National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, and Microsoft Windows 10 Hyper-V

Report Number: CCEVS-VR-10823-2017
Dated: November 20, 2017
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Sheldon Durrant
Jerome Myers

Common Criteria Testing Laboratory

Leidos
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user to determine the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), (which is where specific security claims are made) as well as this Validation Report (VR) (which describes how those security claims were evaluated, tested, and any restrictions that may be imposed upon the evaluated configuration) to help in that determination. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Microsoft Windows Server 2016, Microsoft Windows Server 2016 Datacenter edition, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012 R2 Datacenter edition, and Microsoft Windows 10 Enterprise Edition (64-bit version) Hyper-V.

The following hardware platforms were used during testing:

- Surface Book
- Dell OptiPlex 3040
- HP ProDesk 600 G2

This report presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of Microsoft Windows Server 2016, Microsoft Windows Server 2016 Datacenter edition, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012 R2 Datacenter edition, and Microsoft Windows 10 Enterprise Edition (64-bit version) Hyper-V was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in November 2017. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and the assurance activities specified in Protection Profile for Server Virtualization, version 1.1, September 14, 2015. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that Microsoft Windows Server 2016, Microsoft Windows Server 2016 Datacenter edition, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012 R2 Datacenter edition, and Microsoft Windows 10 Enterprise Edition (64-bit version) Hyper-V is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfied all of the security functional requirements stated in the ST. The information in this VR is largely derived from the publically available Assurance Activities Report (AAR) and the associated proprietary test report produced by the Leidos evaluation team.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PP had been completed successfully and that the product satisfied all of the security functional and assurance requirements as stated in the 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.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Microsoft Windows Server 2016, Microsoft Windows Server 2016 Datacenter edition, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012 R2 Datacenter edition, and Microsoft Windows 10 Enterprise Edition (64-bit version) Hyper-V
Sponsor & Developer	Michael Grimm Microsoft Corporation
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	November 2017
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	Protection Profile for Server Virtualization, Version 1.1, September 14, 2015 (SV PP)
Evaluation Class	None
Disclaimer	The information contained in this Validation Report is not an endorsement of the Microsoft Windows Server 2016, Microsoft Windows Server 2016 Datacenter edition, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012 R2 Datacenter edition, and Microsoft Windows 10 Enterprise Edition (64-bit version) Hyper-V by any agency of the U.S. Government and no warranty of Microsoft Windows Server 2016, Microsoft Windows Server 2016 Datacenter edition, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012 R2 Datacenter edition, and Microsoft Windows 10 Enterprise Edition (64-bit version) Hyper-V is either expressed or implied.
Evaluation Personnel	Gregory Beaver Dawn Campbell Gary Grainger Robert Russ Amit Sharma Kevin Steiner

Item	Identifier
Validation Personnel	Paul Bicknell: Senior Validator Sheldon Durrant: Lead Validator Jerome Myers: Lead Validator

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) 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 Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows 10 Hyper-V Security Target
ST Version	0.07
Publication Date	November 17, 2017
Vendor and ST Author	Microsoft
TOE Reference	Microsoft Windows Server 2016, Microsoft Windows Server 2016 Datacenter edition, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012 R2 Datacenter edition, Microsoft Windows 10 Enterprise Edition (64-bit version) Hyper-V
TOE Software Version	• Microsoft Windows Server 2016 • Microsoft Windows Server 2016 Datacenter edition • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 R2 Datacenter edition • Microsoft Windows 10 Enterprise Edition (64-bit version)
Keywords	Virtualization, Hypervisor

2.1 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

- If it is possible for data to leak between domains when prohibited by policy, then an adversary on one domain or network can obtain data from another domain. Such cross-domain data leakage can, for example, cause classified information, corporate proprietary information, or medical data to be made accessible to unauthorized entities.
- A malicious party attempts to supply the Administrator with an update to the product that may compromise the security features of the TOE.

- Malware running on the physical host must not be able to undetectably modify Virtualization System components while the system is running or at rest. Likewise, malicious code running within a virtual machine must not be able to modify Virtualization System components.
- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- Vulnerabilities in 3rd party software can lead to VMM compromise. Where possible, the VS should mitigate the results of potential vulnerabilities or malicious content in third-party code.
- Failure of security mechanisms could lead to unauthorized intrusion into or modification of the VMM or bypass of the VMM altogether.
- The hosting of untrusted or malicious domains by the VS cannot be permitted to compromise the security and integrity of the platform on which the VS executes.
- A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- A threat of weak cryptography may arise if the VMM does not provide sufficient entropy to support security-related features that depend on entropy to implement cryptographic algorithms.
- The Virtualization System itself is generally part of a larger enterprise network and must be updated and patched as a normal part of enterprise network operations. Such basic network hygiene is more difficult if the enterprise network is unmanageable

2.2 Organizational Security Policies

There are no Organizational Security Policies for the protection profile.

3 Architectural Information

The TOE is a software solution that consists of Microsoft Windows Server 2016, Microsoft Windows Server 2016 Datacenter edition, Microsoft Windows Server 2012 R2, Microsoft Windows Server 2012 R2 Datacenter edition, Microsoft Windows 10 Enterprise Edition (64-bit version) Hyper-V.

The following hardware platforms were used during testing:

- Surface Book
- Dell OptiPlex 3040
- HP ProDesk 600 G2

The TOE includes hypervisor and virtualization subsystem, known as "Hyper-V" in the Microsoft Windows Server 2016 operating system, the Microsoft Windows Server 2012 R2 operating system, the Microsoft 10 operating system, supporting operating system services, and those applications necessary to manage, support and configure the operating system and virtualization subsystem.

Hyper-V enables the computer administrator to specify "partitions" that have separate address spaces where they can load an operating system and applications operating in parallel of the (host) operating system that executes in the root partition of the computer. An operating system executing in a partition has access to virtualized peripheral devices that is controlled by Hyper-V. An operating system may either access devices using the same I/O related instructions as on a real system or it may use a specific interface offered by Hyper-V, called the VMBus, to communicate with Hyper-V for access to peripheral devices. In the first case the operating system can only access the devices virtualized by Hyper-V. When using the VMBus interface, an operating system in a guest partition must have "enlightenments" that establish the VMBus communication and then use those "synthetic" devices accessible via VMBus. Note that the "enlightenments" within a guest operating system is part of the TOE, but not part of the TSF.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- The platform has not been compromised prior to installation of the Virtualization System.
- Physical security commensurate with the value of the TOE and the data it contains is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific operating system editions and software versions identified in this document, and not any earlier or later versions released or in process. For example, functionality that is offered in Windows 10 Home edition was not evaluated.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities of the product were not covered by this evaluation. Any additional non-security related functional capabilities of the product, even those described in the ST, were not covered by this evaluation.
4. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

5.1 Security Audit

Windows has the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes the date and time of the event, the user identity that caused the event to be generated, and other event specific data. Authorized administrators can review audit logs and have 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. In the context of this evaluation, the protection profile requirements cover generating audit events, selecting which events should be audited, and providing secure storage for audit event entries.

5.2 Cryptographic Support

Windows provides validated cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, cryptographic key agreement (which is not studied in this evaluation), 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. Windows also provides extensive auditing support of cryptographic operations, the ability to replace cryptographic functions and random number generators with alternative implementations[1], and a key isolation service designed to limit the potential exposure of secret and private keys. In addition to using cryptography for its own security functions, Windows offers access to the cryptographic support functions for user-mode and kernel-mode programs. Public key certificates generated and used by Windows authenticate users and machines as well as protect both user and system data in transit.

- IPsec: Windows implements IPsec to provide protected, authenticated, confidential, and tamper-proof networking between two peer computers.
- TLS: Windows implements TLS to provide protected, authenticated, confidential, and tamper-proof networking between two peer computers.

5.3 User Data Protection

In the context of this evaluation Windows protects computer virtualization capabilities.

5.4 Identification and Authentication

In the context of this evaluation, Windows provides the ability to use, store, and protect X.509 certificates that are used for IPsec and TLS authenticates the administrator to the computer.

5.5 Security Management

Windows includes several functions to manage security policies. Policy management is controlled through a combination of access control, membership in administrator groups, and privileges.

[1] This option is not included in the Windows Common Criteria evaluation.

5.6 Protection of the TSF

Windows provides a number of features to ensure the protection of TOE security functions. Windows protects against unauthorized data disclosure and modification by using a suite of Internet standard protocols including IPsec, IKE, and TLS. Windows ensures process isolation security for all processes through private virtual address spaces, execution context, and security context. The Windows data structures defining process address space, execution context, memory protection, and security context are stored in protected kernel-mode memory. Windows includes self-testing features that ensure the integrity of executable program images and its cryptographic functions. Finally, Windows provides a trusted update mechanism to update Windows binaries itself.

5.7 Session Locking

In the context of this evaluation Windows allows an authorized administrator to configure the system to display a logon banner before the logon dialog.

5.8 Trusted Path/Channels

Windows uses the IPsec suite of protocols to provide a Virtual Private Network Connection (VPN) between itself, acting as a VPN client, and a VPN gateway in addition to providing protected communications for HTTPS and TLS.

6 Documentation

Microsoft offers a number of guidance documents along with a CC-specific supplemental document describing the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- *Windows 10, Server 2016, and Server 2012 R2 Server Virtualization Operational Guidance*, Version 0.61, October 30, 2017

The above document is considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

The Security Target used is:

- *Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows 10 Hyper-V Security Target*, Version 0.07, November 17, 2017

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary documents:

- *Microsoft Windows Server 2016, Windows Server 2012 R2, and Windows 10 Hyper-V Common Criteria Test Report and Procedures for Server Virtualization PP Report*, Version 1.0, Dated: October 30, 2017

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- *Microsoft Windows Server 2016, Windows Server 2012 R2, and Windows 10 Hyper-V Assurance Activity Report*, Version 1.0, December 7, 2017

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to (SV PP).

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in (SV PP). The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place primarily at the Leidos CCTL location in Columbia, Maryland. The evaluation team performed limited testing at Microsoft facilities in Redmond, Washington.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for (SV PP) were fulfilled.

8 Evaluated Configuration

The evaluated version of the TOE consists of the following software combinations.

TOE Software Identification: The following Windows Operating System editions are included in the evaluation:

- Microsoft Windows Server 2016
- Microsoft Windows Server 2016 Datacenter edition
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012 R2 Datacenter edition
- Microsoft Windows 10 Enterprise Edition (64-bit version) Hyper-V

The devices used in the test configuration were:

- Surface Book with Microsoft Windows 10 Creators Update Enterprise edition
- Surface Book with Microsoft Windows Server 2016 Datacenter edition
- Dell Optiplex 3040 with Microsoft Windows Server 2016 Standard edition
- Dell Optiplex 3040 with Microsoft Windows Server 2016 Datacenter edition
- HP ProDesk 600 G2 with Microsoft Windows Server 2012 R2 Standard edition
- HP ProDesk 600 G2 with Microsoft Windows Server 2012 R2 Datacenter edition

The following security updates must be applied to the above Windows 10 products:

- All critical updates as of June 30, 2017

The TOE must be deployed as described in section 4 Assumptions of this document and be configured in accordance with the

- *Windows 10, Server 2016, and Server 2012 R2 Server Virtualization Operational Guidance*, Version 0.61, October 30, 2017

Per Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for Server Virtualization, version 1.1, September 14, 2015 (SV PP) in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ASE_CCL.1	Conformance claims
ASE_ECD.1	Extended components definition
ASE_INT.1	ST introduction
ASE_OBJ.1	Security objectives for the operational environment
ASE_REQ.1	Stated security requirements
ASE_SPD.1	Security Problem Definition
ASE_TSS.1	TOE summary specification
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ALC_TSU_EXT.1	Timely Security Updates
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

10 Validator Comments/Recommendations

None

11 Annexes

Not applicable.

12 Security Target

Name	Description
ST Title	Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows 10 Hyper-V Security Target
ST Version	0.07
Publication Date	November 17, 2017

13 Abbreviations and Acronyms

ACE	Access Control Entry
ACL	Access Control List
ACP	Access Control Policy
AD	Active Directory
ADAM	Active Directory Application Mode
AES	Advanced Encryption Standard
AGD	Administrator Guidance Document
AH	Authentication Header
ALPC	Advanced Local Process Communication
ANSI	American National Standards Institute
API	Application Programming Interface
APIC	Advanced Programmable Interrupt Controller
BTG	BitLocker To Go
CA	Certificate Authority
CBAC	Claims Basic Access Control, see DYN
CBC	Cipher Block Chaining
CC	Common Criteria
CD-ROM	Compact Disk Read Only Memory
CIFS	Common Internet File System
CIMCPP	Certificate Issuing and Management Components For Basic Robustness Environments Protection Profile, Version 1.0, April 27, 2009
CM	Configuration Management; Control Management
COM	Component Object Model
CP	Content Provider
CPU	Central Processing Unit
CRL	Certificate Revocation List
CryptoAPI	Cryptographic API
CSP	Cryptographic Service Provider
DAC	Discretionary Access Control
DACL	Discretionary Access Control List
DC	Domain Controller
DEP	Data Execution Prevention
DES	Data Encryption Standard
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DFS	Distributed File System
DMA	Direct Memory Access
DNS	Domain Name System
DS	Directory Service
DSA	Digital Signature Algorithm
DYN	Dynamic Access Control
EAL	Evaluation Assurance Level
ECB	Electronic Code Book
EFS	Encrypting File System
ESP	Encapsulating Security Protocol

FEK	File Encryption Key
FIPS	Federal Information Processing Standard
FRS	File Replication Service
FSMO	Flexible Single Master Operation
FTP	File Transfer Protocol
FVE	Full Volume Encryption
GB	Gigabyte
GC	Global Catalog
GHz	Gigahertz
GPC	Group Policy Container
GPO	Group Policy Object
GPOSPP	US Government Protection Profile for General-Purpose Operating System in a Networked Environment
GPT	Group Policy Template
GPT	GUID Partition Table
GUI	Graphical User Interface
GUID	Globally Unique Identifiers
HTTP	Hypertext Transfer Protocol
HTTPS	Secure HTTP
I/O	Input / Output
I&A	Identification and Authentication
IA	Information Assurance
ICF	Internet Connection Firewall
ICMP	Internet Control Message Protocol
ICS	Internet Connection Sharing
ID	Identification
IDE	Integrated Drive Electronics
IETF	Internet Engineering Task Force
IFS	Installable File System
IIS	Internet Information Services
IKE	Internet Key Exchange
IP	Internet Protocol
IPv4	IP Version 4
IPv6	IP Version 6
IPC	Inter-process Communication
IPI	Inter-process Interrupt
IPsec	IP Security
ISAPI	Internet Server API
IT	Information Technology
KDC	Key Distribution Center
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPC	Local Procedure Call
LSA	Local Security Authority
LSASS	LSA Subsystem Service
LUA	Least-privilege User Account
MAC	Message Authentication Code
MB	Megabyte
MMC	Microsoft Management Console

MSR	Model Specific Register
NAC	(Cisco) Network Admission Control
NAP	Network Access Protection
NAT	Network Address Translation
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NLB	Network Load Balancing
NMI	Non-maskable Interrupt
NTFS	New Technology File System
NTLM	New Technology LAN Manager
OS	Operating System
PAE	Physical Address Extension
PC/SC	Personal Computer/Smart Card
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PP	Protection Profile
RADIUS	Remote Authentication Dial In Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RAS	Remote Access Service
RC4	Rivest's Cipher 4
RID	Relative Identifier
RNG	Random Number Generator
RPC	Remote Procedure Call
RSA	Rivest, Shamir and Adleman
RSASSA	RSA Signature Scheme with Appendix
SA	Security Association
SACL	System Access Control List
SAM	Security Assurance Measure
SAML	Security Assertion Markup Language
SAR	Security Assurance Requirement
SAS	Secure Attention Sequence
SD	Security Descriptor
SHA	Secure Hash Algorithm
SID	Security Identifier
SIP	Session Initiation Protocol
SIPI	Startup IPI
SF	Security Functions
SFP	Security Functional Policy
SFR	Security Functional Requirement
SMB	Server Message Block
SMI	System Management Interrupt
SMTP	Simple Mail Transport Protocol
SP	Service Pack
SPI	Security Parameters Index
SPI	Stateful Packet Inspection
SRM	Security Reference Monitor
SSL	Secure Sockets Layer

SSP	Security Support Providers
SSPI	Security Support Provider Interface
ST	Security Target
SYSVOL	System Volume
TCP	Transmission Control Protocol
TDI	Transport Driver Interface
TLS	Transport Layer Security
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSS	TOE Summary Specification
UART	Universal Asynchronous Receiver / Transmitter
UI	User Interface
UID	User Identifier
UNC	Universal Naming Convention
US	United States
UPN	User Principal Name
URL	Uniform Resource Locator
USB	Universal Serial Bus
USN	Update Sequence Number
v5	Version 5
VDS	Virtual Disk Service
VMM	Virtual Machine Manager
VPN	Virtual Private Network
VS	Virtualization System
WAN	Wide Area Network
WCF	Windows Communications Framework
WebDAV	Web Document Authoring and Versioning
WebSSO	Web Single Sign On
WDM	Windows Driver Model
WIF	Windows Identity Framework
WMI	Windows Management Instrumentation
WSC	Windows Security Center
WU	Windows Update
WSDL	Web Service Description Language
WWW	World-Wide Web
X64	A 64-bit instruction set architecture
X86	A 32-bit instruction set architecture

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] Microsoft Windows Server 2016, Microsoft Windows Server 2012 R2, Microsoft Windows 10 Hyper-V Security Target, Version 0.07, November 17, 2017

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report for Microsoft Hyper-V Server Virtualization Evaluation, Version 1.0, December 7, 2017

[8] Microsoft Windows 10, Server 2016, and Server 2012 R2 Server Virtualization Operational Guidance, Version 0.61, October 30, 2017