows 7 and Windows Server 2008 R2 Part 2 (Proprietary)*, Version 1.0, December 3, 2010.

[7] Science Applications International Corporation. *Evaluation Team Test Report for Windows 7 and Windows Server 2008 R2 Part 2 Supplement (SAIC and Microsoft Proprietary)*, Version 1.0, December 3, 2010.

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

[8] *Windows 7 and Windows Server 2008 R2* Security Target, Version 1.0, March 23rd, 2011.