

Protection Profile for Virtualization



Version: 2.0
2025-06-11

National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2016-11-17	Initial Publication
1.1	2021-06-14	Incorporate TDs, Reference TLS Package, Add Equivalency Guidelines, etc.
1.1.1	2021-08-19	Errata release. Fixes a few typos.
2.0	2025-06-11	CC:2022 conversion, remove Modules.

Contents

1	Introduction
1.1	Overview
1.2	Terms
1.2.1	Common Criteria Terms
1.2.2	Technical Terms
1.3	Compliant Targets of Evaluation
1.3.1	TOE Boundary
1.4	Use Cases
2	Conformance Claims
3	Security Problem Definition
3.1	Threats
3.2	Assumptions
3.3	Organizational Security Policies
4	Security Objectives
4.1	Security Objectives for the Operational Environment
4.2	Security Objectives Rationale
5	Security Requirements
5.1	Security Functional Requirements
5.1.1	Auditable Events for Mandatory SFRs
5.1.2	Security Audit (FAU)
5.1.3	Cryptographic Support (FCS)
5.1.4	User Data Protection (FDP)
5.1.5	Identification and Authentication (FIA)
5.1.6	Security Management (FMT)
5.1.7	Protection of the TSF (FPT)
5.1.8	TOE Access Banner (FTA)
5.1.9	Trusted Path/Channel (FTP)
5.1.10	TOE Security Functional Requirements Rationale
5.2	Security Assurance Requirements
5.2.1	Class ASE: Security Target Evaluation
5.2.2	Class ADV: Development
5.2.3	Class AGD: Guidance Documents
5.2.4	Class ALC: Life-Cycle Support
5.2.5	Class ATE: Tests
5.2.6	Class AVA: Vulnerability Assessment
Appendix A	- Optional Requirements
A.1	Strictly Optional Requirements
A.1.1	Auditable Events for Strictly Optional Requirements
A.1.2	Class ALC: Life-Cycle Support
A.1.3	Security Audit (FAU)
A.1.4	Protection of the TSF (FPT)
A.2	Objective Requirements
A.2.1	Auditable Events for Objective Requirements
A.2.2	Protection of the TSF (FPT)
A.3	Implementation-dependent Requirements
Appendix B	- Selection-based Requirements
B.1	Auditable Events for Selection-based Requirements
B.2	Cryptographic Support (FCS)
B.3	Identification and Authentication (FIA)
B.4	Protection of the TSF (FPT)
B.5	Trusted Path/Channel (FTP)
Appendix C	- Extended Component Definitions
C.1	Extended Components Table
C.2	Extended Component Definitions
C.2.1	Cryptographic Support (FCS)
C.2.1.1	FCS_ENT_EXT Entropy for Virtual Machines
C.2.1.2	FCS_HTTPS_EXT HTTPS Protocol
C.2.1.3	FCS_IPSEC_EXT IPsec Protocol
C.2.2	Identification and Authentication (FIA)
C.2.2.1	FIA_AFL_EXT Authentication Failure Handling
C.2.2.2	FIA_PMG_EXT Password Management
C.2.2.3	FIA_UIA_EXT Administrator Identification and Authentication
C.2.2.4	FIA_X509_EXT X.509 Certificate
C.2.3	Protection of the TSF (FPT)
C.2.3.1	FPT_DDI_EXT Device Driver Isolation

- C.2.3.2 FPT_DVD_EXT Non-Existence of Disconnected Virtual Devices
 - C.2.3.3 FPT_EEM_EXT Execution Environment Mitigations
 - C.2.3.4 FPT_GVI_EXT guest VM Integrity
 - C.2.3.5 FPT_HAS_EXT Hardware Assists
 - C.2.3.6 FPT_HCL_EXT Hypervisor Controls
 - C.2.3.7 FPT_IDV_EXT Software Identification and Versions
 - C.2.3.8 FPT_INT_EXT Support for Introspection
 - C.2.3.9 FPT_ML_EXT Measured Launch of Platform and VMM
 - C.2.3.10 FPT_RDM_EXT Removable Devices and Media
 - C.2.3.11 FPT_TUD_EXT Trusted Updates
 - C.2.3.12 FPT_VDP_EXT Virtual Device Parameters
 - C.2.3.13 FPT_VIV_EXT VMM Isolation from VMs
- C.2.4 Security Management (FMT)
- C.2.4.1 FMT_SMO_EXT Separation of Management and Operational Networks
 - C.2.4.2 FMT_MOF_EXT Management of Security Functions Behavior
- C.2.5 Trusted Path/Channel (FTP)
- C.2.5.1 FTP_ITC_EXT Trusted Channel Communications
 - C.2.5.2 FTP_UIF_EXT User Interface
- C.2.6 User Data Protection (FDP)
- C.2.6.1 FDP_HBI_EXT Hardware-Based Isolation Mechanisms
 - C.2.6.2 FDP_PPR_EXT Physical Platform Resource Controls
 - C.2.6.3 FDP_RIP_EXT Residual Information in Memory
 - C.2.6.4 FDP_VMS_EXT VM Separation
 - C.2.6.5 FDP_VNC_EXT Virtual Networking Components

Appendix D - Implicitly Satisfied Requirements

Appendix E - Entropy Documentation and Assessment

E.1 Design Description

E.2 Entropy Justification

E.3 Operating Conditions

E.4 Health Testing

Appendix F - Equivalency Guidelines

F.1 Introduction

F.2 Approach to Equivalency Analysis

F.3 Specific Guidance for Determining Product Model Equivalence

F.4 Specific Guidance for Determining Product Version Equivalence

F.5 Specific Guidance for Determining Platform Equivalence

F.5.1 Hardware Platform Equivalence

F.5.2 Software Platform Equivalence

F.6 Level of Specificity for Tested and Claimed Equivalent Configurations

Appendix G - Acronyms

Appendix H - Bibliography

1 Introduction

1.1 Overview

The scope of this Protection Profile (PP) is to describe the security functionality of virtualization technologies in terms of [CC] and to define security functional and assurance requirements for such products. This PP includes the requirements formerly specified in the PP-Module for Server Virtualization and the PP-Module for Client Virtualization. These two PP-Modules have been incorporated as use cases in this document.

Due to the increasing prevalence of virtualization technology in enterprise computing environments and the shift to cloud computing, it is essential to ensure that this technology is implemented securely in order to mitigate the risk introduced by sharing multiple computers and their resident data across a single physical system.

1.2 Terms

The following sections list Common Criteria and technology terms used in this document.

1.2.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-PP)	Protection Profile used as a basis to build a PP-Configuration.
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Extended Package (EP)	A deprecated document form for collecting SFRs that implement a particular protocol, technology, or functionality. See Functional Packages.
Functional Package (FP)	A document that collects SFRs for a particular protocol, technology, or functionality.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base-PPs.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of	The product under evaluation.

Evaluation (TOE)

TOE Security Functionality (TSF) The security functionality of the product under evaluation.

TOE Summary Specification (TSS) A description of how a TOE satisfies the SFRs in an ST.

1.2.2 Technical Terms

Administrator	Administrators perform management activities on the VS. These management functions do not include administration of software running within guest VMs, such as the guest OS. Administrators need not be human as in the case of embedded or headless VMs. Administrators are often nothing more than software entities that operate within the VM.
Auditor	Auditors are responsible for managing the audit capabilities of the TOE. An Auditor may also be an administrator. It is not a requirement that the TOE be capable of supporting an Auditor role that is separate from that of an administrator.
Domain	A Domain or Information Domain is a policy construct that groups together execution environments and networks by sensitivity of information and access control policy. For example, classification levels represent information domains. Within classification levels, there might be other domains representing communities of interest or coalitions. In the context of a VS, information domains are generally implemented as collections of VMs connected by virtual networks. The VS itself can be considered an Information Domain, as can its Management Subsystem.
Guest Network	See Operational Network.
Guest Operating System	An operating system that runs within a guest VM.
Helper VM	A Helper VM is a VM that performs services on behalf of one or more guest VMs, but does not qualify as a Service VM—and therefore is not part of the VMM. Helper VMs implement functions or services that are particular to the workloads of guest VMs. For example, a VM that provides a virus scanning service for a guest VM would be considered a Helper VM. For the purposes of this document, Helper VMs are considered a type of guest VM, and are therefore subject to all the same requirements, unless specifically stated otherwise.
Host Operating System	An operating system onto which a VS is installed. Relative to the VS, the Host OS is part of the Platform. There need not be a Host OS, but often VSes employ a Host OS or Control Domain to support guest access to host resources. Sometimes these domains are themselves encapsulated within VMs.
Hypercall	An API function that allows VM-aware software running within a VM to invoke VMM functionality.
Hypervisor	The hypervisor is part of the VMM. It is the software executive of the physical platform of a VS. A hypervisor's primary function is to mediate access to all CPU and memory resources, but it is also responsible for either the direct management or the delegation of the management of all other hardware devices on the hardware platform.
Information Domain	See Domain.
Introspection	A capability that allows a specially designated and privileged domain to have visibility into another domain for purposes of anomaly detection or monitoring.
Management Network	A network, which may have both physical and virtualized components, used to manage and administer a VS. Management networks include networks used by VS administrators to communicate with management components of the VS, and networks used by the VS for communications between VS components. For purposes of this document, networks that connect physical hosts and backend storage networks for purposes of VM transfer or backup are considered management networks.
Management Subsystem	Components of the VS that allow VS administrators to configure and manage the VMM, as well as configure guest VMs. VMM management functions include VM configuration, virtualized network configuration, and allocation of physical resources.
Operational Network	An Operational Network is a network, which may have both physical and virtualized components, used to connect guest VMs to each other and potentially to other entities outside of the VS. Operational Networks support mission workloads and customer-specific client or server functionality. Also called a "Guest Network."
Physical Platform	The hardware environment on which a VS executes. Physical platform resources include processors, memory, devices, and associated firmware.
Platform	The hardware, firmware, and software environment into which a VS is installed and executes.

Service VM	A Service VM is a VM whose purpose is to support the hypervisor in providing the resources or services necessary to support guest VMs. Service VMs may implement some portion of hypervisor functionality, but also may contain important system functionality that is not necessary for hypervisor operation. As with any VM, Service VMs necessarily execute without full hypervisor privileges—only the privileges required to perform its designed functionality. Examples of Service VMs include device driver VMs that manage access to physical devices, VMs that provide life-cycle management and provisioning of hypervisor and guest VMs, and name-service VMs that help establish communication paths between VMs.
System Security Policy (SSP)	The overall policy enforced by the VS defining constraints on the behavior of VMs and users.
User	Users operate guest VMs and are subject to configuration policies applied to the VS by administrators. Users need not be human as in the case of embedded or headless VMs, users are often nothing more than software entities that operate within the VM.
Virtual Machine (VM)	A Virtual Machine is a virtualized hardware environment in which an operating system may execute.
Virtual Machine Manager (VMM)	A VMM is a collection of software components responsible for enabling VMs to function as expected by the software executing within them. Generally, the VMM consists of a hypervisor, Service VMs, and other components of the VS, such as virtual devices, binary translation systems, and physical device drivers. It manages concurrent execution of all VMs and virtualizes platform resources as needed.
Virtualization System (VS)	A software product that enables multiple independent computing systems to execute on the same physical hardware platform without interference from one another. For the purposes of this document, the VS consists of a Virtual Machine Manager (VMM), Virtual Machine abstractions, a management subsystem, and other components.
guest VM	A guest VM is a VM that contains a virtual environment for the execution of an independent computing system. Virtual environments execute mission workloads and implement customer-specific client or server functionality in guest VMs, such as a web server or desktop productivity applications.

1.3 Compliant Targets of Evaluation

A Virtualization System (VS) is a software product that enables multiple independent computing systems to execute on the same physical hardware platform without interference from one another. A VS creates a virtualized hardware environment (virtual machines or VMs) for each instance of an operating system permitting these environments to execute concurrently while maintaining isolation and the appearance of exclusive control over assigned computing resources. For the purposes of this document, the VS consists of a Virtual Machine Manager (VMM), Virtual Machine (VM) abstractions, a management subsystem, and other components.

A VMM is a collection of software components responsible for enabling VMs to function as expected by the software executing within them. Generally, the VMM consists of a hypervisor, Service VMs, and other components of the VS, such as virtual devices, binary translation systems, and physical device drivers. It manages concurrent execution of all VMs and virtualizes platform resources as needed.

The hypervisor is the software executive of the physical platform of a VS. A hypervisor operates at the highest CPU privilege level and manages access to all of the physical resources of the hardware platform. It exports a well-defined, protected interface for access to the resources it manages. A hypervisor's primary function is to mediate access to all CPU and memory resources, but it is also responsible for either the direct management or the delegation of the management of all other hardware devices on the hardware platform. This document does not specify any hypervisor-specific requirements, though many VMM requirements would naturally apply to a hypervisor.

A Service VM is a VM whose purpose is to support the hypervisor in providing the resources or services necessary to support guest VMs. Service VMs may implement some portion of hypervisor functionality, but also may contain important system functionality that is not necessary for hypervisor operation. As with any VM, Service VMs necessarily execute without full hypervisor privileges—only the privileges required to perform its designed functionality. Examples of Service VMs include device driver VMs that manage access to physical devices, VMs that provide life-cycle management and provisioning of hypervisor and guest VMs, and name-service VMs that help establish communication paths between VMs.

A guest VM is a VM that contains a virtual environment for the execution of an independent computing system. Virtual environments execute mission workloads and implement customer-specific client or server functionality in guest VMs, such as a web server or desktop productivity applications. A Helper VM is a VM that performs services on behalf of one or more guest VMs, but does not qualify as a Service VM—and therefore is not part of the VMM. Helper VMs implement functions or services that are particular to the workloads of guest VMs. For example, a VM that provides a virus scanning service for a guest VM would be considered a Helper VM. The line between Helper and Service VMs can easily be blurred. For instance, a VM that implements a cryptographic function—such as an in-line encryption VM—could be identified as either a Service or Helper VM depending on the particular virtualization solution. If the cryptographic functions are necessary only for the privacy of guest VM data in support of the Guest's mission applications, it would be proper to classify the encryption VM as a Helper. But if the encryption VM is necessary for the VMM to isolate guest VMs, it would be proper to classify the encryption VM as a Service VM. For the purposes of this document, Helper VMs are subject to all requirements that apply to guest VMs, unless specifically stated

otherwise.

1.3.1 TOE Boundary

Figure 1 shows a greatly simplified view of a generic virtualization system and platform. TOE components are displayed in Red. Non-TOE components are in Blue. The Platform is the hardware, firmware, and software onto which the VS is installed. The VMM includes the hypervisor, Service VMs, and VM containers, but not the software that runs inside guest VMs or Helper VMs. The Management Subsystem is part of the TOE, but may or may not be part of the VMM.

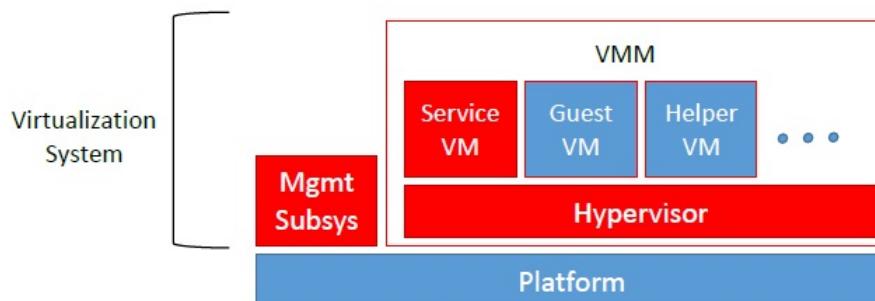


Figure 1: Virtualization System and Platform

For purposes of this Protection Profile, the virtualization system is the TOE, subject to some caveats. The Platform onto which the VS is installed (which includes hardware, platform firmware, and Host Operating System) is not part of the TOE. Software installed with the VS on the Host OS specifically to support the VS or implement VS functionality is part of the TOE. General purpose software—such as device drivers for physical devices and the Host OS itself—is not part of the TOE, regardless of whether it supports VS functionality or runs inside a Service VM or control domain. Software that runs within Guest and Helper VMs is not part of the TOE.

In general, for virtualization products that are installed onto “bare metal,” the entire set of installed components constitute the TOE, and the hardware constitutes the Platform. Also in general, for products that are hosted by or integrated into a commodity operating system, the components installed expressly for implementing and supporting virtualization are in the TOE, and the Platform comprises the hardware and Host OS.

1.4 Use Cases

This Protection Profile supports two use cases: Server Virtualization and Client Virtualization. A product must align with one use case or the other to be evaluated against this PP.

This document does not address virtualization on mobile devices (typically devices that use a baseband processor or connect to a cellular network), nor does it address application virtualization or containers.

[USE CASE 1] Server Virtualization

Server Virtualization, for the purposes of this PP, refers to a virtualization system that implements virtualized hardware components on server-class hardware. It creates a virtualized hardware environment for each instance of an operating system (virtual machines or VMs) permitting these environments to execute concurrently while maintaining isolation and the appearance of exclusive control over assigned computing resources. Each VM instance supports applications such as file servers, web servers, and mail servers. Server virtualization may also support client operating systems in a virtual desktop or thin-client environment. Typically, virtualized servers provide services to remote clients from a data center, and are generally not directly accessible by non-administrative users.

Claiming of the Server Virtualization use case requires that the ST Author:

- Not permit Users to invoke management function [4](#),
- Not permit Users to invoke management function [9](#),
- Require that Administrators be able to invoke management function [10](#), and
- Not permit Users to invoke management function [10](#).

[USE CASE 2] Client Virtualization

Client Virtualization, for the purposes of this PP, refers to a virtualization system that implements virtualized hardware components locally on an endpoint machine. Endpoints are typically client hardware such as desktop or laptop computers that a user interacts with directly, but may also include headless embedded systems without direct human interaction. A virtualization system creates a virtualized hardware environment for each instance of a guest operating system (a virtual machine) permitting these environments to execute concurrently while maintaining isolation and the appearance of exclusive control over assigned computing resources. Client virtualization is generally used on endpoint systems, making use of the local machine's resources (memory, CPU, etc.) to provide isolated user environments.

Claiming of the Client Virtualization use case requires that the ST Author:

- Optionally allow Users to invoke management function [4](#),
- Optionally allow Users to invoke management function [9](#), and
- Optionally allow Administrators and Users to invoke management function [10](#).

2 Conformance Claims

Conformance Statement

An ST must claim exact conformance to this PP.

The evaluation methods used for evaluating the TOE are a combination of the workunits defined in [CEM] as well as the Evaluation Activities for ensuring that individual SFRs and SARs have a sufficient level of supporting evidence in the Security Target and guidance documentation and have been sufficiently tested by the laboratory as part of completing ATE_IND.1. Any functional packages this PP claims similarly contain their own Evaluation Activities that are used in this same manner.

CC Conformance Claims

This PP is conformant to Part 2 (extended) and Part 3 (extended) of Common Criteria CC:2022, Revision 1.

PP Claim

This PP does not claim conformance to any Protection Profile.

There are no PPs or PP-Modules that are allowed in a PP-Configuration with this PP.

Package Claim

- This PP is Functional Package for Secure Shell Version 2.0 conformant.
- This PP is Functional Package for Transport Layer Security Version 2.1 conformant.
- This PP is Functional Package for X.509 Version 1.0 conformant.
- This PP does not conform to any assurance packages.

The functional packages to which the PP conforms may include SFRs that are not mandatory to claim for the sake of conformance. An ST that claims one or more of these functional packages may include any non-mandatory SFRs that are appropriate to claim based on the capabilities of the TSF and on any triggers for their inclusion based inherently on the SFR selections made.

3 Security Problem Definition

3.1 Threats

T.3P_SOFTWARE

Malicious or poorly-coded third-party software or firmware that supports the functionality of the TOE (e.g., device drivers, operating systems) may be used to compromise the VS or its VMs if they have excessive privileges to interact with the TSF (e.g., physical device drivers that are not encapsulated within a VM could expose entities outside of that VM to compromise).

T.DATA_LEAKAGE

A poorly-implemented mechanism for domain separation could allow data to be maliciously or inadvertently transmitted between two VMs that should not be permitted to share information.

T.DENIAL_OF_SERVICE

A maliciously-configured or poorly-implemented VM may block other VMs from accessing system resources (e.g., system memory, persistent storage, and processing time) via a resource exhaustion attack.

T.MISCONFIGURATION

A malicious or inattentive administrator may misconfigure the VS, or faulty configuration data may cause the VS to behave in an unintended manner, which could impact its functioning and security.

T.PLATFORM_COMPROMISE

A malicious user or process may operate a VM in a manner that allows it to compromise the behavior of the system on which the VS runs (e.g., through shared access to system-level resources), leading to either unauthorized modification of the system or the behavior of the VS.

T.UNAUTHORIZED_ACCESS

A malicious user or outside entity may gain access to the TSF or its data, either through poorly implemented access control or through insecure communications, allowing for unintended management actions to be performed against the VS without proper authorization.

T.UNAUTHORIZED_MODIFICATION

A malicious user or administrator could alter the behavior of the VS by having it execute illicitly modified code, whether as an alteration of the VS itself or as code running within a VM, that causes it to behave in an unintended manner.

T.UNAUTHORIZED_UPDATE

A malicious user or process may attempt to illicitly modify the behavior of the VS by applying a software update to it that was modified in a manner that will compromise its behavior.

T.UNPATCHED_SOFTWARE

Vulnerabilities in outdated or unpatched software can be exploited by adversaries to compromise the VS or platform.

T.USER_ERROR

A careless user may inadvertently introduce information to a particular VM that is not intended to receive it because the VMs are identified in an ambiguous manner.

T.VMM_COMPROMISE

A malicious user or process may alter the behavior of the VMM or cause it to fail in a way that eliminates domain separation between multiple VMs that are not intended to be visible to one another.

T.WEAK_CRYPTO

A malicious user or process could force the disclosure of sensitive data at rest or in transit because weak cryptographic algorithms were used to protect this data or because implementation flaws in the generation and use of cryptographic data did not maximize the effective strength of the implementation.

3.2 Assumptions

A.NON_MALICIOUS_USER

The user of the VS is not willfully negligent or hostile, and uses the VS in compliance with the applied enterprise security policy and guidance. At the same time, malicious applications could act as the user, so requirements which confine malicious applications are still in scope.

A.PHYSICAL

Physical security commensurate with the value of the TOE and the data it contains is assumed to be provided by the environment.

A.PLATFORM_INTEGRITY

The platform has not been compromised prior to installation of the VS.

A.TRUSTED_ADMIN

TOE administrators are trusted to follow and apply all administrator guidance.

3.3 Organizational Security Policies

This document does not define any additional OSPs.

4 Security Objectives

4.1 Security Objectives for the Operational Environment

OE.CONFIG

TOE administrators will configure the VS correctly to create the intended security policy.

OE.NON_MALICIOUS_USER

Users are trusted to not be willfully negligent or hostile and use the VS in compliance with the applied enterprise security policy and guidance.

OE.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.TRUSTED_ADMIN

TOE administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.2 Security Objectives Rationale

This section describes how the assumptions and organizational security policies map to operational environment security objectives.

Table 1: Security Objectives Rationale

Assumption or OSP	Security Objectives	Rationale
A.NON_MALICIOUS_USER	OE.NON_MALICIOUS_USER	If the organization properly vets and trains users, it is expected that they will be non-malicious.
	OE.CONFIG	If the TOE is administered by a non-malicious and non-negligent user, the expected result is that the TOE will be configured in a correct and secure manner.
A.PHYSICAL	OE.PHYSICAL	If the TOE is deployed in a location that has appropriate physical safeguards, it can be assumed to be physically secure.
A.PLATFORM_INTEGRITY	OE.PHYSICAL	If the underlying platform has not been compromised prior to installation of the TOE, its integrity can be assumed to be intact.
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN	Providing guidance to administrators and ensuring that individuals are properly trained and vetted before being given administrative responsibilities will ensure that they are trusted.

5 Security Requirements

This chapter describes the security requirements which have to be fulfilled by the product under evaluation. Those requirements comprise functional components from Part 2 and assurance components from Part 3 of [CC]. The following conventions are used for the completion of operations:

- **Refinement** operation (denoted by **bold text** or ~~strikethrough text~~): Is used to add details to a requirement or to remove part of the requirement that is made irrelevant through the completion of another operation, and thus further restricts a requirement.
- **Selection** (denoted by *italicized text*): Is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): Is used to assign a specific value to an unspecified parameter, such as the length of a password. Showing the value in square brackets indicates assignment.
- **Iteration** operation: Is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."

5.1 Security Functional Requirements

5.1.1 Auditable Events for Mandatory SFRs

Table 2: Auditable Events for Mandatory Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	No events specified	N/A
FAU_SAR.1	No events specified	N/A
FAU_STG.1	Failure of audit data capture due to lack of disk space or pre-defined limit. On failure of logging function, capture record of failure and record upon restart of logging function.	No additional information No additional information
FAU_STG.2	No events specified	N/A
FCS_CKM.1	No events specified	N/A
FCS_CKM.2	No events specified	N/A
FCS_CKM.6	No events specified	N/A
FCS_COP.1/Hash	No events specified	N/A
FCS_COP.1/KeyedHash	No events specified	N/A
FCS_COP.1/Sig	No events specified	N/A
FCS_COP.1/UDE	No events specified	N/A
FCS_ENT_EXT.1	No events specified	N/A
FCS_RBG.1	Failure of the randomization process.	No additional information
FDP_HBI_EXT.1	No events specified	N/A
FDP_PPR_EXT.1	Successful and failed VM connections to physical devices where connection is governed by configurable policy. Security policy violations.	VM and physical device identifiers. Identifier for the security policy that was violated.
FDP_RIP_EXT.1	No events specified	N/A
FDP_RIP_EXT.2	No events specified	N/A
FDP_VMS_EXT.1	No events specified	N/A
FDP_VNC_EXT.1	Successful and failed attempts to connect VMs to virtual and physical networking components. Security policy violations.	VM and virtual or physical networking component identifiers. • Identifier for the security policy that was violated. • VM and virtual or physical networking component identifiers.
	Administrator configuration of inter-	VM and virtual or physical networking

	VM communications channels between VMs.	component identifiers.
FIA_AFL_EXT.1	Unsuccessful login attempts limit is met or exceeded.	Origin of attempt (e.g., IP address).
FIA_UAU.5	No events specified	N/A
FIA_UIA_EXT.1	Administrator authentication attempts.	Provided user identity, origin of the attempt (e.g., console, remote IP address).
	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., console, remote IP address).
	[selection, choose one of: Start and end of administrator session., none]	Start time and end time of administrator session.
FMT_MOF_EXT.1	.	<ul style="list-style-type: none"> • Success or failure of attempt • Identity of actor
FMT_SMO_EXT.1	No events specified	N/A
FPT_DVD_EXT.1	No events specified	N/A
FPT_EEM_EXT.1	No events specified	N/A
FPT_FLS.1	Failure of the TSF.	No additional information
FPT_HAS_EXT.1	No events specified	N/A
FPT_HCL_EXT.1	[selection, choose one of: Invalid parameter to hypercall detected., none]	Hypercall interface for which access was attempted
	[selection, choose one of: Hypercall interface invoked when documented preconditions are not met, none]	No additional information
FPT_RDM_EXT.1	Connection/disconnection of removable media or device to/from a VM.	VM Identifier, Removable media/device identifier, event description or identifier (connect/disconnect, ejection/insertion, etc.).
	Ejection/insertion of removable media or device from/to an already connected VM.	VM Identifier, Removable media/device identifier, event description or identifier (connect/disconnect, ejection/insertion, etc.).
FPT_TST.1	Indication that the TSF self-tests were completed and any failures of the tests.	No additional information
	Execution of the TSF self-tests and the results of the tests.	No additional information
FPT_TUD_EXT.1	Initiation of update.	No additional information
	Failure of signature verification.	No additional information
FPT_VDP_EXT.1	No events specified	N/A
FPT_VIV_EXT.1	No events specified	N/A
FTA_TAB.1	No events specified	N/A
FTP_ITC_EXT.1	Initiation of the trusted channel.	User ID and remote source (IP Address) if feasible.
	Termination of the trusted channel.	User ID and remote source (IP Address) if feasible.
	Failures of the trusted path functions.	User ID and remote source (IP Address) if feasible.
FTP_UIF_EXT.1	No events specified	N/A
FTP_UIF_EXT.2	No events specified	N/A

5.1.2 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

The TSF shall be able to generate an audit **data** of the following auditable events:

1. Start-up and shutdown of audit functions
2. [Auditable events defined in [Table 2](#)]
3. [selection:
 - [Auditable events defined in Table 7 for Strictly Optional SFRs](#)
 - [Auditable events defined in Table 8 for Objective SFRs](#)
 - [Auditable events defined in Table 9 for Selection-Based SFRs](#)
 - [Auditable events for the Functional Package for Transport Layer Security \(TLS\), version 2.1 listed in Table 3](#)
 - [Auditable events defined in the audit table for the Functional Package for Secure Shell \(SSH\), version 2.0](#)
 - **no other auditable events**

1

The TSF shall record within each audit **data** at least the following information:

1. Date and time of the event
2. Type of event
3. Subject and object identity (if applicable)
4. The outcome (success or failure) of the event
5. [Additional information defined in [Table 2](#)]
6. [selection:
 - [Additional information defined in Table 7 for Strictly Optional SFRs](#)
 - [Additional information defined in Table 8 for Objective SFRs](#)
 - [Additional information defined in Table 9 for Selection-Based SFRs](#)
 - [Additional information for the Functional Package for Transport Layer Security \(TLS\), version 2.1 listed in Table 3](#)
 - [Additional information defined in the audit table for the Functional Package for Secure Shell \(SSH\), version 2.0](#)
 - **no other information**

1

Application Note: The ST author can include other auditable events directly in [Table 2](#); they are not limited to the list presented. The ST author should update the table in [FAU_GEN.1.2](#) with any additional information generated. “Subject identity” in [FAU_GEN.1.2](#) could be a user id or an identifier specifying a VM, for example.

Appropriate entries from [Table 7](#), [Table 8](#), and [Table 9](#) should be included in the ST if the associated SFRs and selections are included.

The [Table 2](#) entry for [FDP_VNC_EXT.1](#) refers to configuration settings that attach VMs to virtualized network components. Changes to these configurations can be made during VM execution or when VMs are not running. Audit records must be generated for either case.

The intent of the audit requirement for [FDP_PPR_EXT.1](#) is to log that the VM is connected to a physical device (when the device becomes part of the VM's hardware view), not to log every time that the device is accessed. Generally, this is only once at VM startup. However, some devices can be connected and disconnected during operation (e.g., virtual USB devices such as CD-ROMs). All such connection/disconnection events must be logged.

The following table contains the events enumerated in the auditable events table for the [Functional Package for Transport Layer Security \(TLS\), version 2.1](#). Inclusion of these events in the ST is subject to selection above, inclusion of the corresponding SFRs in the ST, and support in the FP as represented by a selection in the table below.

Table 3: Auditable Events for the Functional Package for Transport Layer Security (TLS), version 2.1

FCS_TLSC_EXT.1	Failure to establish a session.	Reason for failure.
FCS_TLSC_EXT.1	Failure to verify presented identifier.	Presented identifier and reference identifier.
FCS_TLSC_EXT.1	Establishment/termination of a TLS session.	Non-TOE endpoint of connection.
FCS_TLSS_EXT.1	Failure to establish a session.	Reason for failure.
FCS_DTLSC_EXT.1	Failure of the certificate validity check.	Issuer Name and Subject Name of certificate.

Evaluation Activities ▼

[FAU_GEN.1.1](#)

TSS

The evaluator shall check the TSS and ensure that it lists all of the auditable events and provides a format for audit records. Each audit record format type shall be covered, along with a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP-Configuration is described in the TSS.

Guidance

The evaluator shall also make a determination of the administrative actions that are relevant in the context of this PP-Configuration. The evaluator shall examine the administrative guide and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are security-relevant with respect to this PP-Configuration.

Tests

The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed and administrative actions. For administrative actions, the evaluator shall test that each action determined by the evaluator above to be security relevant in the context of this PP is auditable. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.

Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.

FAU_SAR.1 Audit Review

FAU_SAR.1.1

The TSF shall provide [administrators] with the capability to read [*all information*] from the audit data.

FAU_SAR.1.2

The TSF shall provide the audit data in a manner suitable for the user to interpret the information.

Evaluation Activities ▼

[FAU_SAR.1.1](#)

TSS

There are no additional TSS evaluation activities for this element.

Guidance

The evaluator shall review the operational guidance for the procedure on how to review the audit records.

Tests

The evaluator shall verify that the audit records provide all of the information specified in FAU_GEN.1 and that this information is suitable for human interpretation. The evaluation activity for this requirement is performed in conjunction with the evaluation activity for FAU_GEN.1.

FAU_STG.1 External Audit Storage

FAU_STG.1.1

The TSF shall be able to store generated audit data on the [transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC].

Evaluation Activities ▼

[FAU_STG.1.1](#)

Protocols used for implementing the trusted channel must be selected in FTP_ITC_EXT.1.

TSS

The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.

Guidance

The evaluator shall examine the operational guidance to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration

of the TOE needed to communicate with the audit server.

Tests

Testing of the trusted channel mechanism is to be performed as specified in the evaluation activities for [FTP_ITC_EXT.1](#).

The evaluator shall perform the following test for this requirement:

- **Test FAU_STG.1.1:1**: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing.

FAU_STG.2 Protected Audit Trail Storage

FAU_STG.2.1

The TSF shall protect the stored audit data in the audit trail from unauthorized deletion.

FAU_STG.2.2

The TSF shall be able to [prevent] unauthorized modifications to the stored audit in the audit trail.

Application Note: The evaluation activity for this SFR is not intended to imply that the TOE must support an administrator's ability to designate individual audit records for deletion. That level of granularity is not required.

Evaluation Activities ▼

FAU_STG.2.1

TSS

The evaluator shall ensure that the TSS describes how the audit records are protected from unauthorized modification or deletion. The evaluator shall ensure that the TSS describes the conditions that must be met for authorized deletion of audit records.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall perform the following tests:

- **Test FAU_STG.2.1.1**: The evaluator shall access the audit trail as an unauthorized administrator and attempt to modify and delete the audit records. The evaluator shall verify that these attempts fail.
- **Test FAU_STG.2.1.2**: The evaluator shall access the audit trail as an authorized administrator and attempt to delete the audit records. The evaluator shall verify that these attempts succeed. The evaluator shall verify that only the records authorized for deletion are deleted.

FAU_STG.5 Prevention of Audit Data Loss

FAU_STG.5.1

The TSF shall [selection: ignore audited events, "prevent audited `` events, except those taken by the authorized user with special rights", overwrite the oldest stored audit records], [assignment: other actions to be taken in case of audit storage failure and conditions for the actions] if the audit data storage is full.

Application Note: An external log server, if available, might be used as alternative storage space in case the local storage space is full. An 'other action' could be defined in this case as 'send the new audit data to an external IT entity'.

Evaluation Activities ▼

FAU_STG.5.1

TSS

The evaluator shall examine the TSS to ensure it describes what happens when the local audit data store is full.

Guidance

The evaluator shall also examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.

Tests

The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behavior defined in the ST for FAU_STG.5

5.1.3 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1

The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [**selection**]:

- RSA schemes using cryptographic key sizes [3072-bit or greater] that meet the following: [FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix B.3]
- ECC schemes using ["NIST curves" P-384,] and [**selection**: P-521, no other curves] that meet the following: [FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix B.4]
- FFC Schemes using Diffie-Hellman group 14 that meet the following: [RFC 3526] and FFC Schemes using safe primes that meet the following: [NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes"]

] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

Application Note: The ST author selects all key generation schemes used for key establishment and device authentication. When key generation is used for key establishment, the schemes in [FCS_CKM.2.1](#) and selected cryptographic protocols shall match the selection. When key generation is used for device authentication, the public key is expected to be associated with an X.509v3 certificate.

If the TOE acts as a receiver in the RSA key establishment scheme, the TOE does not need to implement RSA key generation.

Evaluation Activities ▼

[FCS_CKM.1.1](#)

TSS

The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.

Guidance

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key generation schemes and key sizes for all uses defined in this PP.

Tests

Note: The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.

Key Generation for FIPS PUB 186-5 RSA Schemes

The evaluator shall verify the implementation of RSA Key Generation by the TOE using the Key Generation test. This test verifies the ability of the TSF to correctly produce values for the key components including the public verification exponent e , the private prime factors p and q , the public modulus n and the calculation of the private signature exponent d .

Key Pair generation specifies 5 ways (or methods) to generate the primes p and q . These include:

- Random Primes:
 - Provable primes
 - Probable primes
- Primes with Conditions:
 - Primes p_1, p_2, q_1, q_2, p and q shall all be provable primes
 - Primes p_1, p_2, q_1 , and q_2 shall be provable primes and p and q shall be probable primes
 - Primes p_1, p_2, q_1, q_2, p and q shall all be probable primes

To test the key generation method for the Random Provable primes method and for all the Primes with Conditions methods, the evaluator shall seed the TSF key generation routine with sufficient data to deterministically generate the RSA key pair. This includes the random seeds, the public exponent of the RSA key, and the desired key length. For each key length supported, the evaluator shall have the TSF generate 25 key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation.

Key Generation for Elliptic Curve Cryptography (ECC)

FIPS 186-5 ECC Key Generation Test

For each supported NIST curve (i.e., P-384 and P-521) the evaluator shall require the

implementation under test (IUT) to generate 10 private/public key pairs. The private key shall be generated using an approved random bit generator (RBG). To determine correctness, the evaluator shall submit the generated key pairs to the public key verification (PKV) function of a known good implementation.

FIPS 186-5 Public Key Verification (PKV) Test

For each supported NIST curve (i.e., P-384 and P-521) the evaluator shall generate 10 private/public key pairs using the key generation function of a known good implementation and modify five of the public key values so that they are incorrect, leaving five values unchanged (i.e., correct). The evaluator shall obtain in response a set of 10 PASS/FAIL values.

Key Generation for Finite-Field Cryptography (FFC)

The evaluator shall verify the implementation of the Parameters Generation and the Key Generation for FFC by the TOE using the Parameter Generation and Key Generation test. This test verifies the ability of the TSF to correctly produce values for the field prime p , the cryptographic prime q (dividing $p-1$), the cryptographic group generator g , and the calculation of the private key x and public key y .

The Parameter generation specifies two ways (or methods) to generate the cryptographic prime q and the field prime p :

- Primes q and p shall both be provable primes
- Primes q and field prime p shall both be probable primes

and two ways to generate the cryptographic group generator g :

- Generator g constructed through a verifiable process
- Generator g constructed through an unverifiable process.

The Key generation specifies two ways to generate the private key x :

- $\text{len}(q)$ bit output of RBG where $1 \leq x \leq q-1$
- $\text{len}(q) + 64$ bit output of RBG, followed by a mod $q-1$ operation where $1 \leq x \leq q-1$

The security strength of the RBG shall be at least that of the security offered by the FFC parameter set.

To test the cryptographic and field prime generation method for the provable primes method and the group generator g for a verifiable process, the evaluator shall seed the TSF parameter generation routine with sufficient data to deterministically generate the parameter set.

For each key length supported, the evaluator shall have the TSF generate 25 parameter sets and key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation. Verification shall also confirm

- $g \neq 0, 1$
- q divides $p-1$
- $g^q \bmod p = 1$
- $g^x \bmod p = y$

for each FFC parameter set and key pair.

Diffie-Hellman Group 14 and FFC Schemes using "safe-prime" groups

Testing for FFC Schemes using Diffie-Hellman group 14 and "safe-prime" groups is done as part of testing in [FCS_CKM.2.1](#).

FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2.1

The TSF shall distribute cryptographic keys implement functionality to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [selection:

- RSA-based key establishment schemes that meets the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2"
- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"
- Finite field-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"
- Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526

] that meets the following [assignment: list of standards].

Evaluation Activities ▼

[FCS_CKM.2.1](#)

TSS

The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in [FCS_CKM.1.1](#). If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.

Guidance

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment schemes.

Tests

The evaluator shall verify the implementation of the key establishment schemes of the supported by the TOE using the applicable tests below.

Key Establishment Schemes

RSAES-PKCS1-v1_5 Key Establishment Schemes

The evaluator shall verify the correctness of the TSF's implementation of RSAES-PKCS1-v1_5 by using a known good implementation for each protocol selected in [FTP_ITC_EXT.1](#) that uses RSAES-PKCS1-v1_5.

SP800-56A ECC Key Establishment Schemes

The evaluator shall verify a TOE's implementation of SP800-56A key agreement schemes using the following Function and Validity tests. These validation tests for each key agreement scheme verify that a TOE has implemented the components of the key agreement scheme according to the specifications in the Recommendation. These components include the calculation of the DLC primitives (the shared secret value Z) and the calculation of the derived keying material (DKM) via the Key Derivation Function (KDF). If key confirmation is supported, the evaluator shall also verify that the components of key confirmation have been implemented correctly, using the test procedures described below. This includes the parsing of the DKM, the generation of MACdata and the calculation of MACtag.

Function Test

The Function test verifies the ability of the TOE to implement the key agreement schemes correctly. To conduct this test, the evaluator shall generate or obtain test vectors from a known good implementation of the TOE supported schemes. For each supported key agreement scheme-key agreement role combination, KDF type, and, if supported, key confirmation role- key confirmation type combination, the tester shall generate 10 sets of test vectors. The data set consists of one set of domain parameter values (FFC) or the NIST approved curve (ECC) per 10 sets of public keys. These keys are static, ephemeral, or both depending on the scheme being tested.

The evaluator shall obtain the DKM, the corresponding TOE's public keys (static and ephemeral), the MAC tags, and any inputs used in the KDF, such as the Other Information field OI and TOE ID fields.

If the TOE does not use a KDF defined in SP 800-56A, the evaluator shall obtain only the public keys and the hashed value of the shared secret.

The evaluator shall verify the correctness of the TSF's implementation of a given scheme by using a known good implementation to calculate the shared secret value, derive the keying material DKM, and compare hashes or MAC tags generated from these values.

If key confirmation is supported, the TSF shall perform the above for each implemented approved MAC algorithm.

Validity Test

The Validity test verifies the ability of the TOE to recognize another party's valid and invalid key agreement results with or without key confirmation. To conduct this test, the evaluator shall obtain a list of the supporting cryptographic functions included in the SP800-56A key agreement implementation to determine which errors the TOE should be able to recognize. The evaluator generates a set of 24 (FFC) or 30 (ECC) test vectors consisting of data sets including domain parameter values or NIST approved curves, the evaluator's public keys, the TOE's public/private key pairs, MACTag, and any inputs used in the KDF, such as the other info and TOE ID fields.

The evaluator shall inject an error in some of the test vectors to test that the TOE recognizes invalid key agreement results caused by the following fields being incorrect: the shared secret value Z, the DKM, the other information field OI, the data to be MACed, or the generated MACTag. If the TOE contains the full or partial (only ECC) public key validation, the evaluator will also individually inject errors in both parties' static public keys, both parties' ephemeral public keys and the TOE's static private key to assure the TOE detects errors in the public key validation function and the partial key validation function (in ECC only). At least two of the test vectors shall remain unmodified and therefore should result in valid key agreement results (they should pass).

The TOE shall use these modified test vectors to emulate the key agreement scheme using the corresponding parameters. The evaluator shall compare the TOE's results with the results using a known good implementation verifying that the TOE detects these errors.

Diffie-Hellman Group 14

The evaluator shall verify the correctness of the TSF's implementation of Diffie-Hellman group 14 by using a known good implementation for each protocol selected in [FTP_ITC_EXT.1](#) that uses Diffie-Hellman Group 14.

FFC Schemes using "safe-prime" groups (identified in Appendix D of SP 800-56A Revision 3)

The evaluator shall verify the correctness of the TSF's implementation of "safe-prime" groups by using a known good implementation for each protocol selected in [FTP_ITC_EXT.1](#) that uses "safe-prime" groups. This test must be performed for each "safe-prime" group that each protocol uses.

FCS_CKM.6 Cryptographic Key Destruction

FCS_CKM.6.1

The TSF shall destroy [**assignment**: *list of cryptographic keys (including keying material)*] when [**selection**: *no longer needed, [assignment]: other circumstances for key or keying material destruction*]

Application Note: The threat addressed by this element is the recovery of disused cryptographic keys from volatile memory by unauthorized processes. The TSF must destroy or cause to be destroyed all copies of cryptographic keys created and managed by the TOE once the keys are no longer needed. This requirement is the same for all instances of keys within TOE volatile memory regardless of whether the memory is controlled by TOE manufacturer software or by third-party TOE modules. The evaluation activities are designed with flexibility to address cases where the TOE manufacturer has limited insight into the behavior of third-party TOE components.

The preferred method for destroying keys in TOE volatile memory is by direct overwrite of the memory occupied by the keys. The values used for overwriting can be all zeros, all ones, or any other pattern or combination of values significantly different than the value of the key itself such that the keys are rendered inaccessible to running processes.

Some implementations may find that direct overwriting of memory is not feasible or possible due to programming language constraints. Many memory- and type-safe languages provide no mechanism for programmers to specify that a particular memory location be accessed or written. The value of such languages is that it is much harder for a programming error to result in a buffer or heap overflow. The downside is that multiple copies of keys might be scattered throughout language-runtime memory. In such cases, the TOE should take whatever actions are feasible to cause the keys to become inaccessible—freeing memory, destroying objects, closing applications, programming using the minimum possible scope for variables containing keys.

Likewise, if keys reside in memory within the execution context of a third-party module, then the TOE should take whatever feasible actions it can to cause the keys to be destroyed.

Cryptographic keys in non-TOE volatile memory are not covered by this requirement. This expressly includes keys created and used by guest VMs. The Guest is responsible for disposing of such keys.

FCS_CKM.6.2

The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [**assignment**: *cryptographic key destruction method*] that meets the following: [**assignment**: *list of standards*].

Application Note: The ultimate goal of this element is to ensure that disused cryptographic keys are inaccessible not only to components of the running system, but are also unrecoverable through forensic analysis of discarded storage media. The element is designed to reflect the fact that the latter may not be wholly practical at this time due to the way some storage technologies are implemented (e.g., wear-leveling of flash storage). Key storage areas in non-volatile storage can be overwritten with any value that renders the keys unrecoverable. The value used can be all zeros, all ones, or any other pattern or combination of values significantly different than the value of the key itself.

The TSF must destroy all copies of cryptographic keys created and managed by the TOE once the keys are no longer needed. Since this is a software-only TOE, the hardware controllers that manage non-volatile storage media are necessarily outside the TOE boundary. Thus, the TOE manufacturer is likely to have little control over—or insight into—the functioning of these storage devices. The TOE must make a “best-effort” to destroy disused cryptographic keys by invoking the appropriate platform interfaces—recognizing that the specific actions taken by the platform are out of the TOE’s control.

But in cases where the TOE has insight into the non-volatile storage technologies used by the platform, or where the TOE can specify a preference or method for destroying keys, the destruction should be executed by a single, direct overwrite consisting of pseudorandom data or a new key, by a repeating pattern of any static value, or by a block erase.

For keys stored on encrypted media, it is sufficient for the media encryption keys to be destroyed for all keys stored on the media to be considered destroyed.

Evaluation Activities ▼

FCS_CKM.6.1

TSS

The evaluator shall check to ensure the TSS lists each type of key and its origin and location in memory or storage. The evaluator shall verify that the TSS describes when each type of key is cleared.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

For each key clearing situation the evaluator shall perform one of the following activities:

- *The evaluator shall use appropriate combinations of specialized operational or development environments, development tools (debuggers, emulators, simulators, etc.), or instrumented builds (developmental, debug, or release) to demonstrate that keys are cleared correctly, including all intermediate copies of the key that may have been created internally by the TOE during normal cryptographic processing.*
- *In cases where testing reveals that third-party software modules or programming language run-time environments do not properly overwrite keys, this fact must be documented. Likewise, it must be documented if there is no practical way to determine whether such modules or environments destroy keys properly.*
- *In cases where it is impossible or impracticable to perform the above tests, the evaluator shall describe how keys are destroyed in such cases, to include:*
 - *Which keys are affected*
 - *The reasons why testing is impossible or impracticable*
 - *Evidence that keys are destroyed appropriately (e.g., citations to component documentation, component developer/vendor attestation, component vendor test results)*
 - *Aggravating and mitigating factors that may affect the timeliness or execution of key destruction (e.g., caching, garbage collection, operating system memory management)*

Use of debug or instrumented builds of the TOE and TOE components is permitted in order to demonstrate that the TOE takes appropriate action to destroy keys. These builds should be based on the same source code as are release builds (of course, with instrumentation and debug-specific code added).

FCS_COP.1/Hash Cryptographic Operation (Hashing)

FCS_COP.1.1/Hash

The TSF shall perform [cryptographic hashing] in accordance with a specified cryptographic algorithm [**selection**: SHA-384, SHA-512, SHA-3-256, SHA-3-384, SHA-3-512] and **message** key sizes [**selection**: 160, 256, 384, 512 bits] that meet the following: [**selection**: FIPS PUB 180-4 "Secure Hash Standard", ISO/IEC 10118-3:2018]

Application Note: Per NIST SP 800-131A, SHA-1 for generating digital signatures is no longer allowed, and SHA-1 for verification of digital signatures is strongly discouraged as there may be risk in accepting these signatures. It is expected that vendors will implement SHA-2 algorithms in accordance with SP 800-131A.

The intent of this requirement is to specify the hashing function. The hash selection shall support the message digest size selection. The hash selection should be consistent with the overall strength of the algorithm used (for example, SHA 256 for 128-bit keys).

Evaluation Activities ▼

FCS_COP.1.1/Hash

TSS

The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

Guidance

The evaluator checks the AGD documents to determine that any configuration that is required to be done to configure the functionality for the required hash sizes is present.

Tests

SHA-1 and SHA-2 Tests The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented test MACs.

The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP.

The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.

Short Messages Test Bit-oriented Mode

The evaluators devise an input set consisting of $m+1$ messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Short Messages Test Byte-oriented Mode

The evaluators devise an input set consisting of $m/8+1$ messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to $m/8$ bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages Test Bit-oriented Mode

The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm. The length of the i th message is $512 + 99*i$, where $1 \leq i \leq m$. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages Test Byte-oriented Mode

The evaluators devise an input set consisting of $m/8$ messages, where m is the block length of the hash algorithm. The length of the i th message is $512 + 8*99*i$, where $1 \leq i \leq m/8$. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Pseudorandomly Generated Messages Test

This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of [SHAVS]. The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.

SHA-3 Tests The tests below are derived from the The Secure Hash Algorithm-3 Validation System (SHA3VS), Updated: April 7, 2016, from the National Institute of Standards and Technology.

For each SHA-3-XXX implementation, XXX represents d , the digest length in bits. The capacity, c , is equal to $2d$ bits. The rate is equal to $1600-c$ bits.

The TSF hashing functions can be implemented with one of two orientations. The first is a bit-oriented mode that hashes messages of arbitrary length. The second is a byte-oriented mode that hashes messages that are an integral number of bytes in length (i.e., the length (in bits) of the message to be hashed is divisible by 8). Separate tests for each orientation are given below.

The evaluator shall perform all of the following tests for each hash algorithm and orientation implemented by the TSF and used to satisfy the requirements of this PP. The evaluator shall compare digest values produced by a known-good SHA-3 implementation against those generated by running the same values through the TSF.

Short Messages Test, Bit-oriented Mode

The evaluators devise an input set consisting of $rate+1$ short messages. The length of the messages ranges sequentially from 0 to $rate$ bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. The message of length 0 is omitted if the TOE does not support zero-length messages.

Short Messages Test, Byte-oriented Mode

> The evaluators devise an input set consisting of $rate/8+1$ short messages. The length of the messages ranges sequentially from 0 to $rate/8$ bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. The message of length 0 is omitted if the TOE does not support zero-length messages.

Selected Long Messages Test, Bit-oriented Mode

The evaluators devise an input set consisting of 100 long messages ranging in size from $rate+(rate+1)$ to $rate+(100*(rate+1))$, incrementing by $rate+1$. (For example, SHA-3-256 has a rate of 1088 bits. Therefore, 100 messages will be generated with lengths 2177, 3266, ..., 109988 bits.) The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Selected Long Messages Test, Byte-oriented Mode

The evaluators devise an input set consisting of 100 messages ranging in size from $(rate+(rate+8))$ to $(rate+100*(rate+8))$, incrementing by $rate+8$. (For example, SHA-3-256 has a rate of 1088 bits. Therefore 100 messages will be generated of lengths 2184, 3280, 4376, ..., 110688 bits.) The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF.

Pseudorandomly Generated Messages Monte Carlo) Test, Byte-oriented Mode

The evaluators supply a seed of d bits (where d is the length of the message digest produced by the hash function to be tested. This seed is used by a pseudorandom function to generate 100,000 message digests. One hundred of the digests (every 1000th digest) are recorded as checkpoints. The TOE then uses the same procedure to generate the same 100,000 message digests and 100 checkpoint values. The evaluators then compare the results generated to ensure that the correct result is produced when the messages are generated by the TSF.

FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithms)

FCS_COP.1.1/KeyedHash

The TSF shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm [**selection**: HMAC-SHA-384, HMAC-SHA-512, SHA-3-384, SHA-3-512] and cryptographic key sizes [**assignment**: key size (in bits) used in HMAC] and **message digest sizes** [**selection**: **384 bits, 512 bits**] that meet the following: [FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code," and FIPS Pub 180-4, "Secure Hash Standard"].

Application Note: The selection in this requirement must be consistent with the key size specified for the size of the keys used in conjunction with the keyed-hash message authentication.

Evaluation Activities ▼

FCS_COP.1.1/KeyedHash

TSS

The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.

For each of the supported parameter sets, the evaluator shall compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator shall have the TSF generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating HMAC tags with the same key and IV using a known good implementation.

FCS_COP.1/Sig Cryptographic Operation (Signature Algorithms)

FCS_COP.1.1/Sig

The TSF shall perform [*cryptographic signature services (generation and verification)*] in accordance with a specified cryptographic algorithm [**selection**:

- RSA schemes using cryptographic key sizes [3072-bit or greater] that meet the following: [FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 4]
- ECDSA schemes using cryptographic key sizes [P-384 and [**selection**: P-521, no other curves]] that meet the following: [FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5]

].

Application Note: The ST author should choose the algorithm implemented to perform digital signatures; if more than one algorithm is available, this requirement should be iterated to specify the functionality. For the algorithm chosen, the ST author should make the appropriate assignments/selections to specify the parameters that are implemented for that algorithm.

Evaluation Activities ▼

FCS_COP.1.1/Sig

TSS

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.

ECDSA Algorithm Tests

ECDSA FIPS 186-5 Signature Generation Test
For each supported NIST curve (i.e., P-384 and P-521) and SHA function pair, the evaluator shall generate 10 1024-bit long messages and obtain for each message a public key and the resulting signature values R and S. To determine correctness, the evaluator shall use the signature verification function of a known good implementation.

ECDSA FIPS 186-5 Signature Verification Test

For each supported NIST curve (i.e., P-384 and P-521) and SHA function pair, the evaluator shall generate a set of 10 1024-bit message, public key and signature tuples and modify one of the values (message, public key or signature) in five of the 10 tuples. The evaluator shall obtain in response a set of 10 PASS/FAIL values.

RSA Signature Algorithm Tests

Signature Generation Test

The evaluator shall verify the implementation of RSA Signature Generation by the TOE using the Signature Generation Test. To conduct this test, the evaluator shall generate or obtain 10 messages from a trusted reference implementation for each modulus size/SHA combination supported by the TSF. The evaluator shall have the TOE use their private key and modulus value to sign these messages.

The evaluator shall verify the correctness of the TSF's signature using a known good implementation and the associated public keys to verify the signatures.

Signature Verification Test

The evaluator shall perform the Signature Verification test to verify the ability of the TOE to recognize another party's valid and invalid signatures. The evaluator shall inject errors into the test vectors produced during the Signature Verification Test by introducing errors in some of the public keys e , messages, IR format, or signatures. The TOE attempts to verify the signatures and returns success or failure.

The evaluator shall use these test vectors to emulate the signature verification test using the corresponding parameters and verify that the TOE detects these errors.

FCS_COP.1/UDE Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1/UDE

The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [**selection**]:

- AES Key Wrap (KW) (as defined in NIST SP 800-38F)
- AES Key Wrap with Padding (KWP) (as defined in NIST SP 800-38F)
- AES-GCM (as defined in NIST SP 800-38D)
- AES-CCM (as defined in NIST SP 800-38C)
- AES-XTS (as defined in NIST SP 800-38E) mode
- AES-CCMP-256 (as defined in NIST SP800-38C and IEEE 802.11ac-2013)
- AES-GCMP-256 (as defined in NIST SP800-38D and IEEE 802.11ac-2013)
- AES-CCMP (as defined in FIPS PUB 197, NIST SP 800-38C and IEEE 802.11-2012)
- AES-CBC (as defined in FIPS PUB 197, and NIST SP 800-38A) mode
- AES-CTR (as defined in NIST SP 800-38A) mode

] and cryptographic key sizes [384-bit key sizes]. that meet the following [**assignment**: list of standards]

Application Note: For the first selection of FCS_COP.1.1/UDE, the ST author should choose the mode or modes in which AES operates. For the second selection, the ST author should choose the key sizes that are supported by this functionality.

Evaluation Activities ▼

FCS_COP.1.1/UDE

TSS

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products.

AES-CBC Tests

AES-CBC Known Answer Tests

There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

KAT-1. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 plaintext values and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros key, and the other five shall be encrypted with a 256-bit all-zeros key.

To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using 10 ciphertext values as input and AES-CBC decryption.

KAT-2. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 key values and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys.

To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using an all-zero ciphertext value as input and AES-CBC decryption.

KAT-3. To test the encrypt functionality of AES-CBC, the evaluator shall supply the two sets of key values described below and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using the given key value and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the second set shall have 256 256-bit keys. Key i in each set shall have the leftmost i bits be ones and the rightmost $N-i$ bits be zeros, for i in $[1,N]$.

To test the decrypt functionality of AES-CBC, the evaluator shall supply the two sets of key and ciphertext value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit key/ciphertext pairs. Key i in each set shall have the leftmost i bits be ones and the rightmost $N-i$ bits be zeros, for i in $[1,N]$. The ciphertext value in each pair shall be the value that results in an all-zeros plaintext when decrypted with its corresponding key.

KAT-4. To test the encrypt functionality of AES-CBC, the evaluator shall supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from AES-CBC encryption of the given plaintext using a 128-bit key value of all zeros with an IV of all zeros and using a 256-bit key value of all zeros with an IV of all zeros, respectively. Plaintext value i in each set shall have the leftmost i bits be ones and the rightmost $128-i$ bits be zeros, for i in $[1,128]$.

To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC decryption.

AES-CBC Multi-Block Message Test

The evaluator shall test the encrypt functionality by encrypting an i -block message where $1 < i \leq 10$. The evaluator shall choose a key, an IV and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key and IV. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation.

The evaluator shall also test the decrypt functionality for each mode by decrypting an i -block message where $1 < i \leq 10$. The evaluator shall choose a key, an IV and a ciphertext message of length i blocks and decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key and IV using a known good implementation.

AES-CBC Monte Carlo Tests

The evaluator shall test the encrypt functionality using a set of 200 plaintext, IV, and key 3-tuples. 100 of these shall use 128 bit keys, and 100 shall use 256 bit keys. The plaintext and IV values shall be 128-bit blocks. For each 3-tuple, 1000 iterations shall be run as follows:

```
# Input: PT, IV, Key
for i = 1 to 1000:
    if i == 1:
        CT[1] = AES-CBC-Encrypt(Key, IV, PT)
        PT = IV
    else:
        CT[i] = AES-CBC-Encrypt(Key, PT)
        PT = CT[i-1]
```

The ciphertext computed in the 1000th iteration (i.e., $CT[1000]$) is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.

The evaluator shall test the decrypt functionality using the same test as for encrypt, exchanging CT and PT and replacing AES-CBC-Encrypt with AES-CBC-Decrypt.

AES-CCM Tests

The evaluator shall test the generation-encryption and decryption-verification functionality of AES-CCM for the following input parameter and tag lengths:

128 bit and 256 bit keys

Two payload lengths. One payload length shall be the shortest supported payload length, greater than or equal to zero bytes. The other payload length shall be the longest supported payload length, less than or equal to 32 bytes (256 bits).

Two or three associated data lengths. One associated data length shall be 0, if supported. One associated data length shall be the shortest supported payload length, greater than or equal to zero bytes. One associated data length shall be the longest supported payload length, less than or equal to 32 bytes (256 bits). If the implementation supports an associated data length of 2^{16} bytes, an associated data length of 2^{16} bytes shall be tested.

Nonce lengths. All supported nonce lengths between 7 and 13 bytes, inclusive, shall be tested.

Tag lengths. All supported tag lengths of 4, 6, 8, 10, 12, 14 and 16 bytes shall be tested.

To test the generation-encryption functionality of AES-CCM, the evaluator shall perform the following four tests:

To determine correctness in each of the above tests, the evaluator shall compare the ciphertext with the result of generation-encryption of the same inputs with a known good implementation.

To test the decryption-verification functionality of AES-CCM, for EACH combination of supported

associated data length, payload length, nonce length and tag length, the evaluator shall supply a key value and 15 nonce, associated data and ciphertext 3-tuples and obtain either a FAIL result or a PASS result with the decrypted payload. The evaluator shall supply 10 tuples that should FAIL and 5 that should PASS per set of 15.

Additionally, the evaluator shall use tests from the IEEE 802.11-02/362r6 document "Proposed Test vectors for IEEE 802.11 TGi", dated September 10, 2002, Section 2.1 AES-CCMP Encapsulation Example and Section 2.2 Additional AES CCMP Test Vectors to further verify the IEEE 802.11-2007 implementation of AES-CCMP.

AES-GCM Test

The evaluator shall test the authenticated encrypt functionality of AES-GCM for each combination of the following input parameter lengths:

128 bit and 256 bit keys

Two plaintext lengths. One of the plaintext lengths shall be a non-zero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported.

Three AAD lengths. One AAD length shall be 0, if supported. One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported.

Two IV lengths. If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested.

The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known.

The evaluator shall test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail.

The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

XTS-AES Test

The evaluator shall test the encrypt functionality of XTS-AES for each combination of the following input parameter lengths:

- 256 bit (for AES-128) and 512 bit (for AES-256) keys
- **Three data unit (i.e., plaintext) lengths.** One of the data unit lengths shall be a non-zero integer multiple of 128 bits, if supported. One of the data unit lengths shall be an integer multiple of 128 bits, if supported. The third data unit length shall be either the longest supported data unit length or 2^{16} bits, whichever is smaller.

using a set of 100 (key, plaintext and 128-bit random tweak value) 3-tuples and obtain the ciphertext that results from XTS-AES encrypt.

The evaluator may supply a data unit sequence number instead of the tweak value if the implementation supports it. The data unit sequence number is a base-10 number ranging between 0 and 255 that implementations convert to a tweak value internally.

The evaluator shall test the decrypt functionality of XTS-AES using the same test as for encrypt, replacing plaintext values with ciphertext values and XTS-AES encrypt with XTS-AES decrypt.

AES Key Wrap (AES-KW) and Key Wrap with Padding (AES-KWP) Test

The evaluator shall test the authenticated encryption functionality of AES-KW for EACH combination of the following input parameter lengths:

- 128 and 256 bit key encryption keys (KEKs)
- **Three plaintext lengths.** One of the plaintext lengths shall be two semi-blocks (128 bits). One of the plaintext lengths shall be three semi-blocks (192 bits). The third data unit length shall be the longest supported plaintext length less than or equal to 64 semi-blocks (4096 bits).

using a set of 100 key and plaintext pairs and obtain the ciphertext that results from AES-KW authenticated encryption. To determine correctness, the evaluator shall use the AES-KW authenticated-encryption function of a known good implementation.

The evaluator shall test the authenticated-decryption functionality of AES-KW using the same test as for authenticated-encryption, replacing plaintext values with ciphertext values and AES-KW authenticated-encryption with AES-KW authenticated-decryption.

The evaluator shall test the authenticated-encryption functionality of AES-KWP using the same test as for AES-KW authenticated-encryption with the following change in the three plaintext lengths:

One plaintext length shall be one octet. One plaintext length shall be 20 octets (160 bits).

One plaintext length shall be the longest supported plaintext length less than or equal to 512 octets (4096 bits).

The evaluator shall test the authenticated-decryption functionality of AES-KWP using the same test as for AES-KWP authenticated-encryption, replacing plaintext values with ciphertext values

and AES-KWP authenticated-encryption with AES-KWP authenticated-decryption.

AES-CTR Test If "invoke platform-provided" is selected, the evaluator confirms that SSH connections are only successful if appropriate algorithms and appropriate key sizes are configured. To do this, the evaluator shall perform the following tests:

- Test FCS_COP.1.1/UDE:1: For EACH supported key and associated data length and ANY supported payload, nonce and tag length, the evaluator shall supply one key value, one nonce value and 10 pairs of associated data and payload values and obtain the resulting ciphertext.
- Test FCS_COP.1.1/UDE:2: For EACH supported key and payload length and ANY supported associated data, nonce and tag length, the evaluator shall supply one key value, one nonce value and 10 pairs of associated data and payload values and obtain the resulting ciphertext.
- Test FCS_COP.1.1/UDE:3: For EACH supported key and nonce length and ANY supported associated data, payload and tag length, the evaluator shall supply one key value and 10 associated data, payload and nonce value 3-tuples and obtain the resulting ciphertext.
- Test FCS_COP.1.1/UDE:4: For EACH supported key and tag length and ANY supported associated data, payload and nonce length, the evaluator shall supply one key value, one nonce value and 10 pairs of associated data and payload values and obtain the resulting ciphertext.
- Test FCS_COP.1.1/UDE:5: Known Answer Tests (KATs)

There are four Known Answer Tests (KATs) described below. For all KATs, the plaintext, initialization vector (IV), and ciphertext values shall be 128-bit blocks. The results from each test may either be obtained by the validator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

Test 1a: To test the encrypt functionality, the evaluator shall supply a set of 10 plaintext values and obtain the ciphertext value that results from encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all zeros key, and the other five shall be encrypted with a 256-bit all zeros key. To test the decrypt functionality, the evaluator shall perform the same test as for encrypt, using 10 ciphertext values as input.

Test 1b: To test the encrypt functionality, the evaluator shall supply a set of 10 key values and obtain the ciphertext value that results from encryption of an all zeros plaintext using the given key value and an IV of all zeros. Five of the key values shall be 128-bit keys, and the other five shall be 256-bit keys. To test the decrypt functionality, the evaluator shall perform the same test as for encrypt, using an all zero ciphertext value as input.

Test 1c: To test the encrypt functionality, the evaluator shall supply the two sets of key values described below and obtain the ciphertext values that result from AES encryption of an all zeros plaintext using the given key values and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the second shall have 256 256-bit keys. Key_i in each set shall have the leftmost *i* bits be ones and the rightmost *N-i* bits be zeros, for *i* in [1, *N*]. To test the decrypt functionality, the evaluator shall supply the two sets of key and ciphertext value pairs described below and obtain the plaintext value that results from decryption of the given ciphertext using the given key values and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit pairs. Key_i in each set shall have the leftmost *i* bits be ones and the rightmost *N-i* bits be zeros for *i* in [1, *N*]. The ciphertext value in each pair shall be the value that results in an all zeros plaintext when decrypted with its corresponding key.

Test 1d: To test the encrypt functionality, the evaluator shall supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from encryption of the given plaintext using a 128-bit key value of all zeros and using a 256 bit key value of all zeros, respectively, and an IV of all zeros. Plaintext value *i* in each set shall have the leftmost bits be ones and the rightmost 128-*i* bits be zeros, for *i* in [1, 128]. To test the decrypt functionality, the evaluator shall perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input.

- Test FCS_COP.1.1/UDE:6: Multi-Block Message Test

The evaluator shall test the encrypt functionality by encrypting an *i*-block message where 1 less-than *i* less-than-or-equal to 10. For each *i* the evaluator shall choose a key, IV, and plaintext message of length *i* blocks and encrypt the message, using the mode to be tested, with the chosen key. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation. The evaluator shall also test the decrypt functionality by decrypting an *i*-block message where 1 less-than *i* less-than-or-equal to 10. For each *i* the evaluator shall choose a key and a ciphertext message of length *i* blocks and decrypt the message, using the mode to be tested, with the chosen key. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key using a known good implementation.

- Test FCS_COP.1.1/UDE:7: Monte-Carlo Test

For AES-CTR mode perform the Monte Carlo Test for ECB Mode on the encryption engine of the counter mode implementation. There is no need to test the decryption engine.

The evaluator shall test the encrypt functionality using 200 plaintext/key pairs. 100 of these shall use 128 bit keys, and 100 of these shall use 256 bit keys. The plaintext values shall be 128-bit blocks. For each pair, 1000 iterations shall be run as follows:

For AES-ECB mode

Input: PT, Key

for i = 1 to 1000:

CT[i] = AES-ECB-Encrypt(Key, PT)

PT = CT[i]

The ciphertext computed in the 1000th iteration is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.

- Test FCS_COP.1.1/UDE:8: [Conditional: TOE is an SSH server] The evaluator shall configure an SSH client to connect with an invalid cryptographic algorithm and key size for each listening SSH socket connection on the TOE. The evaluator initiates SSH client connections to each listening SSH socket connection on the TOE and observes that the connection fails in each attempt.
- Test FCS_COP.1.1/UDE:9: [Conditional: TOE is an SSH client] The evaluator shall configure a listening SSH socket on a remote SSH server that accepts only invalid cryptographic algorithms and keys. The evaluator uses the TOE to attempt an SSH connection to this server and observes that the connection fails.

FCS_ENT_EXT.1 Entropy for Virtual Machines

FCS_ENT_EXT.1.1

The TSF shall provide a mechanism to make available to VMs entropy that meets FCS_RBG.1 through [selection: hypercall interface, virtual device interface, pass-through access to hardware entropy source].

FCS_ENT_EXT.1.2

The TSF shall provide independent entropy across multiple VMs.

Application Note: This requirement ensures that sufficient entropy is available to any VM that requires it. The entropy need not provide high-quality entropy for every possible method that a VM might acquire it. The VMM must, however, provide some means for VMs to get sufficient entropy. For example, the VMM can provide an interface that returns entropy to a guest VM. Alternatively, the VMM could provide pass-through access to entropy sources provided by the host platform.

This requirement allows for three general ways of providing entropy to guests: 1) The VS can provide a hypercall accessible to VM-aware guests, 2) access to a virtualized device that provides entropy, or 3) pass-through access to a hardware entropy source (including a source of random numbers). In all cases, it is possible that the guest is made VM-aware through installation of software or drivers. For the second and third cases, it is possible that the guest could be VM-unaware. There is no requirement that the TOE provide entropy sources as expected by VM-unaware guests. That is, the TOE does not have to anticipate every way a guest might try to acquire entropy as long as it supplies a mechanism that can be used by VM-aware guests, or provides access to a standard mechanism that a VM-unaware guest would use.

The ST author should select “hypercall interface” if the TSF provides an API function through which guest-resident software can obtain entropy or random numbers. The ST author should select “virtual device interface” if the TSF presents a virtual device interface to the guest OS through which it can obtain entropy or random numbers. Such an interface could present a virtualized real device, such as a TPM, that can be accessed by VM-unaware guests, or a virtualized fictional device that would require the guest OS to be VM-aware. The ST author should select “pass-through access to hardware entropy source” if the TSF permits guest VMs to have direct access to hardware entropy or random number source on the platform. The ST author should select all items that are appropriate.

For FCS_ENT_EXT.1.2, the VMM must ensure that the provision of entropy to one VM cannot affect the quality of entropy provided to another VM on the same platform.

Evaluation Activities ▼

FCS_ENT_EXT.1.1

TSS

The evaluator shall verify that the TSS describes how the TOE provides entropy to guest VMs, and how to access the interface to acquire entropy or random numbers. The evaluator shall verify that the TSS describes the mechanisms for ensuring that one VM does not affect the entropy acquired by another.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall perform the following tests:

- Test FCS_ENT_EXT.1.1.1: The evaluator shall invoke entropy from each guest VM. The evaluator shall verify that each VM acquires values from the interface.
- Test FCS_ENT_EXT.1.1.2: The evaluator shall invoke entropy from multiple VMs as nearly simultaneously as practicable. The evaluator shall verify that the entropy used in one VM is not identical to that invoked from the other VMs.

FCS_RBG.1 Cryptographic Operation (Random Bit Generation)

FCS_RBG.1.1

The TSF shall perform deterministic random bit generation services using [selection]:

- Hash_DRBG (any)
- HMAC_DRBG (any)
- CTR_DRBG (AES)

] in accordance with [NIST SP 800-90A] after initialization with a seed.

FCS_RBG.1.2

The TSF shall use a [selection: TSF noise source [assignment: name of noise source], multiple TSF noise sources [assignment: names of noise sources], TSF interface for seeding] for initialized seeding.

Application Note: For the selection in this requirement, the ST author selects "TSF noise source" if a single noise source is used as input to the DRBG. The ST author selects "multiple TSF noise sources" if a seed is formed from a combination of two or more noise sources within the TOE boundary. If the TSF implements two or more separate DRBGs that are seeded in separate manners, this SFR should be iterated for each DRBG. If multiple distinct noise sources exist such that each DRBG only uses one of them, then each iteration would select "TSF noise source"; "multiple TSF noise sources" is only selected if a single DRBG uses multiple noise sources for its seed. The ST author selects "TSF interface for seeding" if noise source data is generated outside the TOE boundary.

If "TSF noise source" is selected, [FCS_RBG.3](#) must be claimed.

If "multiple TSF noise sources" is selected, [FCS_RBG.4](#) and [FCS_RBG.5](#) must be claimed.

If "TSF interface for seeding" is selected, [FCS_RBG.2](#) must be claimed.

FCS_RBG.1.3

The TSF shall update the RBG state by [selection: reseeding, uninstantiating and reinstating] using a [selection: TSF noise source [assignment: name of noise source], TSF interface for seeding] in the following situations: [selection]:

- never
- on demand
- on the condition: [assignment: condition]
- after [assignment: time]

] in accordance with [assignment: list of standards].

Evaluation Activities ▼

[FCS_RBG.1.1](#)

TSS

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall perform the following tests, depending on the standard to which the RBG conforms.

The evaluator shall perform 15 trials for the RBG implementation. If the RBG is configurable, the evaluator shall perform 15 trials for each configuration. The evaluator shall also confirm that the operational guidance contains appropriate instructions for configuring the RBG functionality.

If the RBG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 - 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90A).

If the RBG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 - 14). The

next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.

The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.

- Entropy input: the length of the entropy input value must equal the seed length
- Nonce: If a nonce is supported (CTR_DRBG with no df does not use a nonce), the nonce bit length is one-half the seed length.
- Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is supported, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.
- Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.

5.1.4 User Data Protection (FDP)

FDP_HBI_EXT.1 Hardware-Based Isolation Mechanisms

FDP_HBI_EXT.1.1

The TSF shall use [**selection**: no mechanism, **assignment**: list of platform-provided, hardware-based mechanisms] to constrain a guest VM's direct access to the following physical devices: [**selection**: no devices, **assignment**: physical devices to which the VMM allows guest VMs physical access]].

Application Note: The TSF must use available hardware-based isolation mechanisms to constrain VMs when VMs have direct access to physical devices. "Direct access" in this context means that the VM can read or write device memory or access device I/O ports without the VMM being able to intercept and validate every transaction.

Evaluation Activities ▾

FDP_HBI_EXT.1.1

TSS

The evaluator shall ensure that the TSS provides evidence that hardware-based isolation mechanisms are used to constrain VMs when VMs have direct access to physical devices, including an explanation of the conditions under which the TSF invokes these protections.

Guidance

The evaluator shall verify that the operational guidance contains instructions on how to ensure that the platform-provided, hardware-based mechanisms are enabled.

Tests

There are no test activities for this element.

FDP_PPR_EXT.1 Physical Platform Resource Controls

FDP_PPR_EXT.1.1

The TSF shall allow an authorized administrator to control guest VM access to the following physical platform resources: [**assignment**: list of physical platform resources the VMM is able to control access to].

FDP_PPR_EXT.1.2

The TSF shall explicitly deny all guest VMs access to the following physical platform resources: [**selection**: no physical platform resources, **assignment**: list of physical platform resources to which access is explicitly denied]].

FDP_PPR_EXT.1.3

The TSF shall explicitly allow all guest VMs access to the following physical platform resources: [**selection**: no physical platform resources, **assignment**: list of physical platform resources to which access is always allowed]].

Application Note: For purposes of this requirement, physical platform resources are divided into three categories:

- those to which guest OS access is configurable and moderated by the VMM
- those to which the guest OS is never allowed to have direct access, and
- those to which the guest OS is always allowed to have direct access.

For element 1, the ST author lists the physical platform resources that can be configured for guest VM access by an administrator. For element 2, the ST author lists the physical platform resources to which guest VMs may never be allowed direct access. If there are no such resources, the ST author selects "no physical platform resources." Likewise, any resources to which all guest VMs automatically have access to are to be listed in the third element. If there are no such resources, then "no physical platform resources" is selected.

Evaluation Activities ▼

[FDP_PPR_EXT.1.1](#)

TSS

The evaluator shall examine the TSS to determine that it describes the mechanism by which the VMM controls a guest VM's access to physical platform resources. This description shall cover all of the physical platforms allowed in the evaluated configuration by the ST. It should explain how the VMM distinguishes among guest VMs, and how each physical platform resource that is controllable (that is, listed in the assignment statement in the first element) is identified to an administrator.

The evaluator shall ensure that the TSS describes how the guest VM is associated with each physical resource, and how other guest VMs cannot access a physical resource without being granted explicit access. For TOEs that implement a robust interface (other than just "allow access" or "deny access"), the evaluator shall ensure that the TSS describes the possible operations or modes of access between a guest VM's and physical platform resources.

If physical resources are listed in the second element, the evaluator shall examine the TSS and operational guidance to determine that there appears to be no way to configure those resources for access by a guest VM. The evaluator shall document in the evaluation report their analysis of why the controls offered to configure access to physical resources can't be used to specify access to the resources identified in the second element (for example, if the interface offers a drop-down list of resources to assign, and the denied resources are not included on that list, that would be sufficient justification in the evaluation report).

Guidance

The evaluator shall examine the operational guidance to determine that it describes how an administrator is able to configure access to physical platform resources for guest VMs for each platform allowed in the evaluated configuration according to the ST. The evaluator shall also determine that the operational guidance identifies those resources listed in the second and third elements of the component and notes that access to these resources is explicitly denied/allowed, respectively.

Tests

Using the operational guidance, the evaluator shall perform the following tests for each physical platform identified in the ST:

- Test FDP_PPR_EXT.1.1:1: For each physical platform resource identified in the first element, the evaluator shall configure a guest VM to have access to that resource and show that the guest VM is able to successfully access that resource.
- Test FDP_PPR_EXT.1.1:2: For each physical platform resource identified in the first element, the evaluator shall configure the system such that a guest VM does not have access to that resource and show that the guest VM is unable to successfully access that resource.
- Test FDP_PPR_EXT.1.1:3: [conditional]: For TOEs that have a robust control interface, the evaluator shall exercise each element of the interface as described in the TSS and the operational guidance to ensure that the behavior described in the operational guidance is exhibited.
- Test FDP_PPR_EXT.1.1:4: [conditional]: If the TOE explicitly denies access to certain physical resources, the evaluator shall attempt to access each listed (in [FDP_PPR_EXT.1.2](#)) physical resource from a guest VM and observe that access is denied.
- Test FDP_PPR_EXT.1.1:5: [conditional]: If the TOE explicitly allows access to certain physical resources, the evaluator shall attempt to access each listed (in [FDP_PPR_EXT.1.3](#)) physical resource from a guest VM and observe that the access is allowed. If the operational guidance specifies that access is allowed simultaneously by more than one guest VM, the evaluator shall attempt to access each resource listed from more than one guest VM and show that access is allowed.

FDP_RIP_EXT.1 Residual Information in Memory

FDP_RIP_EXT.1.1

The TSF shall ensure that any previous information content of physical memory is cleared prior to allocation to a guest VM.

Application Note: Physical memory must be zeroed before it is made accessible to a VM for general use by a guest OS.

The purpose of this requirement is to ensure that a VM does not receive memory containing data previously used by another VM or the host.

"For general use" means for use by the guest OS in its page tables for running applications or system software.

This does not apply to pages shared by design or policy between VMs or between the VMMs and VMs, such as read-only OS pages or pages used for virtual device buffers.

Evaluation Activities ▼

[FDP_RIP_EXT.1.1](#)

TSS

The evaluator shall ensure that the TSS documents the process used for clearing physical

memory prior to allocation to a guest VM, providing details on when and how this is performed. Additionally, the evaluator shall ensure that the TSS documents the conditions under which physical memory is not cleared prior to allocation to a guest VM, and describes when and how the memory is cleared.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

There are no test activities for this element.

FDP_RIP_EXT.2 Residual Information on Disk

FDP_RIP_EXT.2.1

The TSF shall ensure that any previous information content of physical disk storage is cleared to zeros upon allocation to a guest VM.

Application Note: The purpose of this requirement is to ensure that a VM does not receive disk storage containing data previously used by another VM or by the host.

Clearing of disk storage only upon deallocation does not meet this requirement.

This does not apply to disk-resident files shared by design or policy between VMs or between the VMMs and VMs, such as read-only data files or files used for inter-VM data transfers permitted by policy.

Evaluation Activities ▼

FDP_RIP_EXT.2.1

TSS

The evaluator shall ensure that the TSS documents how the TSF ensures that disk storage is zeroed upon allocation to guest VMs. Also, the TSS must document any conditions under which disk storage is not cleared prior to allocation to a guest VM. Any file system format and metadata information needed by the evaluator to perform the below test shall be made available to the evaluator, but need not be published in the TSS.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall perform the following test:

- *Test FDP_RIP_EXT.2.1.1: On the host, the evaluator creates a file that is more than half the size of a connected physical storage device (or multiple files whose individual sizes add up to more than half the size of the storage media). This file (or files) shall be filled entirely with a non-zero value. Then, the file (or files) shall be released (freed for use but not cleared). Next, the evaluator (as a VS administrator) creates a virtual disk at least that large on the same physical storage device and connects it to a powered-off VM. Then, from outside the guest VM, scan through and check that all the non-metadata (as documented in the TSS) in the file corresponding to that virtual disk is set to zero.*

FDP_VMS_EXT.1 VM Separation

FDP_VMS_EXT.1.1

The VS shall provide the following mechanisms for transferring data between guest VMs: [selection:

- *no mechanism*
- *virtual networking*
- *[assignment: other inter-VM data sharing mechanisms]*

].

FDP_VMS_EXT.1.2

The TSF shall by default enforce a policy prohibiting sharing of data between guest VMs.

FDP_VMS_EXT.1.3

The TSF shall allow administrators to configure the mechanisms selected in [FDP_VMS_EXT.1.1](#) to enable and disable the transfer of data between guest VMs.

FDP_VMS_EXT.1.4

The VS shall ensure that no guest VM is able to read or transfer data to or from another guest VM except through the mechanisms listed in [FDP_VMS_EXT.1.1](#).

Application Note: The fundamental requirement of a virtualization system is the ability to enforce separation between information domains implemented as Virtual Machines and Virtual Networks. The intent of this requirement is to ensure that VMs, VMMs, and the VS as a whole is implemented with this fundamental requirement in mind.

The ST author should select “no mechanism” in the unlikely event that the VS implements no mechanisms for transferring data between guest VMs. Otherwise, the ST author should select “virtual networking” and identify all other mechanisms through which data can be transferred between guest VMs.

Examples of non-network inter-VM sharing mechanisms are:

- User interface-based mechanisms, such as copy-paste and drag-and-drop
- Shared virtual or physical devices
- API-based mechanisms such as hypercalls

For data transfer mechanisms implemented in terms of hypercall functions, [FDP_VMS_EXT.1.3](#) is met if [FPT_HCL_EXT.1.1](#) is met for those hypercall functions (hypercall function parameters are checked).

For data transfer mechanisms that use shared physical devices, [FDP_VMS_EXT.1.3](#) is met if the device is listed in and meets [FDP_PPR_EXT.1.1](#) (VM access to the physical device is configurable).

For data transfer mechanisms that use virtual networking, [FDP_VMS_EXT.1.3](#) is met if [FDP_VNC_EXT.1.1](#) is met (VM access to virtual networks is configurable).

Evaluation Activities ▼

[FDP_VMS_EXT.1.1](#)

TSS

The evaluator shall examine the TSS to verify that it documents all inter-VM communications mechanisms (as defined above), and explains how the TSF prevents the transfer of data between VMs outside of the mechanisms listed in [FDP_VMS_EXT.1.1](#).

Guidance

The evaluator shall examine the operational guidance to ensure that it documents how to configure all inter-VM communications mechanisms, including how they are invoked and how they are disabled.

Tests

The evaluator shall perform the following tests for each documented inter-VM communications channel:

- Test [FDP_VMS_EXT.1.1:1](#):
 - a. Create two VMs without specifying any communications mechanism or overriding the default configuration.
 - b. Test that the two VMs cannot communicate through the mechanisms selected in [FDP_VMS_EXT.1.1](#).
 - c. Create two new VMs, overriding the default configuration to allow communications through a channel selected in [FDP_VMS_EXT.1.1](#).
 - d. Test that communications can be passed between the VMs through the channel.
 - e. Create two new VMs, the first with the inter-VM communications channel currently being tested enabled, and the second with the inter-VM communications channel currently being tested disabled.
 - f. Test that communications cannot be passed between the VMs through the channel.
 - g. As an administrator, enable inter-VM communications between the VMs on the second VM.
 - h. Test that communications can be passed through the inter-VM channel.
 - i. As an administrator again, disable inter-VM communications between the two VMs.
 - j. Test that communications can no longer be passed through the channel.

[FDP_VMS_EXT.1.2](#) is met if communication is unsuccessful in step (b). [FDP_VMS_EXT.1.3](#) is met if communication is successful in step (d) and unsuccessful in step (f).

FDP_VNC_EXT.1 Virtual Networking Components

[FDP_VNC_EXT.1.1](#)

The TSF shall allow administrators to configure virtual networking components to connect VMs to each other and to physical networks.

[FDP_VNC_EXT.1.2](#)

The TSF shall ensure that network traffic visible to a guest VM on a virtual network-or virtual segment of a physical network-is visible only to guest VMs configured to be on that virtual network or segment.

Application Note: Virtual networks must be separated from one another to provide isolation commensurate with that provided by physically separate networks. It must not be possible for data to cross between properly configured virtual networks regardless of whether the traffic originated from a local guest VM or a remote host.

Unprivileged users must not be able to connect VMs to each other or to external networks.

Evaluation Activities ▼

[FDP_VNC_EXT.1.1](#)

TSS

The evaluator shall examine the TSS (or a proprietary annex) to verify that it describes the mechanism by which virtual network traffic is ensured to be visible only to guest VMs configured to be on that virtual network.

Guidance

The evaluator must ensure that the Operational Guidance describes how to create virtualized networks and connect VMs to each other and to physical networks.

Tests

- Test FDP_VNC_EXT.1.1:1: The evaluator shall assume the role of the administrator and attempt to configure a VM to connect to a network component. The evaluator shall verify that the attempt is successful. The evaluator shall then assume the role of an unprivileged user and attempt the same connection. If the attempt fails, or there is no way for an unprivileged user to configure VM network connections, the requirement is met.
- Test FDP_VNC_EXT.1.1:2: The evaluator shall assume the role of the administrator and attempt to configure a VM to connect to a physical network. The evaluator shall verify that the attempt is successful. The evaluator shall then assume the role of an unprivileged user and make the same attempt. If the attempt fails, or there is no way for an unprivileged user to configure VM network connections, the requirement is met.

5.1.5 Identification and Authentication (FIA)

FIA_AFL_EXT.1 Authentication Failure Handling

FIA_AFL_EXT.1.1

The TSF shall detect when [selection:

- [**assignment**: a positive integer number]
- an administrator configurable positive integer within a [**assignment**: range of acceptable values]

] unsuccessful authentication attempts occur related to administrators attempting to authenticate remotely using [selection: username and password, username and PIN].

FIA_AFL_EXT.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall: [selection: prevent the offending administrator from successfully establishing a remote session using any authentication method that involves a password or PIN until [**assignment**: action to unlock] is taken by an administrator, prevent the offending administrator from successfully establishing a remote session using any authentication method that involves a password or PIN until an administrator-defined time period has elapsed]

Application Note: The action to be taken shall be populated in the selection of the ST and defined in the administrator guidance.

This requirement applies to a defined number of successive unsuccessful remote password or PIN-based authentication attempts and does not apply to local Administrative access. Compliant TOEs may optionally include cryptographic and local authentication failures in the number of unsuccessful authentication attempts.

Evaluation Activities ▼

FIA_AFL_EXT.1.1

TSS

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall perform the following tests for each credential selected in [FIA_AFL_EXT.1.1](#):

The evaluator will set an administrator-configurable threshold n for failed attempts, or note the ST-specified assignment.

After reaching the limit for unsuccessful authentication attempts the evaluator will proceed as follows:

- Test FIA_AFL_EXT.1.1:1: The evaluator will attempt to authenticate remotely with the credential $n-1$ times. The evaluator will then attempt to authenticate using a good credential and verify that authentication is successful.
- Test FIA_AFL_EXT.1.1:2: The evaluator will make n attempts to authenticate using a bad credential. The evaluator will then attempt to authenticate using a good credential and verify that the attempt is unsuccessful. Note that the authentication attempts and lockouts must also be logged as specified in [FAU_GEN.1](#).
- Test FIA_AFL_EXT.1.1:3: If the administrator action selection in [FIA_AFL_EXT.1.2](#) is selected, then the evaluator will confirm by testing that following the operational guidance and performing each action specified in the ST to re-enable the remote administrator's access results in successful access (when using valid credentials for that administrator).
- Test FIA_AFL_EXT.1.1:4: If the time period selection in [FIA_AFL_EXT.1.2](#) is selected, the

evaluator will wait for just less than the time period configured and show that an authentication attempt using valid credentials does not result in successful access. The evaluator will then wait until just after the time period configured and show that an authentication attempt using valid credentials results in successful access.

FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1

The TSF shall provide [selection]:

- [selection: local, directory-based] authentication based on username and password
- authentication based on username and a PIN that releases an asymmetric key stored in OE-protected storage
- [selection: local, directory-based] authentication based on X.509 certificates
- [selection: local, directory-based] authentication based on an SSH public key credential

] to support user authentication.

Application Note: Selection of 'authentication based on username and password' requires that FIA_PMG_EXT.1 be included in the ST. This also requires that the ST claim management function 2 for password management. If the ST author selects 'authentication based on an SSH public-key credential', the TSF shall be validated against the Functional Package for Secure Shell (SSH), version 2.0. The ST must include FIA_X509_EXT.1 and FIA_X509_EXT.2 from the Functional Package for X.509, version 1.0, if 'authentication based on X.509 certificates' is selected.

PINs used to access OE-protected storage are set and managed by the OE-protected storage mechanism. Thus requirements on PIN management are outside the scope of the TOE.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [assignment: rules describing how the multiple authentication mechanisms provide authentication].

Evaluation Activities ▼

FIA_UAU.5.1

TSS

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

If 'username and password authentication' is selected, the evaluator will configure the VS with a known username and password and conduct the following tests: If 'username and PIN that releases an asymmetric key' is selected, the evaluator will examine the TSS for guidance on supported protected storage and will then configure the TOE or OE to establish a PIN which enables release of the asymmetric key from the protected storage (such as a TPM, a hardware token, or isolated execution environment) with which the VS can interface. The evaluator will then conduct the following tests: If 'X.509 certificate authentication' is selected, the evaluator will generate an X.509v3 certificate for an administrator user with the Client Authentication Enhanced Key Usage field set. The evaluator will provision the VS for authentication with the X.509v3 certificate. The evaluator shall ensure that the certificates are validated by the VS as per FIA_X509_EXT.1.1 in the Functional Package for X.509, version 1.0 and then conduct the following tests: If 'SSH public-key credential authentication' is selected, the evaluator shall generate a public-private host key pair on the TOE using RSA or ECDSA, and a second public-private key pair on a remote client. The evaluator shall provision the VS with the client public key for authentication over SSH, and conduct the following tests:

- Test FIA_UAU.5.1:1: The evaluator will attempt to authenticate to the VS using the known username and password. The evaluator will ensure that the authentication attempt is successful.
- Test FIA_UAU.5.1:2: The evaluator will attempt to authenticate to the VS using the known username but an incorrect password. The evaluator will ensure that the authentication attempt is unsuccessful.
- Test FIA_UAU.5.1:3: The evaluator will attempt to authenticate to the VS using the known user name and PIN. The evaluator will ensure that the authentication attempt is successful.
- Test FIA_UAU.5.1:4: The evaluator will attempt to authenticate to the VS using the known user name but an incorrect PIN. The evaluator will ensure that the authentication attempt is unsuccessful.
- Test FIA_UAU.5.1:5: The evaluator will attempt to authenticate to the VS using the X.509v3 certificate. The evaluator will ensure that the authentication attempt is successful.
- Test FIA_UAU.5.1:6: The evaluator will generate a second certificate identical to the first except for the public key and any values derived from the public key. The evaluator will attempt to authenticate to the VS with this certificate. The evaluator will ensure that the

authentication attempt is unsuccessful.

- *Test FIA_UAU.5.1.7: The evaluator will attempt to authenticate to the VS using a message signed by the client private key that corresponds to provisioned client public key. The evaluator will ensure that the authentication attempt is successful.*
- *Test FIA_UAU.5.1.8: The evaluator will generate a second client key pair and will attempt to authenticate to the VS with the private key over SSH without first provisioning the VS to support the new key pair. The evaluator will ensure that the authentication attempt is unsuccessful.*

FIA_UIA_EXT.1 Administrator Identification and Authentication

FIA_UIA_EXT.1.1

The TSF shall require administrators to be successfully identified and authenticated using one of the methods in [FIA_UAU.5](#) before allowing any TSF-mediated management function to be performed by that administrator.

Application Note: Users do not have to authenticate, only administrators need to authenticate.

Evaluation Activities ▼

[**FIA_UIA_EXT.1.1**](#)

TSS

The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed or used, any protocol transactions that take place, and what constitutes a “successful logon.”

Guidance

The evaluator shall examine the operational guidance to determine that any necessary preparatory steps (e.g., establishing credential material such as pre-shared keys, tunnels, certificates) to logging in are described. For each supported login method, the evaluator shall ensure the operational guidance provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the operational guidance provides sufficient instruction on limiting the allowed services.

Tests

There are no test activities for this element.

5.1.6 Security Management (FMT)

FMT_MOF_EXT.1 Management of Security Functions Behavior

FMT_MOF_EXT.1.1

The TSF shall be capable of supporting [**selection**: local, remote] administration.

Application Note: Selection of “remote” requires the selection-based requirement [FTP_TRP.1](#) to be claimed in the ST.

FMT_MOF_EXT.1.2

The TSF shall be capable of performing the following management functions: [

Table 4: Management Functions

Status Markers: M = Mandatory (TOE must provide that function to that role) O = Optional>Selectable/Conditional (TOE may provide the function to that role) X = Not Permitted (TOE must not provide that function to that role)

Table 5: Management Functions

Status Markers:

O - Indicates that this function is optional for this role

M - Indicates that this function is mandatory for this role.

X - Indicates that this function is not permitted for this role

#	Management Function	Admin	User
1	Ability to update the virtualization system.	M	X
2	[selection : Ability to configure administrator password policy as defined in FIA_PMG_EXT.1 , Not applicable]	O	X
3	Ability to create, configure and delete VMs	M	O
4	Ability to set default initial VM configurations	M	O

5	Ability to configure virtual networks including VM	M	O
6	Ability to configure and manage the audit system and audit data	M	X
7	Ability to configure VM access to physical devices	M	O
8	Ability to configure inter-VM data sharing	M	O
9	Ability to configure removable media policy	M	O
10	Ability to configure the cryptographic functionality	O	O
11	Ability to change default authorization factors	M	X
12	Ability to enable/disable screen lock	O	O
13	Ability to configure screen lock inactivity timeout	O	O
14	Ability to configure remote connection inactivity timeout	M	X
15	Ability to configure lockout policy for unsuccessful authentication attempts through [selection: timeouts between attempts, limiting number of attempts during a time period]	M	X
16	[selection: Ability to configure name/address of directory server to bind with, Not applicable]	O	X
17	Ability to configure name/address of audit/logging server to which to send audit/logging records	M	X
18	Ability to configure name/address of network time server	M	O
19	Ability to configure banner	M	X
20	Ability to connect/disconnect removable devices to/from a VM	O	O
21	Ability to start a VM	O	O
22	Ability to stop/halt a VM	O	O
23	Ability to checkpoint a VM	O	O
24	Ability to suspend a VM	O	O
25	Ability to resume a VM	O	O
26	[selection: Ability to configure action taken if unable to determine the validity of a certificate, Not applicable]	O	X

].

Application Note: The ST author is expected to update [Table 4](#) with an indication as to whether any of the optional functions are included as part of the TOE. The ST author may also omit the 'Notes' column as it is provided in this PP as an aid to the ST author in constructing the table.

This SFR addresses the roles of the CC Part 2 SFRs FMT_MOF.1, FMT_SMF.1, and FMT_SMR.2.

Administration is considered "local" if the administrator is physically present at the machine on which the VS is installed.

Administration is considered "remote" if communications between the administrator and the Management Subsystem travel on a network.

There is no requirement to authenticate users of the virtualization system. Users that have access to VMs but not to the Management Subsystem need not authenticate to the virtualization system in order to use Guest VMs.

Requirements for authentication of VM users is determined by the policies of the domains running within the Guest VMs.

For a VS where the OS is part of the platform and not part of the TOE, it is acceptable for the VS to invoke the Host OS screen lock.

Function-specific Application Notes:

See [FPT_TUD_EXT.1](#).

Must be selected if [FIA_PMG_EXT.1](#) is claimed.

Optional for Users in the Client use case. Forbidden for Users in the Server use case.

See [FDP_VNC_EXT.1](#).

See [FDP_PPR_EXT.1](#)

See [FDP_VMS_EXT.1](#)

See [FPT_RDM_EXT.1](#)

Optional for Users in the Client use case. Forbidden for Users in the Server use case.

Mandatory for Admin role for the Server use case.

Forbidden for Users for the Server use case.

Optional for all roles for the Client use case.

See [FIA_PMG_EXT.1](#)

See [FIA_AFL_EXT.1](#)

Must be selected if "directory-based" is selected anywhere in [FIA_UAU.5.1](#).

See [FAU_STG_EXT.1](#)

See [FTA_TAB.1](#)

See [FPT_RDM_EXT.1](#)

This function must be selected if "allow the administrator to choose whether to accept the certificate in these cases" in [FIA_X509_EXT.2.2](#)

Evaluation Activities ▼

[FMT_MOF_EXT.1](#)

[FMT_MOF_EXT.1.1](#)

TSS

The evaluator shall examine the TSS and Operational Guidance to ensure that it describes which security management functions require administrator privilege and the actions associated with each management function. The evaluator shall verify that for each management function and role specified in [Table 4](#), the defined role is able to perform all mandatory functions as well as all optional or selection-based functions claimed in the ST.

Guidance

The evaluator shall examine the Operational Guidance to ensure that it describes how the administrator and user are able to perform each management function that the ST claims the TOE supports.

The evaluator shall verify for each claimed management function that the Operational Guidance is sufficiently detailed to allow the function to be performed and that the function can be performed.

Tests

The evaluator shall test each management function for each role listed in the [FMT_MOF_EXT.1.1 Table 4](#) in the ST to demonstrate that the function can be performed by the roles that are authorized to do so and the result of the function is demonstrated. The evaluator shall also verify for each claimed management function in [Table 4](#), that if the TOE claims not to provide a particular role with access to the function, then it is not possible to access the TOE as that role and perform that function.

The following EAs correspond to specific management functions.

Function 1

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 2 [CONDITIONAL]

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 3

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 4**TSS**

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 5**TSS**

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 6**TSS**

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 7**TSS**

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 8**TSS**

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 9**TSS**

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 10 [CONDITIONAL]**TSS**

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 11**TSS**

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 12 [CONDITIONAL]

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 13 [CONDITIONAL]

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 14

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 15

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 16 [CONDITIONAL]

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 17

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 18

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 19

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 20 [CONDITIONAL]

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 21 [CONDITIONAL]

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 22 [CONDITIONAL]

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 23 [CONDITIONAL]

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 24 [CONDITIONAL]

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 25 [CONDITIONAL]

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

Function 26 [CONDITIONAL]

TSS

There are no additional TSS evaluation activities for this management function.

Guidance

There are no additional Guidance evaluation activities for this management function.

Tests

There are no test activities for this management function.

FMT_SMO_EXT.1 Separation of Management and Operational Networks

FMT_SMO_EXT.1.1

The TSF shall support the separation of management and operational network traffic through [**selection: separate physical networks, separate logical networks, trusted channels as defined in [FTP_ITC_EXT.1](#), data encryption using an algorithm specified in FCS_COP.1/UDE**].

Application Note: Management communications must be separate from user workload communications. Administrative network traffic—including communications between physical hosts concerning load balancing, audit data, VM startup and shutdown—must be isolated from guest operational networks. For purposes of this requirement, management traffic also includes VMs transmitted over management networks whether for backup, live migration, or deployment.

“Separate physical networks” refers to using separate physical interfaces and cables to isolate management and operational networks from each other.

“Separate logical networks” refers to using logical networking constructs, such as separate IP spaces or virtual networks to isolate traffic across general-purpose networking ports. Management and operational networks are kept separate within the hosts using separate virtualized networking components.

If the ST author selects “trusted channels...” then the protocols used for network separation must be selected in [FTP_ITC_EXT.1](#).

The ST author selects “data encryption...” if, for example, the TOE encrypts VMs as data blobs for backup, storage, deployment, or live migration, and does not send the data through a tunnel. If the ST author selects “data encryption...” then the algorithms and key sizes must be selected in [FCS_COP.1/UDE](#).

The ST author should select as many mechanisms as apply.

Evaluation Activities ▼

FMT_SMO_EXT.1.1

TSS

The evaluator shall examine the TSS to verify that it describes how management and operational traffic is separated.

Guidance

The evaluator shall examine the operational guidance to verify that it details how to configure the VS to keep Management and Operational traffic separate.

Tests

The evaluator shall configure the TOE as documented in the guidance. If separation is logical, then the evaluator shall capture packets on the management network. If plaintext Guest network traffic is detected, the requirement is not met.

If separation uses trusted channels, then the evaluator shall capture packets on the network over which traffic is tunneled. If plaintext Guest network traffic is detected, the requirement is not met.

If data encryption is used, then the evaluator shall capture packets on the network over which the data is sent while a VM or other large data structure is being transmitted. If plaintext VM contents are detected, the requirement is not met.

5.1.7 Protection of the TSF (FPT)

FPT_DVD_EXT.1 Non-Existence of Disconnected Virtual Devices

FPT_DVD_EXT.1.1

The TSF shall prevent guest VMs from accessing virtual device interfaces that are not present in the VM's current virtual hardware configuration.

Application Note: The virtualized hardware abstraction implemented by a particular VS might include the virtualized interfaces for many different devices.

Sometimes these devices are not present in a particular instantiation of a VM. The interface for devices not present must not be accessible by the VM.

Such interfaces include memory buffers, PCI Bus interfaces, and processor I/O ports.

The purpose of this requirement is to reduce the attack surface of the VMM by blocking access to unused interfaces.

Evaluation Activities ▼

[FPT_DVD_EXT.1.1](#)

TSS

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall connect a device to a VM, then from within the guest scan the VM's devices to ensure that the connected device is present—using a device driver or other available means to scan the VM's I/O ports or PCI Bus interfaces. (The device's interface should be documented in the TSS under [FPT_VDP_EXT.1](#).) The evaluator shall remove the device from the VM and run the scan again. This requirement is met if the device's interfaces are no longer present.

FPT_EEM_EXT.1 Execution Environment Mitigations

FPT_EEM_EXT.1.1

The TSF shall take advantage of execution environment-based vulnerability mitigation mechanisms supported by the Platform such as: [selection]:

- *Address space randomization*
- *Memory execution protection (e.g., DEP)*
- *Stack buffer overflow protection*
- *Heap corruption detection*
- *[assignment: other mechanisms]*
- *No mechanisms*

]

Application Note: Processor manufacturers, compiler developers, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Software can often take advantage of these mechanisms by using APIs provided by the operating system or by enabling the mechanism through compiler or linker options. This requirement does not mandate that these protections be enabled throughout the virtualization system—only that they be enabled where they have likely impact. For example, code that receives and processes user input should take advantage of these mechanisms.

For the selection, the ST author selects the supported mechanisms and uses the assignment to include mechanisms not listed in the selection, if any.

Evaluation Activities ▼

[FPT_EEM_EXT.1.1](#)

TSS

The evaluator shall examine the TSS to ensure that it states, for each platform listed in the ST, the execution environment-based vulnerability mitigation mechanisms used by the TOE on that platform. The evaluator shall ensure that the lists correspond to what is specified in [FPT_EEM_EXT.1.1](#).

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

There are no test activities for this element.

FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [DRBG self-test failure].

Application Note: The intent of this requirement is to ensure that cryptographic services requiring random bit generation cannot be performed if a failure of a self-test defined in [FPT_TST.1](#) occurs.

Evaluation Activities ▼

FPT_FLS.1.1

TSS

The evaluator shall verify that the TSF describes how the TOE enters an error state in the event of a DRBG self-test failure.

Guidance

The evaluator shall verify that the guidance documentation describes the error state that results from a DRBG self-test failure and the actions that a user or administrator should take in response to attempt to resolve the error state.

Tests

There are no test activities for this element.

FPT_HAS_EXT.1 Hardware Assists

FPT_HAS_EXT.1.1

The VMM shall use [**assignment**: *list of hardware-based virtualization assists*] to reduce or eliminate the need for binary translation.

FPT_HAS_EXT.1.2

The VMM shall use [**assignment**: *list of hardware-based virtualization memory-handling assists*] to reduce or eliminate the need for shadow page tables.

Application Note: These hardware-assists help reduce the size and complexity of the VMM, and thus, of the trusted computing base, by eliminating or reducing the need for paravirtualization or binary translation. Paravirtualization involves modifying guest software so that instructions that cannot be properly virtualized are never executed on the physical processor.

For the assignment in [FPT_HAS_EXT.1](#), the ST author lists the hardware-based virtualization assists on all platforms included in the ST that are used by the VMM to reduce or eliminate the need for software-based binary translation. Examples for the x86 platform are Intel VT-x and AMD-V. “None” is an acceptable assignment for platforms that do not require virtualization assists in order to eliminate the need for binary translation. This must be documented in the TSS.

For the assignment in [FPT_HAS_EXT.1.2](#), the ST author lists the set of hardware-based virtualization memory-handling extensions for all platforms listed in the ST that are used by the VMM to reduce or eliminate the need for shadow page tables. Examples for the x86 platform are Intel EPT and AMD RVI. “None” is an acceptable assignment for platforms that do not require memory-handling assists in order to eliminate the need for shadow page tables. This must be documented in the TSS.

Evaluation Activities ▼

FPT_HAS_EXT.1.1

TSS

The evaluator shall examine the TSS to ensure that it states, for each platform listed in the ST, the hardware assists and memory-handling extensions used by the TOE on that platform. The evaluator shall ensure that these lists correspond to what is specified in the applicable FPT_HAS_EXT component.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

There are no test activities for this element.

FPT_HCL_EXT.1 Hypervisor Call Controls

FPT_HCL_EXT.1.1

The TSF shall validate the parameters passed to hypervisor call interfaces prior to execution of the VMM functionality exposed by each interface.

Application Note: The purpose of this requirement is to help ensure the integrity of the VMM by protecting the attack surface exposed to untrusted guest VMs through hypervisor calls.

A hypervisor call interface allows VMM functionality to be invoked by VM-aware guest software. For example, a hypervisor call interface could be used to get information about the real world, such as the time of day or the underlying hardware of the host system. A hypervisor call could also be used to transfer data between VMs through a copy-paste mechanism. Because hypervisor call interfaces expose the VMM to Guest software, these interfaces constitute attack surface.

There is no expectation that the evaluator will need to review source code in

order to accomplish the evaluation activity.

Evaluation Activities ▼

FPT_HCL_EXT.1.1

TSS

The evaluator shall examine the TSS (or proprietary TSS Annex) to ensure that all hypercall functions are documented at the level necessary for the evaluator to run the below test. Documentation for each hypercall interface must include: how to invoke the interface, parameters and legal values, and any conditions under which the interface can be invoked (e.g., from guest user mode, guest privileged mode, during guest boot only).

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall perform the following test:

For each hypercall interface documented in the TSS or proprietary TSS Annex, the evaluator shall attempt to invoke the function from within the VM using an invalid parameter (if any). If the VMM or VS crashes or generates an exception, or if no error is returned to the guest, then the test fails. If an error is returned to the guest, then the test succeeds.

FPT_RDM_EXT.1 Removable Devices and Media

FPT_RDM_EXT.1.1

The TSF shall implement controls for handling the transfer of virtual and physical removable media and virtual and physical removable media devices between information domains.

FPT_RDM_EXT.1.2

The TSF shall enforce the following rules when [**assignment**: *virtual or physical removable media and virtual or physical removable media devices*] are switched between information domains, then [**selection**]:

- *the administrator has granted explicit access for the media or device to be connected to the receiving domain*
- *the media in a device that is being transferred is ejected prior to the receiving domain being allowed access to the device*
- *the user of the receiving domain expressly authorizes the connection*
- *the device or media that is being transferred is prevented from being accessed by the receiving domain*

]

Application Note: The purpose of these requirements is to ensure that VMs are not given inadvertent access to information from different domains because of media or removable media devices left connected to physical machines.

Removable media is media that can be ejected from a device, such as a compact disc, floppy disk, SD, or compact flash memory card.

Removable media devices are removable devices that include media, such as USB flash drives and USB hard drives. Removable media devices can themselves contain removable media (e.g., USB CDROM drives).

For purposes of this requirement, an Information Domain is:

- a. A VM or collection of VMs
- b. The virtualization system
- c. Host OS
- d. Management Subsystem

These requirements also apply to virtualized removable media—such as virtual CD drives that connect to ISO images—as well as physical media—such as CDROMs and USB flash drives. In the case of virtual CDROMs, virtual ejection of the virtual media is sufficient.

In the first assignment, the ST author lists all removable media and removable media devices (both virtual and real) that are supported by the TOE. The ST author then selects actions that are appropriate for all removable media and removable media devices (both virtual and real) that are being claimed in the assignment.

For clarity, the ST author may iterate this requirement so that like actions are grouped with the removable media or devices to which they apply (e.g., the first iteration could contain all devices for which media is ejected on a switch; the second iteration could contain all devices for which access is prevented on a switch, etc.).

Evaluation Activities ▼

FPT_RDM_EXT.1.1

TSS

The evaluator shall examine the TSS to ensure it describes the association between the media or devices supported by the TOE and the actions that can occur when switching information domains.

Guidance

The evaluator shall examine the operational guidance to ensure it documents how an administrator or user configures the behavior of each media or device.

Tests

The evaluator shall perform the following test for each listed media or device:

- *Test FPT_RDM_EXT.1.1.1: The evaluator shall configure two VMs that are members of different information domains, with the media or device connected to one of the VMs. The evaluator shall disconnect the media or device from the VM and connect it to the other VM. The evaluator shall verify that the action performed is consistent with the action assigned in the TSS.*

FPT_TST.1 TSF Self-Testing

FPT_TST.1.1

The TSF shall run a suite of the following self-tests [**selection**: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-test should occur]*] to demonstrate the correct operation of [TSF DRBG specified in [FCS_RBG.1](#)].

FPT_TST.1.2

The TSF shall provide authorized users with the capability to verify the integrity of [[DRBG seed/output data]].

FPT_TST.1.3

The TSF shall provide authorized users with the capability to verify the integrity of [[TSF DRBG specified in [FCS_RBG.1](#)]].

Application Note: This SFR is a required dependency of [FCS_RBG.1](#). It is intended to require that any DRBG implemented by the TOE undergo health testing to ensure that the random bit generation functionality has not been degraded. If the TSF supports multiple DRBGs, this SFR should be iterated to describe the self-test behavior for each.

Evaluation Activities ▼

[FPT_TST.1.1](#)

TSS

The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF along with how they are run. This description should include an outline of what the tests are actually doing. The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the DRBG is operating correctly.

Note that this information may also be placed in the entropy documentation specified by .

Guidance

If a self-test can be executed at the request of an authorized user, the evaluator shall verify that the operational guidance provides instructions on how to execute that self-test.

Tests

For each self-test, the evaluator shall verify that evidence is produced that the self-test is executed when specified by [FPT_TST.1.1](#).

If a self-test can be executed at the request of an authorized user, the evaluator shall verify that following the steps documented in the operational guidance to perform the self-test will result in execution of the self-test.

FPT_TUD_EXT.1 Trusted Updates to the Virtualization System

FPT_TUD_EXT.1.1

The TSF shall provide administrators the ability to query the currently executed version of the TOE firmware and software as well as the most recently installed version of the TOE firmware and software.

Application Note: The version currently running (being executed) may not be the version most recently installed. For instance, maybe the update was installed but the system requires a reboot before this update will run. Therefore, it needs to be clear that the query should indicate both the most recently executed version as well as the most recently installed update.

FPT_TUD_EXT.1.2

The TSF shall provide administrators the ability to manually initiate updates to TOE firmware and software and [**selection**: *automatic updates, no other update mechanism*].

FPT_TUD_EXT.1.3

The TSF shall provide means to authenticate firmware and software updates to

the TOE using a [**selection**: digital signature mechanism using certificates, digital signature mechanism not using certificates, published hash] prior to installing those updates.

Application Note: The digital signature mechanism referenced in [FPT_TUD_EXT.1.3](#) is one of the algorithms specified in FCS_COP.1/SIG.

If certificates are used by the update verification mechanism, then FIA_X509_EXT.1 and FIA_X509_EXT.2 in the Functional Package for X.509, version 1.0 must be included in the ST. Certificates are validated in accordance with FIA_X509_EXT.1 in the Functional Package for X.509, version 1.0 and the appropriate selections should be made in FIA_X509_EXT.2.1 in the Functional Package for X.509, version 1.0. Additionally, [FPT_TUD_EXT.2](#) must be included in the ST.

"Update" in the context of this SFR refers to the process of replacing a non-volatile, system resident software component with another. The former is referred to as the NV image, and the latter is the update image. While the update image is typically newer than the NV image, this is not a requirement. There are legitimate cases where the system owner may want to rollback a component to an older version (e.g., when the component manufacturer releases a faulty update, or when the system relies on an undocumented feature no longer present in the update). Likewise, the owner may want to update with the same version as the NV image to recover from faulty storage.

All discrete software components (e.g., applications, drivers, kernel, firmware) of the TSF, should be digitally signed by the corresponding manufacturer and subsequently verified by the mechanism performing the update. Since it is recognized that components may be signed by different manufacturers, it is essential that the update process verify that both the update and NV images were produced by the same manufacturer (e.g., by comparing public keys) or signed by legitimate signing keys (e.g., successful verification of certificates when using X.509 certificates).

The Digital Signature option is the preferred mechanism for authenticating updates. The Published Hash option will be removed from a future version of this PP.

Evaluation Activities ▼

[FPT_TUD_EXT.1.1](#)

TSS

The evaluator shall verify that the TSS describes all TSF software update mechanisms for updating the system software. Updates to the TOE either have a hash associated with them, or are signed by an authorized source. The evaluator shall verify that the description includes either a digital signature or published hash verification of the software before installation and that installation fails if the verification fails. The evaluator shall verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the update, and the actions that take place for both successful and unsuccessful verification. If digital signatures are used, the evaluator shall also ensure the definition of an authorized source is contained in the TSS.

If the ST author indicates that a certificate-based mechanism is used for software update digital signature verification, the evaluator shall verify that the TSS contains a description of how the certificates are contained on the device. The evaluator also ensures that the TSS (or administrator guidance) describes how the certificates are installed/updated/selected, if necessary.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall perform the following tests:

- Test FPT_TUD_EXT.1.1.1: The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains a legitimate update using procedures described in the operational guidance and verifies that it is successfully installed on the TOE. After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update.
- Test FPT_TUD_EXT.1.1.2: The evaluator performs the version verification activity to determine the current version of the product. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:
 1. A modified version (e.g., using a hex editor) of a legitimately signed or hashed update
 2. An image that has not been signed/hashed
 3. An image signed with an invalid hash or invalid signature (e.g., by using a different key as expected for creating the signature or by manual modification of a legitimate hash/signature)

FPT_VDP_EXT.1 Virtual Device Parameters

FPT_VDP_EXT.1.1

The TSF shall provide interfaces for virtual devices implemented by the VMM as part of the virtual hardware abstraction.

FPT_VDP_EXT.1.2

The TSF shall validate the parameters passed to the virtual device interface prior to execution of the VMM functionality exposed by those interfaces.

Application Note: The purpose of this requirement is to ensure that the VMM is not vulnerable to compromise through the processing of malformed data passed to the virtual device interface from a guest OS. The VMM cannot assume that any data coming from a VM is well-formed—even if the virtual device interface is unique to the VS and the data comes from a virtual device driver supplied by the Virtualization Vendor.

Evaluation Activities ▼

[FPT_VDP_EXT.1.1](#)

TSS

The evaluator shall examine the TSS to ensure it lists all virtual devices accessible by the guest OS. The TSS, or a separate proprietary document, must also document all virtual device interfaces at the level of I/O ports or PCI Bus interfaces - including port numbers (absolute or relative to a base), port name, address range, and a description of legal input values.

The TSS must also describe the expected behavior of the interface when presented with illegal input values. This behavior must be deterministic and indicative of parameter checking by the TSF.

The evaluator must ensure that there are no obvious or publicly known virtual I/O ports missing from the TSS.

There is no expectation that evaluators will examine source code to verify the “all” part of the evaluation activity.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

For each virtual device interface, the evaluator shall attempt to access the interface using at least one parameter value that is out of range or illegal. The test is passed if the interface behaves in the manner documented in the TSS. Interfaces that do not have input parameters need not be tested. This test can be performed in conjunction with the tests for [FPT_DVD_EXT.1](#).

FPT_VIV_EXT.1 VMM Isolation from VMs

FPT_VIV_EXT.1.1

The TSF must ensure that software running in a VM is not able to degrade or disrupt the functioning of other VMs, the VMM, or the platform.

FPT_VIV_EXT.1.2

The TSF must ensure that a guest VM is unable to invoke platform code that runs at a privilege level equal to or exceeding that of the VMM without involvement of the VMM.

Application Note: This requirement is intended to ensure that software running within a guest VM cannot compromise other VMs, the VMM, or the platform. This requirement is not met if guest VM software—whatever its privilege level—can crash the VS or the Platform, or breakout of its virtual hardware abstraction to gain execution on the platform, within or outside of the context of the VMM.

This requirement is not violated if software running within a VM can crash the guest OS and there is no way for an attacker to gain execution in the VMM or outside of the virtualized domain.

[FPT_VIV_EXT.1.2](#) addresses several specific mechanisms that must not be permitted to bypass the VMM and invoke privileged code on the Platform.

At a minimum, the TSF should enforce the following:

- On the x86 platform, a virtual System Management Interrupt (SMI) cannot invoke platform System Management Mode (SMM).
- An attempt to update virtual firmware or virtual BIOS cannot cause physical platform firmware or physical platform BIOS to be modified.
- An attempt to update virtual firmware or virtual BIOS cannot cause the VMM to be modified.

Of the above, the first bullet does not apply to platforms that do not support SMM. The rationale behind the third bullet is that a firmware update of a single VM must not affect other VMs. So if multiple VMs share the same firmware image as part of a common hardware abstraction, then the update of a single machine’s BIOS must not be allowed to change the common abstraction. The virtual hardware abstraction is part of the VMM.

Evaluation Activities ▼

[FPT_VIV_EXT.1.1](#)

TSS

The evaluator shall verify that the TSS (or a proprietary annex to the TSS) describes how the TSF ensures that guest software cannot degrade or disrupt the functioning of other VMs, the VMM or the platform. And how the TSF prevents guests from invoking higher-privilege platform code, such as the examples in the note.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

There are no test activities for this element.

5.1.8 TOE Access Banner (FTA)

FTA_TAB.1 TOE Access Banner

FTA_TAB.1.1

Before establishing a user session, the [**selection**: TSF, TOE platform] shall display a [**assignment**: description of the message] message.

Application Note: This requirement is intended to apply to interactive sessions between a human user and a TOE. IT entities establishing connections or programmatic connections (e.g., remote procedure calls over a network) are not required to be covered by this requirement.

Evaluation Activities ▼

[FTA_TAB.1.1](#)

TSS

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall configure the TOE to display the advisory warning message "TEST TEST Warning Message TEST TEST". The evaluator shall then log out and confirm that the advisory message is displayed before login can occur.

5.1.9 Trusted Path/Channel (FTP)

FTP_ITC_EXT.1 Trusted Channel Communications

FTP_ITC_EXT.1.1

The TSF shall use [**selection**:

- TLS as conforming to the
- TLS/HTTPS as conforming to [FCS_HTTPS_EXT.1](#)
- IPsec as conforming to [FCS_IPSEC_EXT.1](#)
- SSH as conforming to the [Functional Package for Secure Shell](#)

] and [**selection**:

- certificate-based authentication of the remote peer
- non-certificate-based authentication of the remote peer
- no authentication of the remote peer

] to provide a trusted communication channel between itself and

- audit servers (as required by [FAU_STG.1](#)) and

[**selection**:

- remote administrators (as required by [FTP_TRP.1.1](#) if selected in [FMT_MOF_EXT.1.1](#))
- separation of management and operational networks (if selected in [FMT_SMO_EXT.1](#))
- [**assignment**: other capabilities]
- no other capabilities

] that is logically distinct from other communication paths and provides assured identification of its endpoints and protection of the communicated data from disclosure and detection of modification of the communicated data.

Application Note: If the ST author selects either TLS or HTTPS, the TSF shall be validated against the [Functional Package for Transport Layer Security \(TLS\), version 2.1](#). This PP does not mandate that a product implement TLS with mutual authentication, but if the product includes the capability to perform TLS with mutual authentication, then mutual authentication must be included within the TOE boundary. The TLS Package requires that the X.509 requirements be included by the PP, so selection of TLS or HTTPS causes [FIA_X509_EXT.*](#) to be

selected.

If the ST author selects SSH, the TSF shall be validated against the [Functional Package for Secure Shell \(SSH\), version 2.0](#).

If the ST author selects "certificate-based authentication of the remote peer," then FIA_X509_EXT.1 and FIA_X509_EXT.2 in the Functional Package for X.509, version 1.0 must be included in the ST. "No authentication of the remote peer" should be selected only if the TOE is acting as a server in a non-mutual authentication configuration.

The ST author must include the security functional requirements for the trusted channel protocol selected in [FTP_ITC_EXT.1](#) in the main body of the ST.

Evaluation Activities ▼

[FTP_ITC_EXT.1.1](#)

TSS

The evaluator will review the TSS to determine that it lists all trusted channels the TOE uses for remote communications, including both the external entities and remote users used for the channel as well as the protocol that is used for each.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator will configure the TOE to communicate with each external IT entity and type of remote user identified in the TSS. The evaluator will monitor network traffic while the VS performs communication with each of these destinations. The evaluator will ensure that for each session a trusted channel was established in conformance with the protocols identified in the selection.

FTP_UIF_EXT.1 User Interface: I/O Focus

FTP_UIF_EXT.1.1

The TSF shall indicate to users which VM, if any, has the current input focus.

Application Note: This requirement applies to all users—whether user or administrator. In environments where multiple VMs run at the same time, the user must have a way of knowing which VM user input is directed to at any given moment. This is especially important in multiple-domain environments.

In the case of a human user, this is usually a visual indicator. In the case of headless VMs, the user is considered to be a program, but this program still needs to know which VM it is sending input to; this would typically be accomplished through programmatic means.

Evaluation Activities ▼

[FTP_UIF_EXT.1.1](#)

TSS

The evaluator shall ensure that the TSS lists the supported user input devices.

Guidance

The evaluator shall ensure that the operational guidance specifies how the current input focus is indicated to the user.

Tests

For each supported input device, the evaluator shall demonstrate that the input from each device listed in the TSS is directed to the VM that is indicated to have the input focus.

FTP_UIF_EXT.2 User Interface: Identification of VM

FTP_UIF_EXT.2.1

The TSF shall support the unique identification of a VM's output display to users.

Application Note: In environments where a user has access to more than one VM at the same time, the user must be able to determine the identity of each VM displayed in order to avoid inadvertent cross-domain data entry.

There must be a mechanism for associating an identifier with a VM so that an application or program displaying the VM can identify the VM to users. This is generally indicated visually for human users (e.g., VM identity in the window title bar) and programmatically for headless VMs (e.g., an API function). The identification must be unique to the VS, but does not need to be universally unique.

Evaluation Activities ▼

FTP_UIF_EXT.2.1**TSS**

The evaluator shall ensure that the TSS describes the mechanism for identifying VMs to the user, how identities are assigned to VMs, and how conflicts are prevented.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall perform the following test:

The evaluator shall attempt to create and start at least three guest VMs on a single display device where the evaluator attempts to assign two of the VMs the same identifier. If the user interface displays different identifiers for each VM, then the requirement is met. Likewise, the requirement is met if the system refuses to create or start a VM when there is already a VM with the same identifier.

5.1.10 TOE Security Functional Requirements Rationale

The following rationale provides justification for each SFR for the TOE, showing that the SFRs are suitable to address the specified threats:

Table 6: SFR Rationale

Threat	Addressed by	Rationale
T.3P_SOFTWARE	FAU_GEN.1	This threat is mitigated by this SFR because the audit events can report potential integrity breaches and attempts.
	FCS_COP.1/Hash	This threat is mitigated by this SFR by implementing cryptographic integrity verification measures.
	FCS_COP.1/KeyedHash	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FCS_COP.1/Sig	This threat is mitigated by this SFR by implementing cryptographic Authenticity verification measures.
	FDP_PPR_EXT.1	This threat is mitigated by this SFR by requiring support for reducing attack surface through disabling access to unneeded physical platform resources.
	FDP_VMS_EXT.1	This threat is mitigated by this SFR by ensuring that authorized data transfers between VMs are done securely.
	FDP_VNC_EXT.1	This threat is mitigated by this SFR by ensuring that network traffic is visible only to VMs configured to be that network.
	FPT_DDI_EXT.1 (Objective)	This threat is mitigated by this SFR by requiring that physical device drivers be isolated other parts of the TOE and from one another (optional).
	FPT_EEM_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use security mechanisms supported by the physical platform.
	FPT_HAS_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use platform-supported virtualization assists to reduce attack surface.
	FPT_HCL_EXT.1	This threat is mitigated by this SFR by requiring that hypercall parameters be validated.
	FPT_ML_EXT.1 (Objective)	This threat is mitigated by this SFR by requiring measured launch of the platform and VMM (objective).
T.DATA_LEAKAGE	FPT_VDP_EXT.1	This threat is mitigated by this SFR by requiring validation of parameter data passed to the hardware abstraction by untrusted VMs.
	FPT_VIV_EXT.1	Ensures that untrusted VMs cannot invoke privileged code without proper hypervisor mediation.
	FAU_GEN.1	This threat is mitigated by this SFR because the audit events can report attempts to breach isolation.
FCS_CKM.6		This threat is mitigated by this SFR by requiring cryptographic key destruction to protect domain data in shared storage.
	FCS_COP.1/Hash	This threat is mitigated by this SFR by implementing

		cryptographic integrity verification measures.
	FCS_COP.1/KeyedHash	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FCS_COP.1/Sig	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FCS_ENT_EXT.1	This threat is mitigated by this SFR by requiring that domains have access to high-quality entropy for cryptographic purposes.
	FDP_PPR_EXT.1	This threat is mitigated by this SFR by requiring support for reducing attack surface through disabling access to unneeded physical platform resources.
	FDP_RIP_EXT.1	This threat is mitigated by this SFR by ensuring that domain data is cleared from memory before memory is re-allocated.
	FDP_RIP_EXT.2	This threat is mitigated by this SFR by ensuring that domain data is cleared from physical storage upon re-allocation of the storage.
	FDP_VMS_EXT.1	This threat is mitigated by this SFR by ensuring that authorized data transfers between VMs are done securely.
	FDP_VNC_EXT.1	This threat is mitigated by this SFR by ensuring that network traffic is visible only to VMs configured to be that network.
	FPT_DVD_EXT.1	This threat is mitigated by this SFR by ensuring that VMs can access only those virtual devices that they are configured to access.
	FPT_EEM_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use security mechanisms supported by the physical platform.
	FPT_GVI_EXT.1 (Optional)	This threat is mitigated by this SFR by requiring that the TOE support guest VM measurements and integrity checks (optional).
	FPT_HAS_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use platform-supported virtualization assists to reduce attack surface.
	FPT_INT_EXT.1 (Objective)	This threat is mitigated by this SFR by requiring that the TOE support introspection into guest VMs (optional).
	FPT_RDM_EXT.1	This threat is mitigated by this SFR by requiring support for rules for switching removable media between domains to reduce the chance of data spillage.
	FPT_VDP_EXT.1	This threat is mitigated by this SFR by requiring validation of parameter data passed to the hardware abstraction by untrusted VMs.
	FPT_VIV_EXT.1	This threat is mitigated by this SFR by ensuring that untrusted VMs cannot invoke privileged code without proper hypervisor mediation.
	FPT_UIF_EXT.1	This threat is mitigated by this SFR by ensuring that users are able to determine the domain with the current input focus.
	FPT_UIF_EXT.2	This threat is mitigated by this SFR by ensuring that users can know the identity of any VM that they can access.
T.DENIAL_OF_SERVICE	FCS_CKM.6	This threat is mitigated by this SFR by requiring cryptographic key destruction to ensure residual data in shared storage is unrecoverable.
	FDP_RIP_EXT.1	This threat is mitigated by this SFR by ensuring that domain data is cleared from memory before memory is re-allocated.
	FDP_RIP_EXT.2	This threat is mitigated by this SFR by ensuring that domain data is cleared from storage upon re-allocation of the storage.
T.MISCONFIGURATION	FDP_VMS_EXT.1	This threat is mitigated by this SFR by ensuring that

		data sharing between VMs is turned off by default.
T.PLATFORM_COMPROMISE	FDP_HBI_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use platform-supported mechanisms for access to physical devices.
	FDP_PPR_EXT.1	This threat is mitigated by this SFR by requiring support for reducing attack surface through disabling access to unneeded physical platform resources.
	FDP_VMS_EXT.1	This threat is mitigated by this SFR by ensuring that authorized data transfers between VMs are done securely.
	FDP_VNC_EXT.1	This threat is mitigated by this SFR by ensuring that network traffic is visible only to VMs configured to be that network.
	FPT_DVD_EXT.1	This threat is mitigated by this SFR by ensuring that VMs cannot access virtual devices that they are not configured to access.
	FPT_EEM_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use security mechanisms supported by the physical platform.
	FPT_HAS_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use platform-supported virtualization assists to reduce attack surface.
	FPT_HCL_EXT.1	This threat is mitigated by this SFR by requiring that hypercall parameters be validated.
	FPT_ML_EXT.1 (Objective)	This threat is mitigated by this SFR by requiring measured launch of the platform and VMM (objective).
	FPT_VDP_EXT.1	This threat is mitigated by this SFR by requiring validation of parameter data passed to the hardware abstraction by untrusted VMs.
	FPT_VIV_EXT.1	This threat is mitigated by this SFR by ensuring that untrusted VMs cannot invoke privileged code without proper hypervisor mediation.
T.UNAUTHORIZED_ACCESS	FAU_GEN.1	This threat is mitigated by this SFR because the audit events can report potential attempts to access the management subsystem.
	FCS_CKM.1	This threat is mitigated by this SFR by requiring generation of strong asymmetric cryptographic keys.
	FCS_CKM.2	This threat is mitigated by this SFR by requiring use of strong cryptographic key establishment algorithms.
	FCS_COP.1/Hash	This threat is mitigated by this SFR by implementing cryptographic integrity verification measures.
	FCS_COP.1/KeyedHash	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FCS_COP.1/Sig	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FCS_COP.1/UDE	This threat is mitigated by this SFR by implementing cryptographic confidentiality measures.
	FCS_HTTPS_EXT.1 (Selection-based)	This threat is mitigated by this SFR by ensuring that HTTPS trusted communications channels are implemented properly.
	FCS_IPSEC_EXT.1 (Selection-based)	This threat is mitigated by this SFR by ensuring that IPsec trusted communications channels are implemented properly.
	FCS_RB.G.1	This threat is mitigated by this SFR by requiring that the TOE uses a cryptographically strong DRBG.
	FCS_RB.G.2 (Selection-based)	This threat is mitigated by this SFR by ensuring that entropy data used for DRBG seeding is sufficiently unpredictable to result in the generation of strong keys.
	FCS_RB.G.3 (Selection-based)	This threat is mitigated by this SFR by ensuring that entropy data used for DRBG seeding is sufficiently unpredictable to result in the generation of strong keys.

	FCS_RBG.4 (Selection-based)	This threat is mitigated by this SFR by ensuring that entropy data used for DRBG seeding is sufficiently unpredictable to result in the generation of strong keys.
	FCS_RBG.5 (Selection-based)	This threat is mitigated by this SFR by ensuring that entropy data used for DRBG seeding is sufficiently unpredictable to result in the generation of strong keys.
	FIA_AFL_EXT.1	This threat is mitigated by this SFR by requiring that the TOE detect failed authentication attempts for administrator access.
	FIA_PMG_EXT.1 (Selection-based)	This threat is mitigated by this SFR by ensuring that password-based administrator login is properly implemented.
	FIA_UAU.5	This threat is mitigated by this SFR by ensuring that strong mechanisms are used for administrator authentication.
	FIA_UIA_EXT.1	This threat is mitigated by this SFR by requiring that administrators be successfully authenticated before performing management functions.
	FIA_X509_EXT.4 (Selection-based)	This threat is mitigated by this SFR by requiring an exception to be met without the need to validate the revocation of the certificate.
	FMT_MOF_EXT.1	This threat is mitigated by this SFR by limiting the management functions to be limited to authorized administrators as managed through controls required by FMT_MOF_EXT.1 .
	FMT_SMO_EXT.1	This threat is mitigated by this SFR by requiring that the TOE support having separate management and operational networks.
	FPT_FLS.1	This threat is mitigated by this SFR by ensuring that the TOE enters a failure state if it is unable to implement its DRBG function to adequately protect data in transit.
	FPT_TST.1	This threat is mitigated by this SFR by requiring self-testing for DRBG functionality to ensure that keys used for protection of data in transit are adequately strong.
	FTA_TAB.1	This threat is mitigated by this SFR by displays advisory notice and consent warning message regarding use of the TOE to administrators.
	FTP_ITC_EXT.1	This threat is mitigated by this SFR by ensuring that trusted communications channels are implemented using good cryptography.
	FTP_TRP.1 (Selection-based)	This threat is mitigated by this SFR by ensuring that certain communications use a trusted path.
T.UNAUTHORIZED_MODIFICATION	FAU_ARP.1 (Optional)	This threat is mitigated by this SFR by requiring support for automatic responses to audit events (optional).
	FAU_GEN.1	This threat is mitigated by this SFR because the audit events can report potential integrity breaches and attempts.
	FAU_SAA.1 (Optional)	This threat is mitigated by this SFR by requiring support for rules for indicating security violations based on audit events (optional).
	FAU_SAR.1	This threat is mitigated by this SFR by requiring support for administrator review of audit records.
	FAU_STG.1	This threat is mitigated by this SFR by requiring support for protected transmission of audit records off the TOE.
	FAU_STG.2	This threat is mitigated by this SFR by requiring protection of stored audit records.
	FCS_CKM.1	This threat is mitigated by this SFR by requiring generation of asymmetric keys for protection of integrity measures.
	FCS_COP.1/Hash	This threat is mitigated by this SFR by implementing cryptographic integrity verification measures.

	FCS_COP.1/KeyedHash	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FCS_COP.1/Sig	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FDP_PPR_EXT.1	This threat is mitigated by this SFR by requiring support for reducing attack surface through disabling access to unneeded physical platform resources.
	FDP_VMS_EXT.1	This threat is mitigated by this SFR by ensuring that authorized data transfers between VMs are done securely.
	FDP_VNC_EXT.1	This threat is mitigated by this SFR by ensuring that network traffic is visible only to VMs configured to be that network.
	FPT_DDI_EXT.1 (Objective)	This threat is mitigated by this SFR by requiring that physical device drivers be isolated other parts of the TOE and from one another (optional).
	FPT_EEM_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use security mechanisms supported by the physical platform.
	FPT_HAS_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use platform-supported virtualization assists to reduce attack surface.
	FPT_HCL_EXT.1	This threat is mitigated by this SFR by requiring that hypercall parameters be validated.
	FPT_ML_EXT.1 (Objective)	This threat is mitigated by this SFR by requiring measured launch of the platform and VMM (objective).
	FPT_VDP_EXT.1	This threat is mitigated by this SFR by requiring validation of parameter data passed to the hardware abstraction by untrusted VMs.
	FPT_VIV_EXT.1	This threat is mitigated by this SFR by ensuring that untrusted VMs cannot invoke privileged code without proper hypervisor mediation.
T.UNAUTHORIZED_UPDATE	FAU_GEN.1	This threat is mitigated by this SFR because the audit events can report potential integrity breaches and attempts.
	FCS_CKM.1	This threat is mitigated by this SFR by requiring generation of asymmetric keys for protection of integrity measures.
	FCS_COP.1/Hash	This threat is mitigated by this SFR by implementing cryptographic integrity verification measures.
	FCS_COP.1/KeyedHash	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FCS_COP.1/Sig	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FDP_PPR_EXT.1	This threat is mitigated by this SFR by requiring support for reducing attack surface through disabling access to unneeded physical platform resources.
	FDP_VMS_EXT.1	This threat is mitigated by this SFR by ensuring that authorized data transfers between VMs are done securely.
	FDP_VNC_EXT.1	This threat is mitigated by this SFR by ensuring that network traffic is visible only to VMs configured to be that network.
	FMT_MOF_EXT.1	This SFR mitigates this threat by ensuring that the only way to modify the VS is through a trusted update process initiated by an authorized administrator as required by FMT_MOF_EXT.1 .
	FPT_DDI_EXT.1 (Objective)	This threat is mitigated by this SFR by requiring that physical device drivers be isolated other parts of the TOE and from one another.
	FPT_EEM_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use security mechanisms supported by the physical platform.

	FPT_HAS_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use platform-supported virtualization assists to reduce attack surface.
	FPT_HCL_EXT.1	This threat is mitigated by this SFR by requiring that hypercall parameters be validated.
	FPT_ML_EXT.1 (Objective)	This threat is mitigated by this SFR by requiring measured launch of the platform and VMM (objective).
	FPT_VDP_EXT.1	This threat is mitigated by this SFR by requiring validation of parameter data passed to the hardware abstraction by untrusted VMs.
	FPT_VIV_EXT.1	This threat is mitigated by this SFR by ensuring that untrusted VMs cannot invoke privileged code without proper hypervisor mediation.
T.UNPATCHED_SOFTWARE	FPT_IDV_EXT.1 (Objective)	This threat is mitigated by this SFR by requiring support for software identification labels (optional).
	FPT_TUD_EXT.1	This threat is mitigated by this SFR by requiring support for product updates.
	FPT_TUD_EXT.2 (Selection-based)	This threat is mitigated by this SFR by requiring specific requirements for certificate-based code signing for update.
T.USER_ERROR	FAU_GEN.1	This threat is mitigated by this SFR because the audit events can report attempts to breach isolation.
	FCS_CKM.6	This threat is mitigated by this SFR by requiring cryptographic key destruction to protect domain data in shared storage.
	FDP_PPR_EXT.1	This threat is mitigated by this SFR by requiring support for reducing attack surface through disabling access to unneeded physical platform resources.
	FDP_RIP_EXT.1	This threat is mitigated by this SFR by ensuring that domain data is cleared from memory before memory is re-allocated.
	FDP_RIP_EXT.2	This threat is mitigated by this SFR by ensuring that domain data is cleared from physical storage upon re-allocation of the storage.
	FDP_VMS_EXT.1	This threat is mitigated by this SFR by ensuring that authorized data transfers between VMs are done securely.
	FDP_VNC_EXT.1	This threat is mitigated by this SFR by ensuring that network traffic is visible only to VMs configured to be that network.
	FPT_DVD_EXT.1	This threat is mitigated by this SFR by ensuring that VMs can access only those virtual devices that they are configured to access.
	FPT_EEM_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use security mechanisms supported by the physical platform.
	FPT_HAS_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use platform-supported virtualization assists to reduce attack surface.
	FPT_VDP_EXT.1	This threat is mitigated by this SFR by requiring validation of parameter data passed to the hardware abstraction by untrusted VMs.
	FPT_VIV_EXT.1	This threat is mitigated by this SFR by ensuring that untrusted VMs cannot invoke privileged code without proper hypervisor mediation.
T.VMM_COMPROMISE	FAU_GEN.1	This threat is mitigated by this SFR because the audit events can report potential integrity breaches and attempts.
	FCS_CKM.6	This threat is mitigated by this SFR by requiring cryptographic key destruction to protect domain data in shared storage.
	FCS_COP.1/Hash	This threat is mitigated by this SFR by implementing

		cryptographic integrity verification measures.
	FCS_COP.1/KeyedHash	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FCS_COP.1/Sig	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FDP_PPR_EXT.1	This threat is mitigated by this SFR by requiring support for reducing attack surface through disabling access to unneeded physical platform resources.
	FDP_RIP_EXT.1	This threat is mitigated by this SFR by ensuring that domain data is cleared from memory before memory is re-allocated.
	FDP_RIP_EXT.2	This threat is mitigated by this SFR by ensuring that domain data is cleared from physical storage upon re-allocation of the storage.
	FDP_VMS_EXT.1	This threat is mitigated by this SFR by ensuring that authorized data transfers between VMs are done securely.
	FDP_VNC_EXT.1	This threat is mitigated by this SFR by ensuring that network traffic is visible only to VMs configured to be that network.
	FPT_DDI_EXT.1 (Objective)	This threat is mitigated by this SFR by requiring that physical device drivers be isolated other parts of the TOE and from one another (optional).
	FPT_DVD_EXT.1	This threat is mitigated by this SFR by ensuring that VMs can access only those virtual devices that they are configured to access.
	FPT_EEM_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use security mechanisms supported by the physical platform.
	FPT_HAS_EXT.1	This threat is mitigated by this SFR by requiring that the TOE use platform-supported virtualization assists to reduce attack surface.
	FPT_HCL_EXT.1	This threat is mitigated by this SFR by requiring that hypercall parameters be validated.
	FPT_ML_EXT.1 (Objective)	This threat is mitigated by this SFR by requiring measured launch of the platform and VMM (objective).
	FPT_VDP_EXT.1	This threat is mitigated by this SFR by requiring validation of parameter data passed to the hardware abstraction by untrusted VMs.
	FPT_VIV_EXT.1	This threat is mitigated by this SFR by ensuring that untrusted VMs cannot invoke privileged code without proper hypervisor mediation.
T.WEAK_CRYPTO	FCS_CKM.1	This threat is mitigated by this SFR by requiring generation of strong asymmetric cryptographic keys.
	FCS_CKM.2	This threat is mitigated by this SFR by requiring use of strong cryptographic key establishment algorithms.
	FCS_COP.1/Hash	This threat is mitigated by this SFR by implementing cryptographic integrity verification measures.
	FCS_COP.1/KeyedHash	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FCS_COP.1/Sig	This threat is mitigated by this SFR by implementing cryptographic authenticity verification measures.
	FCS_COP.1/UDE	This threat is mitigated by this SFR by implementing cryptographic confidentiality measures.
	FCS_ENT_EXT.1	This threat is mitigated by this SFR by requiring that domains have access to high-quality entropy for cryptographic purposes.
	FCS_RB.G.1	This threat is mitigated by this SFR by requiring that the TOE has access to high-quality entropy for cryptographic purposes.
	FCS_RB.G.2 (Selection-based)	This threat is mitigated by this SFR by ensuring that entropy data used for DRBG seeding is sufficiently

	unpredictable to result in the generation of strong keys.
FCS_RBG.3 (Selection-based)	This threat is mitigated by this SFR by ensuring that entropy data used for DRBG seeding is sufficiently unpredictable to result in the generation of strong keys.
FCS_RBG.4 (Selection-based)	This threat is mitigated by this SFR by ensuring that entropy data used for DRBG seeding is sufficiently unpredictable to result in the generation of strong keys.
FCS_RBG.5 (Selection-based)	This threat is mitigated by this SFR by ensuring that entropy data used for DRBG seeding is sufficiently unpredictable to result in the generation of strong keys.
FPT_FLS.1	This threat is mitigated by this SFR by ensuring that the TOE enters a failure state if it is unable to implement its DRBG function to adequately protect data in transit.
FPT_TST.1	This threat is mitigated by this SFR by requiring self-testing for DRBG functionality to ensure that keys used for protection of data in transit are adequately strong.

5.2 Security Assurance Requirements

The Security Objectives for the TOE in Section 4 were constructed to address threats identified in Section 3.1. The Security Functional Requirements (SFRs) in Section 5.1 are a formal instantiation of the Security Objectives. The PP identifies the Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

This section lists the set of Security Assurance Requirements (SARs) from Part 3 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 that are required in evaluations against this PP. Individual evaluation activities to be performed are specified in both Section 5.1 as well as in this section.

After the ST has been approved for evaluation, the Information Technology Security Evaluation Facility (ITSEF) will obtain the TOE, supporting environmental IT, and the administrative/user guides for the TOE. The ITSEF is expected to perform actions mandated by the CEM for the ASE and ALC SARs. The ITSEF also performs the evaluation activities contained within Section 5, which are intended to be an interpretation of the other CEM assurance requirements as they apply to the specific technology instantiated in the TOE. The evaluation activities that are captured in Section 5 also provide clarification as to what the developer needs to provide to demonstrate the TOE is compliant with the PP.

5.2.1 Class ASE: Security Target Evaluation

As per ASE activities defined in [CEM] plus the TSS evaluation activities defined for any SFRs claimed by the TOE.

5.2.2 Class ADV: Development

The information about the TOE is contained in the guidance documentation available to the end user as well as the TOE Summary Specification (TSS) portion of the ST. The TOE developer must concur with the description of the product that is contained in the TSS as it relates to the functional requirements. The evaluation activities contained in Section 5.2 should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

ADV_FSP.1 Basic functional specification

Developer action elements:

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

The developer shall provide a tracing from the functional specification to the SFRs.

Application Note: As indicated in the introduction to this section, the functional specification is composed of the information contained in the AGD_OPR and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. The evaluation activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element [ADV_FSP.1.2D](#) is implicitly already done and no additional documentation is necessary.

Content and presentation elements:

ADV_FSP.1.1C

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

Application Note: There are no specific evaluation activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described in Section 5.2, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other evaluation activities being performed; if the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.

Evaluation Activities ▼

[ADV_FSP.1](#)

5.2.3 Class AGD: Guidance Documents

The guidance documents will be provided with the developer's security target. Guidance must include a description of how the authorized user verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by an authorized user.

Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes

- instructions to successfully install the TOE in that environment; and
- instructions to manage the security of the TOE as a product and as a component of the larger operational environment.

Guidance pertaining to particular security functionality is also provided; specific requirements on such guidance are contained in the evaluation activities specified with individual SFRs where applicable.

AGD_OPE.1 Operational User Guidance

Developer action elements:

AGD_OPE.1.1D

The developer shall provide operational user guidance.

Application Note: Rather than repeat information here, the developer should review the evaluation activities for this component to ascertain the specifics of the guidance that the evaluators will be checking for. This will provide the necessary information for the preparation of acceptable guidance.

Content and presentation elements:

AGD_OPE.1.1C

The operational user guidance shall describe what ~~for each user role-the authorized user~~-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C

The operational user guidance shall describe, for ~~each user role-the authorized user~~, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C

The operational user guidance shall describe, for ~~each user role-the authorized user~~, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C

The operational user guidance shall, for ~~each user role-the authorized user~~, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their

consequences and implications for maintaining secure operation.

AGD_OPE.1.6C

The operational user guidance shall, for each user role—the authorized user, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluation Activities ▼

AGD_OPE.1

Some of the contents of the operational guidance will be verified by the evaluation activities in Section 5.2 and evaluation of the TOE according to the CEM. The following additional information is also required.

The operational guidance shall contain instructions for configuring the password characteristics, number of allowed authentication attempt failures, the lockout period times for inactivity, and the notice and consent warning that is to be provided when authenticating.

The operational guidance shall contain step-by-step instructions suitable for use by an end-user of the VS to configure a new, out-of-the-box system into the configuration evaluated under this Protection Profile.

The documentation shall describe the process for verifying updates to the TOE, either by checking the hash or by verifying a digital signature. The evaluator shall verify that this process includes the following steps:

- Instructions for querying the current version of the TOE software.
- For hashes, a description of where the hash for a given update can be obtained. For digital signatures, instructions for obtaining the certificate that will be used by the FCS_COP.1/SIG mechanism to ensure that a signed update has been received from the certificate owner. This may be supplied with the product initially, or may be obtained by some other means.
- Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).
- Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the hash/digital signature.

AGD_PRE.1 Preparative procedures

Developer action elements:

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

Application Note: As with the operational guidance, the developer should look to the evaluation activities to determine the required content with respect to preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

Evaluation Activities ▼

AGD_PRE.1

As indicated in the introduction above, there are significant expectations with respect to the

documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms (that is, combination of hardware and operating system) claimed for the TOE in the ST.

The operational guidance shall contain step-by-step instructions suitable for use by an end-user of the VS to configure a new, out-of-the-box system into the configuration evaluated under this Protection Profile.

5.2.4 Class ALC: Life-Cycle Support

At the assurance level specified for TOEs conformant to this PP, life-cycle support is limited to an examination of the TOE vendor's development and configuration management process in order to provide a baseline level of assurance that the TOE itself is developed in a secure manner and that the developer has a well-defined process in place to deliver updates to mitigate known security flaws. This is a result of the critical role that a developer's practices play in contributing to the overall trustworthiness of a product.

ALC_CMC.1 Labeling of the TOE

Developer action elements:

ALC_CMC.1.1D

The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMC.1.1C

The TOE shall be labeled with its unique reference.

Evaluator action elements:

ALC_CMC.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluation Activities ▼

ALC_CMC.1

The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST.

The evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST.

If the vendor maintains a website advertising the TOE, the evaluator shall examine the information on the website to ensure that the information in the ST is sufficient to distinguish the product.

ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.1.1C

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

Evaluator action elements:

ALC_CMS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluation Activities ▼

ALC_CMS.1

The evaluator shall ensure that the developer has identified (in public-facing development guidance for their platform) one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the developer shall provide information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment are invoked (e.g., compiler and linker flags). The evaluator shall ensure that this documentation also includes an indication of whether such protections are on by default, or have to be specifically enabled. The

evaluator shall ensure that the TSF is uniquely identified (with respect to other products from the TSF vendor), and that documentation provided by the developer in association with the requirements in the ST is associated with the TSF using this unique identification.

ALC_TSU_EXT.1 Timely Security Updates

This component requires the TOE developer, in conjunction with any other necessary parties, to provide information as to how the VS is updated to address security issues in a timely manner. The documentation describes the process of providing updates to the public from the time a security flaw is reported/discovered, to the time an update is released. This description includes the parties involved (e.g., the developer, hardware vendors) and the steps that are performed (e.g., developer testing), including worst case time periods, before an update is made available to the public.

Developer action elements:

ALC_TSU_EXT.1.1D

The developer shall provide a description in the TSS of how timely security updates are made to the TOE.

Content and presentation elements:

ALC_TSU_EXT.1.1C

The description shall include the process for creating and deploying security updates for the TOE software/firmware.

ALC_TSU_EXT.1.2C

The description shall express the time window as the length of time, in days, between public disclosure of a vulnerability and the public availability of security updates to the TOE.

Application Note: The total length of time may be presented as a summation of the periods of time that each party (e.g., TOE developer, hardware vendor) on the critical path consumes. The time period until public availability per deployment mechanism may differ; each is described.

ALC_TSU_EXT.1.3C

The description shall include the mechanisms publicly available for reporting security issues pertaining to the TOE.

Application Note: The reporting mechanism could include websites, email addresses, and a means to protect the sensitive nature of the report (e.g., public keys that could be used to encrypt the details of a proof-of-concept exploit).

Evaluator action elements:

ALC_TSU_EXT.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluation Activities ▼

ALC_TSU_EXT.1

5.2.5 Class ATE: Tests

Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through the ATE_IND family, while the latter is through the AVA_VAN family. At the assurance level specified in this PP, testing is based on advertised functionality and interfaces with dependency on the availability of design information. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

ATE_IND.1 Independent Testing - Conformance

Testing is performed to confirm the functionality described in the TSS as well as the administrative (including configuration and operation) documentation provided. The focus of the testing is to confirm that the requirements specified in Section 5.1 are being met, although some additional testing is specified for SARs in Section 5.2. The evaluation activities identify the additional testing activities associated with these components. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the platform/TOE combinations that are claiming conformance to this PP.

Developer action elements:

ATE_IND.1.1D

The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C

The TOE shall be suitable for testing.

Evaluator action elements:

ATE_IND.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

Evaluation Activities ▼

ATE_IND.1

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. While it is not necessary to have one test case per test listed in an evaluation activity, the evaluators must document in the test plan that each applicable testing requirement in the ST is covered.

The Test Plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no effect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of cryptographic engines to be used. The cryptographic algorithms implemented by these engines are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS/HTTPS, SSH).

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

5.2.6 Class AVA: Vulnerability Assessment

For the first generation of this Protection Profile, the evaluation lab is expected to survey open sources to learn what vulnerabilities have been discovered in these types of products. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. Until penetration tools are created and uniformly distributed to the evaluation labs, evaluators will not be expected to test for these vulnerabilities in the TOE. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used in the development of penetration testing tools and for the development of future PPs.

AVA_VAN.1 Vulnerability survey

Developer action elements:

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.1.1C

The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

Evaluation Activities ▼

AVA_VAN.1

As with ATE_IND the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in

ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in virtualization in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.

Appendix A - Optional Requirements

As indicated in the introduction to this PP, the baseline requirements (those that must be performed by the TOE) are contained in the body of this PP. This appendix contains three other types of optional requirements:

The first type, defined in Appendix [A.1 Strictly Optional Requirements](#), are strictly optional requirements. If the TOE meets any of these requirements the vendor is encouraged to claim the associated SFRs in the ST, but doing so is not required in order to conform to this PP.

The second type, defined in Appendix [A.2 Objective Requirements](#), are objective requirements. These describe security functionality that is not yet widely available in commercial technology. Objective requirements are not currently mandated by this PP, but will be mandated in the future. Adoption by vendors is encouraged, but claiming these SFRs is not required in order to conform to this PP.

The third type, defined in Appendix [A.3 Implementation-dependent Requirements](#), are Implementation-dependent requirements. If the TOE implements the product features associated with the listed SFRs, either the SFRs must be claimed or the product features must be disabled in the evaluated configuration.

A.1 Strictly Optional Requirements

A.1.1 Auditable Events for Strictly Optional Requirements

Table 7: Auditable Events for Strictly Optional Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FAU_ARP.1	Actions taken due to potential security violations.	No additional information
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms.	No additional information
	Automated responses performed by the TSF.	No additional information
FPT_GVI_EXT.1	Actions taken due to failed integrity check.	No additional information

A.1.2 Class ALC: Life-Cycle Support

ALC_FLR.1 Basic Flaw Remediation (ALC_FLR.1)

This SAR is optional and may be claimed at the ST-Author's discretion.

Developer action elements:

ALC_FLR.1.1D

The developer shall document and provide flaw remediation procedures addressed to TOE developers.

Content and presentation elements:

ALC_FLR.1.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

Evaluator action elements:

ALC_FLR.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluation Activities ▼

ALC_FLR.1

The evaluator shall inspect the TSS and verify it identifies how to access the flaw remediation procedures.

ALC_FLR.2 Flaw Reporting Procedures (ALC_FLR.2)

This SAR is optional and may be claimed at the ST-Author's discretion.

Developer action elements:

ALC_FLR.2.1D

The developer shall document and provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D

The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D

The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation elements:

ALC_FLR.2.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C

The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C

The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C

The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C

The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

Evaluator action elements:

ALC_FLR.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluation Activities ▼

ALC_FLR.2

The evaluator shall inspect the TSS and verify it identifies how to access the flaw remediation procedures.

The evaluator shall inspect the guidance document and verify it describes how to access the flaw remediation guidance.

ALC_FLR.3 Systematic Flaw Remediation (ALC_FLR.3)

This SAR is optional and may be claimed at the ST-Author's discretion.

Developer action elements:

ALC_FLR.3.1D

The developer shall document and provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.3.2D

The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.3.3D

The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation elements:

ALC_FLR.3.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.3.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.3.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.3.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.3.5C

The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.3.6C

The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

ALC_FLR.3.7C

The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.3.8C

The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.3.9C

The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

ALC_FLR.3.10C

The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.

ALC_FLR.3.11C

The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.

Evaluator action elements:

ALC_FLR.3.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Evaluation Activities ▼

ALC_FLR.3

The evaluator shall inspect the TSS and verify it identifies how to access the flaw remediation procedures.

The evaluator shall inspect the guidance document and verify it describes how to access the flaw remediation guidance.

A.1.3 Security Audit (FAU)

FAU_ARP.1 Security Audit Automatic Response

FAU_ARP.1.1

The TSF shall take [**assignment: list of actions**] upon detection of a potential security violation.

Application Note: In certain cases, it may be useful for virtualization systems

to perform automated responses to certain security events. An example may include halting a VM which has taken some action to violate a key system security policy. This may be especially useful with headless endpoints when there is no human user in the loop.

The potential security violation mentioned in FAU_ARP.1.1 refers to FAU_SAA.1.

Evaluation Activities ▼

FAU_ARP.1.1

TSS

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall generate a potential security violation as defined in FAU_SAA.1 and verify that each action in the assignment in FAU_ARP.1.1 is performed by the TSF as a result. The evaluator shall perform this action for each security violation that is defined in FAU_SAA.1.

FAU_SAA.1 Potential Violation Analysis

FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2

The TSF shall enforce the following rules for monitoring audited events:

1. Accumulation or combination of [**assignment**: *subset of defined auditable events*] known to indicate a potential security violation;
2. [**assignment**: *any other rules*].

Application Note: The potential security violation described in FAU_SAA.1 can be used as a trigger for automated responses as defined in FAU_ARP.1.

Evaluation Activities ▼

FAU_SAA.1.1

TSS

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall cause each combination of auditable events defined in FAU_SAA.1.2 to occur, and verify that a potential security violation is indicated by the TSF.

A.1.4 Protection of the TSF (FPT)

FPT_GVI_EXT.1 guest VM Integrity

FPT_GVI_EXT.1.1

The TSF shall verify the integrity of guest VMs through the following mechanisms: [**assignment**: *list of guest VM integrity mechanisms*].

Application Note: The primary purpose of this requirement is to identify and describe the mechanisms used to verify the integrity of guest VMs that have been 'imported' in some fashion, though these mechanisms could also be applied to all guest VMs, depending on the mechanism used. Importation for this requirement could include VM migration (live or otherwise), the importation of virtual disk files that were previously exported, VMs in shared storage, etc. It is possible that a trusted VM could have been modified during the migration or import/export process, or VMs could have been obtained from untrusted sources in the first place, so integrity checks on these VMs can be a prudent measure to take. These integrity checks could be as thorough as making sure the entire VM exactly matches a previously known VM (by hash for example), or by simply checking certain configuration settings to ensure that the VM's configuration will not violate the security model of the VS.

Evaluation Activities ▼

FPT_GVI_EXT.1.1

TSS

For each mechanism listed in the assignment, the evaluator shall ensure that the TSS documents the mechanism, including how it verifies VM integrity, which set of guest VMs it will check (all guest VMs, only migrated VMs, etc.), when such checks occur (before VM startup, immediately following importation/migration, on demand, etc.), and which actions are taken if a VM fails the integrity check (or which range of actions are possible if the action is configurable).

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

There are no test activities for this element.

A.2 Objective Requirements

A.2.1 Auditable Events for Objective Requirements

Table 8: Auditable Events for Objective Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FPT_DDI_EXT.1	No events specified	N/A
FPT_IDV_EXT.1	No events specified	N/A
FPT_INT_EXT.1	Introspection initiated/enabled.	The VM introspected.
FPT_ML_EXT.1	Integrity initiated/enabled.	Integrity measurement values.

A.2.2 Protection of the TSF (FPT)

FPT_DDI_EXT.1 Device Driver Isolation

FPT_DDI_EXT.1.1

The TSF shall ensure that device drivers for physical devices are isolated from the VMM and all other domains.

Application Note: In order to function on physical hardware, the VMM must have access to the device drivers for the physical platform on which it runs. These drivers are often written by third parties, and yet are effectively a part of the VMM. Thus the integrity of the VMM in part depends on the quality of third party code that the virtualization vendor has no control over. By encapsulating these drivers within one or more dedicated driver domains (e.g., Service VM or VMs) the damage of a driver failure or vulnerability can be contained within the domain, and would not compromise the VMM. When driver domains have exclusive access to a physical device, hardware isolation mechanisms, such as Intel's VT-d, AMD's Input/Output Memory Management Unit (IOMMU), or ARM's System Memory Management Unit (MMU) should be used to ensure that operations performed by Direct Memory Access (DMA) hardware are properly constrained.

Evaluation Activities ▼

FPT_DDI_EXT.1.1

TSS

The evaluator shall examine the TSS documentation to verify that it describes the mechanism used for device driver isolation. If the TSS document indicates that a hardware isolation mechanism is used, the evaluator shall verify that the TSS documentation enumerates the hardware-isolated DMA-capable devices, and that it also provides a complete list of the accessible targets for memory transactions for each of those DMA-capable devices. (An example of information that might be included in the TSS documentation: a listing of all pages belonging to the driver domain, the identification of a subset of the driver domain's pages that the driver domain has permitted the device access to, or the identification of a dedicated area of memory reserved for the device or driver domain).

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

There are no test activities for this element.

FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1

The TSF shall include software identification (SWID) tags that contain a SoftwareIdentity element and an Entity element as defined in ISO/IEC 19770-2:2009.

FPT_IDV_EXT.1.2

The TSF shall store SWIDs in a .swidtag file as defined in ISO/IEC 19770-2:2009.

Application Note: SWID tags are XML files embedded within software that provide a standard method for IT departments to track and manage the software. The presence of SWIDs can greatly simplify the software management process and improve security by enhancing the ability of IT departments to manage updates.

Evaluation Activities ▼

[FPT_IDV_EXT.1.1](#)

TSS

The evaluator shall examine the TSS to ensure it describes how SWID tags are implemented and the format of the tags. The evaluator shall verify that the format complies with [FPT_IDV_EXT.1.1](#) and that SWIDs are stored in accordance with [FPT_IDV_EXT.1.2](#).

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall perform the following test:

- *Test FPT_IDV_EXT.1.1:1: The evaluator shall check for the existence of SWID tags in a .swidtag file. The evaluator shall open the file and verify that each SWID contains at least a SoftwareIdentity element and an Entity element.*

FPT_INT_EXT.1 Support for Introspection

FPT_INT_EXT.1.1

The TSF shall support a mechanism for permitting the VMM or privileged VMs to access the internals of another VM for purposes of introspection.

Application Note: Introspection can be used to support malware and anomaly detection from outside of the guest environment. This not only helps protect the guest OS, it also protects the VS by providing an opportunity for the VS to detect threats to itself that originate within VMs, and that may attempt to break out of the VM and compromise the VMM or other VMs.

The hosting of malware detection software outside of the guest VM helps protect the guest and helps ensure the integrity of the malware detection/antivirus software. This capability can be implemented in the VMM itself, but ideally it should be hosted by a Service VM so that it can be better contained and does not introduce bugs into the VMM.

Evaluation Activities ▼

[FPT_INT_EXT.1.1](#)

TSS

The evaluator shall examine the TSS documentation to verify that it describes the interface for VM introspection and whether the introspection is performed by the VMM or another VM.

Guidance

The evaluator shall examine the operational guidance to ensure that it contains instructions for configuration of the introspection mechanism.

Tests

There are no test activities for this element.

FPT_ML_EXT.1 Measured Launch of Platform and VMM

FPT_ML_EXT.1.1

The TSF shall support a measured launch of the virtualization system. Measured components of the VS shall include the static executable image of the hypervisor and: [selection]:

- *Static executable images of the Management Subsystem*
- *[assignment: list of (static images of) Service VMs]*
- *[assignment: list of configuration files]*
- *no other components*

[]

FPT_ML_EXT.1.2

The TSF shall make the measurements selected in [FPT_ML_EXT.1.1](#) available to the Management Subsystem.

Application Note: A measured launch of the platform and VS demonstrates that the proper TOE software was loaded. A measured launch process employs verifiable integrity measurement mechanisms. For example, a VS may hash components such as the hypervisor, service VMs, or the Management

Subsystem. A measured launch process only allows components to be executed after the measurement has been recorded. An example process may add each component's hash before it is executed so that the final hash reflects the evidence of a component's state prior to execution. The measurement may be verified as the system boots, but this is not required.

The Platform is outside of the TOE. However, this requirement specifies that the VS must be capable of receiving Platform measurements if the Platform provides them. This requirement is requiring TOE support for Platform measurements if provided; it is not placing a requirement on the Platform to take such measurements.

If available, hardware should be used to store measurements in such a manner that they cannot be modified in any manner except to be extended. These measurements should be produced in a repeatable manner so that a third party can verify the measurements if given the inputs. Hardware devices, like Trusted Platform Modules (TPM), TrustZone, and MMU are some examples that may serve as foundations for storing and reporting measurements.

Platforms with a root of trust for measurement (RTM) should initiate the measured launch process. This may include core BIOS or the chipset. The chipset is the preferred RTM, but core BIOS or other firmware is acceptable. In a system without a traditional RTM, the first component that boots would be considered the RTM, this is not preferred.

Evaluation Activities ▼

FPT_ML_EXT.1.1

TSS

The evaluator shall verify that the TSS or Operational Guidance describes how integrity measurements are performed and made available to the Management Subsystem.

Guidance

The evaluator shall examine the operational guidance to verify that it documents how to access the measurements in the Management Subsystem.

Tests

The evaluator shall perform the following test:

- *Test FPT_ML_EXT.1.1:1: The evaluator shall start the VS, login as an administrator, and verify that the measurements for the specified components are viewable in the Management Subsystem.*

A.3 Implementation-dependent Requirements

This PP does not define any Implementation-dependent requirements.

Appendix B - Selection-based Requirements

As indicated in the introduction to this PP, the baseline requirements (those that must be performed by the TOE or its underlying platform) are contained in the body of this PP. There are additional requirements based on selections in the body of the PP: if certain selections are made, then additional requirements below must be included.

B.1 Auditable Events for Selection-based Requirements

Table 9: Auditable Events for Selection-based Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	<ul style="list-style-type: none">• Reason for failure.• Non-TOE endpoint of connection (IP address) for failures.
	Establishment/Termination of a HTTPS session.	Non-TOE endpoint of connection (IP address).
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	<ul style="list-style-type: none">• Reason for failure.• Non-TOE endpoint of connection (IP address).
	Establishment/Termination of an IPsec SA.	Non-TOE endpoint of connection (IP address).
FCS_RB.G.2	No events specified	N/A
FCS_RB.G.3	No events specified	N/A
FCS_RB.G.4	No events specified	N/A
FCS_RB.G.5	No events specified	N/A
FIA_PMG_EXT.1	No events specified	N/A
FIA_X509_EXT.4	No events specified	N/A
FPT_TUD_EXT.2	No events specified	N/A
FTP_TRP.1	Initiation of the trusted channel.	User ID and remote source (IP Address) if feasible.
	Termination of the trusted channel.	User ID and remote source (IP Address) if feasible.
	Failures of the trusted path functions.	User ID and remote source (IP Address) if feasible.

B.2 Cryptographic Support (FCS)

FCS_HTTPS_EXT.1 HTTPS Protocol

The inclusion of this selection-based component depends upon selection in FPT_ITC_EXT.1.1.

FCS_HTTPS_EXT.1.1

The TSF shall implement the HTTPS protocol that complies with RFC 2818.

Application Note: This SFR is included in the ST if the ST author selects "TLS/HTTPS" in [FTP_ITC_EXT.1.1](#).

The ST author must provide enough detail to determine how the implementation is complying with the standards identified; this can be done either by adding elements to this component, or by additional detail in the TSS.

FCS_HTTPS_EXT.1.2

The TSF shall implement HTTPS using TLS.

Evaluation Activities ▼

[FCS_HTTPS_EXT.1.1](#) TSS

The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol vs.

security administrator authentication which may be done at a different level of the processing stack.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

Testing for this activity is done as part of the TLS testing; this may result in additional testing if the TLS tests are done at the TLS protocol level.

FCS_IPSEC_EXT.1 IPsec Protocol

The inclusion of this selection-based component depends upon selection in FPT_ITC_EXT.1.1.

FCS_IPSEC_EXT.1.1

The TSF shall implement the IPsec architecture as specified in RFC 4301.

Application Note: This SFR is included in the ST if the ST author selected "IPsec" in [FPT_ITC_EXT.1.1](#).

RFC 4301 calls for an IPsec implementation to protect IP traffic through the use of a Security Policy Database (SPD). The SPD is used to define how IP packets are to be handled: PROTECT the packet (e.g., encrypt the packet), BYPASS the IPsec services (e.g., no encryption), or DISCARD the packet (e.g., drop the packet). The SPD can be implemented in various ways, including router access control lists, firewall rule-sets, a "traditional" SPD, etc. Regardless of the implementation details, there is a notion of a "rule" that a packet is "matched" against and a resulting action that takes place.

While there must be a means to order the rules, a general approach to ordering is not mandated, as long as the TOE can distinguish the IP packets and apply the rules accordingly. There may be multiple SPDs (one for each network interface), but this is not required.

FCS_IPSEC_EXT.1.2

The TSF shall implement [**selection: transport mode, tunnel mode**].

Application Note: If the TOE is used to connect to a VPN gateway for the purposes of establishing a secure connection to a private network, the ST author shall select tunnel mode. If the TOE uses IPsec to establish an end-to-end connection to another IPsec VPN Client, the ST author shall select transport mode. If the TOE uses IPsec to establish a connection to a specific endpoint device for the purpose of secure remote administration, the ST author shall select transport mode.

FCS_IPSEC_EXT.1.3

The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4

The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [*AES-GCM-256 (as specified in RFC 4106)*] together with a Secure Hash Algorithm (SHA)-based HMAC.

FCS_IPSEC_EXT.1.5

The TSF shall implement the protocol:

[*IKEv2 as defined in RFC 7296 (with mandatory support for NAT traversal as specified in section 2.23), RFC 8784, RFC 8247, and [RFC 4868 for hash functions]*].

FCS_IPSEC_EXT.1.6

The TSF shall ensure the encrypted payload in the [*IKEv2*] protocol uses the cryptographic algorithms [*AES-GCM-256 as specified in RFC 5282*] and no other algorithm.

FCS_IPSEC_EXT.1.7

The TSF shall ensure that [*IKEv2 SA lifetimes can be configured by [selection: an administrator, a VPN Gateway] based on [selection: number of packets/number of bytes, length of time]*]].

Application Note: The ST author is afforded a selection based on which entity is responsible for "configuring" the life of the SA. An implementation that allows an administrator to configure the client or a VPN gateway that pushes the SA lifetime down to the client are both acceptable.

As far as SA lifetimes are concerned, the TOE can limit the lifetime based on the number of bytes transmitted, or the number of packets transmitted. Either packet-based or volume-based SA lifetimes are acceptable; the ST author makes the appropriate selection to indicate which type of lifetime limits are supported.

For IKEv2, there are no hard-coded limits on SA lifetime; therefore it is required that an administrator be able to configure the values. In general, instructions for

setting the parameters of the implementation, including lifetime of the SAs, should be included in the operational guidance generated for AGD_OPE. It is appropriate to refine the requirement in terms of number of MB/KB instead of number of packets, as long as the TOE is capable of setting a limit on the amount of traffic that is protected by the same key (the total volume of all IPsec traffic protected by that key).

FCS_IPSEC_EXT.1.8

The TSF shall ensure that all IKE protocols implement DH groups [19 (256-bit Random ECP), 20 (384-bit Random ECP), and **[selection]: 15 (3072-bit MODP), no other DH groups**].

Application Note: The selection is used to specify additional DH groups supported. This applies to all IKE exchanges. It should be noted that if any additional DH groups are specified, they must comply with the requirements (in terms of the ephemeral keys that are established) listed in FCS_CKM.1.

Since the implementation may allow different Diffie-Hellman groups to be negotiated for use in forming the SAs, the assignments in FCS_IPSEC_EXT.1.9 and FCS_IPSEC_EXT.1.10 may contain multiple values. For each DH group supported, the ST author consults Table 2 in 800-57 to determine the "bits of security" associated with the DH group. Each unique value is then used to fill in the assignment (for 1.9 they are doubled; for 1.10 they are inserted directly into the assignment). For example, suppose the implementation supports group 20 (ECDH using NIST curve P-384). From Table 2, the bits of security value for group 14 is 112, and for group 20 it is 192. For FCS_IPSEC_EXT.1.9, then, the assignment would read "[224, 384]" and for FCS_IPSEC_EXT.1.10 it would read "[112, 192]" (although in this case the requirement should probably be refined so that it makes sense mathematically).

FCS_IPSEC_EXT.1.9

The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange (" x " in $gx \bmod p$) using the random bit generator specified in FCS_RB.G.1, and having a length of at least **[assignment]: (one or more) number of bits that is at least twice the "bits of security" value associated with the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, Recommendation for Key Management - Part 1: General** bits.

FCS_IPSEC_EXT.1.10

The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life of a specific IPsec SA is less than 1 in $2^{\lceil \text{[assignment]: (one or more) "bits of security" value associated with the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, Recommendation for Key Management - Part 1: General} \rceil}$.

FCS_IPSEC_EXT.1.11

The TSF shall ensure that the IKE protocol performs peer authentication using a **[selection]: RSA, ECDSA** that use X.509v3 certificates that conform to RFC 4945 and **[selection]: Pre-shared Keys, no other method**.

Application Note: At least one public-key-based Peer Authentication method is required in order to conform to this PP; one or more of the public key schemes is chosen by the ST author to reflect what is implemented. The ST author also ensures that appropriate FCS requirements reflecting the algorithms used (and key generation capabilities, if provided) are listed to support those methods. Note that the TSS will elaborate on the way in which these algorithms are to be used (for example, 2409 specifies three authentication methods using public keys; each one supported will be described in the TSS).

If "pre-shared keys" is selected, the selection-based requirement FIA_PSK_EXT.1 must be claimed.

FCS_IPSEC_EXT.1.12

The TSF shall not establish an SA if the **[selection]: IP address, Fully Qualified Domain Name (FQDN), user FQDN, Distinguished Name (DN)** and **[selection]: no other reference identifier type, [assignment]: other supported reference identifier types**] contained in a certificate does not match the expected values for the entity attempting to establish a connection.

Application Note: The TOE must support at least one of the following identifier types: IP address, Fully Qualified Domain Name (FQDN), user FQDN, or Distinguished Name (DN). In the future, the TOE will be required to support all of these identifier types. The TOE is expected to support as many IP address formats (IPv4 and IPv6) as IP versions supported by the TOE in general. The ST author may assign additional supported identifier types in the second selection.

FCS_IPSEC_EXT.1.13

The TSF shall not establish an SA if the presented identifier does not match the configured reference identifier of the peer.

Application Note: At this time, only the comparison between the presented identifier in the peer's certificate and the peer's reference identifier is mandated by the testing below. However, in the future, this requirement will address two aspects of the peer certificate validation: 1) comparison of the peer's ID payload to the peer's certificate which are both presented identifiers, as required by RFC

4945 and 2) verification that the peer identified by the ID payload and the certificate is the peer expected by the TOE (per the reference identifier). At that time, the TOE will be required to demonstrate both aspects (i.e. that the TOE enforces that the peer's ID payload matches the peer's certificate which both match configured peer reference identifiers).

Excluding the DN identifier type (which is necessarily the Subject DN in the peer certificate), the TOE may support the identifier in either the Common Name or Subject Alternative Name (SAN) or both. If both are supported, the preferred logic is to compare the reference identifier to a presented SAN, and only if the peer's certificate does not contain a SAN, to fall back to a comparison against the Common Name. In the future, the TOE will be required to compare the reference identifier to the presented identifier in the SAN only, ignoring the Common Name.

The configuration of the peer reference identifier is addressed by FMT_SMF.1.1/VPN.

FCS_IPSEC_EXT.1.14

The [selection: TSF, VPN Gateway] shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv2 CHILD_SA] connection.

Application Note: If this functionality is configurable, the TSF may be configured by a VPN Gateway or by an administrator of the TOE itself.

While it is acceptable for this capability to be configurable, the default configuration in the evaluated configuration (either "out of the box" or by configuration guidance in the AGD documentation) must enable this functionality.

Evaluation Activities ▼

FCS_IPSEC_EXT.1.1

TSS

In addition to the TSS EAs for the individual FCS_IPSEC_EXT.1 elements below, the evaluator shall perform the following:

If the TOE boundary includes a general-purpose operating system or mobile device, the evaluator shall examine the TSS to ensure that it describes whether the VPN client capability is architecturally integrated with the platform itself or whether it is a separate executable that is bundled with the platform.

Guidance

In addition to the Operational Guidance EAs for the individual FCS_IPSEC_EXT.1 elements below, the evaluator shall perform the following:

If the configuration of the IPsec behavior is from an environmental source, most notably a VPN gateway (e.g., through receipt of required connection parameters from a VPN gateway), the evaluator shall ensure that the operational guidance contains any appropriate information for ensuring that this configuration can be properly applied.

Note in this case that the implementation of the IPsec protocol must be enforced entirely within the TOE boundary; i.e. it is not permissible for a software application TOE to be a graphical front-end for IPsec functionality implemented totally or in part by the underlying OS platform. The behavior referenced here is for the possibility that the configuration of the IPsec connection is initiated from outside the TOE, which is permissible so long as the TSF is solely responsible for enforcing the configured behavior. However, it is allowable for the TSF to rely on low-level platform-provided networking functions to implement the SPD from the client (e.g., enforcement of packet routing decisions).

Tests

As a prerequisite for performing the Test EAs for the individual FCS_IPSEC_EXT.1 elements below, the evaluator shall do the following:

The evaluator shall minimally create a test environment equivalent to the test environment illustrated below. The traffic generator used to construct network packets should provide the evaluator with the ability manipulate fields in the ICMP, IPv4, IPv6, UDP, and TCP packet headers. The evaluator shall provide justification for any differences in the test environment.

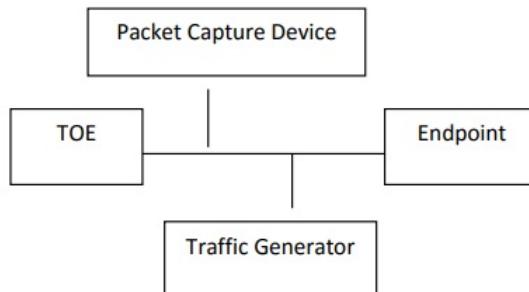


Figure 2: IPsec Test Environment

Note that the evaluator shall perform all tests using the virtualization system and a representative sample of platforms listed in the ST (for TOEs that claim to support multiple platforms).

FCS_IPSEC_EXT.1.1

TSS

The evaluator shall examine the TSS and determine that it describes how the IPsec capabilities are implemented.

The evaluator shall ensure that the TSS describes at a high level the architectural relationship between the IPsec implementation and the rest of the TOE (e.g., is the IPsec implementation an integrated part of the VS or is it a standalone executable that is bundled into the VS).

The evaluator shall ensure that the TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after matching a rule. The TSS describes how the available rules and actions form the SPD using terms defined in RFC 4301 such as BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet), and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.

As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.

Guidance

The evaluator shall examine the operational guidance to verify it instructs the administrator how to construct entries into the SPD that specify a rule for processing a packet. The description includes all three cases – a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without being encrypted. The evaluator shall determine that the description in the operational guidance is consistent with the description in the TSS, and that the level of detail in the operational guidance is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.

Tests

The evaluator uses the operational guidance to configure the TOE to carry out the following tests:

- **Test FCS_IPSEC_EXT.1.1.1:** The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule (e.g., a packet that matches the rule and another that does not match the rule). The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed to flow without modification, encrypted by the IPsec implementation.
- **Test FCS_IPSEC_EXT.1.1.2:** The evaluator shall devise several tests that cover a variety of scenarios for packet processing. As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These scenarios shall exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and operational guidance. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the operational guidance.

FCS_IPSEC_EXT.1.2

TSS

The evaluator checks the TSS to ensure it states that an IPsec VPN can be established to operate in tunnel mode or transport mode (as selected).

Guidance

The evaluator shall confirm that the operational guidance contains instructions on how to configure the connection in each mode selected.

If both transport mode and tunnel mode are implemented, the evaluator shall review the operational guidance to determine how the use of a given mode is specified.

Tests

The evaluator shall perform the following tests based on the selections chosen:

- **Test FCS_IPSEC_EXT.1.2.1: (conditional):** If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE/platform to operate in tunnel mode and also configures a VPN peer to operate in tunnel mode. The evaluator configures the TOE/platform and the VPN peer to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the TOE/Platform to the VPN peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.
- **Test FCS_IPSEC_EXT.1.2.2: (conditional):** If transport mode is selected, the evaluator uses

the operational guidance to configure the TOE/platform to operate in transport mode and also configures a VPN peer to operate in transport mode. The evaluator configures the TOE/platform and the VPN peer to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection from the TOE/platform to connect to the VPN peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.

FCS_IPSEC_EXT.1.3

TSS

The evaluator shall examine the TSS to verify that the TSS provides a description of how a packet is processed against the SPD and that if no “rules” are found to match, that a final rule exists, either implicitly or explicitly, that causes the network packet to be discarded.

Guidance

The evaluator shall check that the operational guidance provides instructions on how to construct or acquire the SPD and uses the guidance to configure the TOE for the following test.

Tests

The evaluator shall perform the following test:

- *Test FCS_IPSEC_EXT.1.3:1: The evaluator shall configure the SPD such that it has entries that contain operations that DISCARD, PROTECT, and (if applicable) BYPASS network packets. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches a BYPASS entry and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a “TOE-created” final entry that discards packets that do not match any previous entries). The evaluator sends the packet, and observes that the packet was not permitted to flow to any of the TOE’s interfaces.*

FCS_IPSEC_EXT.1.4

TSS

The evaluator shall examine the TSS to verify that the algorithm AES-GCM-256 is implemented.

Guidance

The evaluator checks the operational guidance to ensure it provides instructions on how the TOE is configured to use the algorithm selected in this component and whether this is performed through the TOE’s default configuration (i.e., no configuration is necessary), direct configuration of the TOE, configuration defined during initial installation of the TOE, or defined by acquiring configuration settings from an environmental component.

Tests

- *Test FCS_IPSEC_EXT.1.4:1: The evaluator shall configure the TOE/platform as indicated in the operational guidance configuring the TOE/platform to use the supported algorithm, attempt to establish a connection using ESP, and verify that the attempt succeeds.*

FCS_IPSEC_EXT.1.5

TSS

The evaluator shall examine the TSS to verify that IKEv2 is implemented.

Guidance

The evaluator shall check the operational guidance to ensure it instructs the administrator on how to configure the TOE to support only IKEv2 (if necessary), and how to configure the TOE to perform NAT traversal for the test below.

Tests

Tests are performed in conjunction with the other IPsec evaluation activities with the exception of the activities below:

- *Test FCS_IPSEC_EXT.1.5:1: The evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 7296, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed.*
- *Test FCS_IPSEC_EXT.1.5:2: The evaluator shall configure a remote peer to support IKEv1 only. If the TOE’s supported versions of IKE is configurable, the evaluator shall follow the instructions specified in the operational guidance to ensure that only IKEv2 is supported. The evaluator shall then attempt to establish a connection between the TOE and that peer and verify the TSF rejects the connection attempt based on its lack of support for IKEv1.*

FCS_IPSEC_EXT.1.6

TSS

The evaluator shall ensure the TSS identifies the algorithm used for encrypting the IKEv2 payload, and that the algorithm AES-GCM-256 IS specified.

Guidance

The evaluator checks the operational guidance to ensure it provides instructions on how the TOE is configured to use the algorithm selected in this component and whether this is performed through the TOE’s default configuration (i.e., no configuration is necessary), direct configuration of the TOE, configuration defined during initial installation of the TOE, or defined by acquiring configuration settings from an environmental component.

Tests

The evaluator shall use the operational guidance to configure the TOE (or to configure the Operational Environment to have the TOE receive configuration) to perform the following test

for each ciphersuite selected:

- Test FCS_IPSEC_EXT.1.6:1: The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation. The evaluator will confirm that the connection is successful by confirming that data can be passed through the connection once it is established. For example, the evaluator may connect to a web page on the remote network and verify that it can be reached.

[FCS_IPSEC_EXT.1.7](#)

TSS

There are no additional TSS evaluation activities for this element.

Guidance

The evaluator shall check the operational guidance to ensure it provides instructions on how the TOE configures the values for SA lifetimes. In addition, the evaluator shall check that the guidance has the option for either the administrator or VPN Gateway to configure Phase 1 SAs if time-based limits are supported. Currently there are no values mandated for the number of packets or number of bytes, the evaluator shall simply check the operational guidance to ensure that this can be configured if selected in the requirement.

Tests

When testing this functionality, the evaluator needs to ensure that both sides are configured appropriately. From the RFC "In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered."

Each of the following tests shall be performed:

- Test FCS_IPSEC_EXT.1.7:1: (conditional) The evaluator shall configure a maximum lifetime in terms of the # of packets (or bytes) allowed following the operational guidance. The evaluator shall establish an SA and determine that once the allowed # of packets (or bytes) through this SA is exceeded, the connection is closed.
- Test FCS_IPSEC_EXT.1.7:2: (conditional) The evaluator shall construct a test where an IKEv2 IKE_SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.
- Test FCS_IPSEC_EXT.1.7:3: (conditional) The evaluator shall perform a test similar to Test 2 for Child SAs, except that the lifetime will be 8 hours or less instead of 24 hours or less.

[FCS_IPSEC_EXT.1.8](#)

TSS

The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator shall perform the following test:

- Test FCS_IPSEC_EXT.1.8:1: For each supported DH group, the evaluator shall test to ensure that IKEv2 can be successfully completed using that particular DH group.

[FCS_IPSEC_EXT.1.9](#)

TSS

The evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating "x" (as defined in [FCS_IPSEC_EXT.1.9](#)) and each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of "x" and the nonces meet the stipulations in the requirement.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

There are no test activities for this element.

[FCS_IPSEC_EXT.1.10](#)

EAs for this element are tested through EAs for [FCS_IPSEC_EXT.1.9](#).

[FCS_IPSEC_EXT.1.11](#)

TSS

The evaluator ensures that the TSS identifies RSA or ECDSA as being used to perform peer authentication.

If pre-shared keys are chosen in the selection, the evaluator shall check to ensure that the TSS describes how pre-shared keys are established and used in authentication of IPsec connections. The description in the TSS shall also indicate how pre-shared key establishment is accomplished

depending on whether the TSF can generate a pre-shared key, accept a pre-shared key, or both.

The evaluator shall ensure that the TSS describes how the TOE compares the peer's presented identifier to the reference identifier. This description shall include whether the certificate presented identifier is compared to the ID payload presented identifier, which fields of the certificate are used as the presented identifier (DN, Common Name, or SAN) and, if multiple fields are supported, the logical order comparison. If the ST author assigned an additional identifier type, the TSS description shall also include a description of that type and the method by which that type is compared to the peer's presented certificate.

Guidance

The evaluator shall check that the operational guidance describes how pre-shared keys are to be generated and established.

The evaluator ensures the operational guidance describes how to set up the TOE to use the cryptographic algorithms RSA or ECDSA (as selected).

In order to construct the environment and configure the TOE for the following tests, the evaluator shall ensure that the operational guidance also describes how to configure the TOE to connect to a trusted CA, and ensure a valid certificate for that CA is loaded into the TOE as a trusted CA.

The evaluator shall also ensure that the operational guidance includes the configuration of the reference identifiers for the peer.

Tests

For efficiency's sake, the testing that is performed here has been combined with the testing for FIA_X509_EXT.2 and FIA_X509_EXT.3 in the Functional Package for X.509, version 1.0 (for IPsec connections and depending on the Base-PP), [FCS_IPSEC_EXT.1.12](#), and [FCS_IPSEC_EXT.1.13](#). The following tests shall be repeated for each peer authentication protocol selected in the [FCS_IPSEC_EXT.1.11](#) selection above:

- Test FCS_IPSEC_EXT.1.11.1: The evaluator shall have the TOE generate a public-private key pair, and submit a CSR (Certificate Signing Request) to a CA (trusted by both the TOE and the peer VPN used to establish a connection) for its signature. The values for the DN (Common Name, Organization, Organizational Unit, and Country) will also be passed in the request. Alternatively, the evaluator may import to the TOE a previously generated private key and corresponding certificate.
- Test FCS_IPSEC_EXT.1.11.2: The evaluator shall configure the TOE to use a private key and associated certificate signed by a trusted CA and shall establish an IPsec connection with the peer.
- Test FCS_IPSEC_EXT.1.11.3: The evaluator shall test that the TOE can properly handle revoked certificates - conditional on whether CRL or OCSP is selected; if both are selected, and then a test is performed for each method. For this current version of the PP, the evaluator has to only test one up in the trust chain (future drafts may require to ensure the validation is done up the entire chain). The evaluator shall ensure that a valid certificate is used, and that the SA is established. The evaluator then attempts the test with a certificate that will be revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the TOE will not establish an SA.
- Test FCS_IPSEC_EXT.1.11.4: (conditional) The evaluator shall generate a pre-shared key and use it, as indicated in the operational guidance, to establish an IPsec connection with the VPN GW peer. If the generation of the pre-shared key is supported, the evaluator shall ensure that establishment of the key is carried out for an instance of the TOE generating the key as well as an instance of the TOE merely taking in and using the key.

For each supported identifier type (excluding DNs), the evaluator shall repeat the following tests:

- Test FCS_IPSEC_EXT.1.11.5: For each field of the certificate supported for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the field in the peer's presented certificate and shall verify that the IKEv2 authentication succeeds.
- Test FCS_IPSEC_EXT.1.11.6: For each field of the certificate support for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to not match the field in the peer's presented certificate and shall verify that the IKEv2 authentication fails.

The following tests are conditional:

- Test FCS_IPSEC_EXT.1.11.7: (conditional) If, according to the TSS, the TOE supports both Common Name and SAN certificate fields and uses the preferred logic outlined in the Application Note, the tests above with the Common Name field shall be performed using peer certificates with no SAN extension. Additionally, the evaluator shall configure the peer's reference identifier on the TOE to not match the SAN in the peer's presented certificate but to match the Common Name in the peer's presented certificate, and verify that the IKEv2 authentication fails.
- Test FCS_IPSEC_EXT.1.11.8: (conditional) If the TOE supports DN identifier types, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the subject DN in the peer's presented certificate and shall verify that the IKEv2 authentication succeeds. To demonstrate a bit-wise comparison of the DN, the evaluator shall change a single bit in the DN (preferably, in an Object Identifier (OID) in the DN) and verify that the IKEv2 authentication fails. To demonstrate a comparison of DN values, the evaluator shall change any one of the four DN values and verify that the IKEv2 authentication fails.
- Test FCS_IPSEC_EXT.1.11.9: (conditional) If the TOE supports both IPv4 and IPv6 and supports IP address identifier types, the evaluator must repeat test 1 and 2 with both IPv4 address identifiers and IPv6 identifiers. Additionally, the evaluator shall verify that the TOE verifies that the IP header matches the identifiers by setting the presented identifiers and

the reference identifier with the same IP address that differs from the actual IP address of the peer in the IP headers and verifying that the IKEv2 authentication fails.

- *Test FCS_IPSEC_EXT.1.11:10: (conditional) If, according to the TSS, the TOE performs comparisons between the peer's ID payload and the peer's certificate, the evaluator shall repeat the following test for each combination of supported identifier types and supported certificate fields (as above). The evaluator shall configure the peer to present a different ID payload than the field in the peer's presented certificate and verify that the TOE fails to authenticate the IKE peer.*

FCS_IPSEC_EXT.1.12

EAs for this element are tested through EAs for [FCS_IPSEC_EXT.1.11](#).

FCS_IPSEC_EXT.1.13

EAs for this element are tested through EAs for [FCS_IPSEC_EXT.1.11](#).

FCS_IPSEC_EXT.1.14

TSS

The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the checks that are done when negotiating IKEv2 CHILD_SA suites to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKEv2 IKE_SA that is protecting the negotiation.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluator follows the guidance to configure the TOE to perform the following tests:

- *Test FCS_IPSEC_EXT.1.14:1: The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.*
- *Test FCS_IPSEC_EXT.1.14:2: (conditional) The evaluator shall attempt to establish an IKEv2 CHILD_SA for ESP that selects an encryption algorithm with more strength than that being used for the IKEv2 IKE_SA (i.e., symmetric algorithm with a key size larger than that being used for the IKEv2 IKE_SA). Such attempts should fail.*
- *Test FCS_IPSEC_EXT.1.14:3: The evaluator shall attempt to establish an IKEv2 IKE_SA using an algorithm that is not one of the supported algorithms and hash functions identified in the requirements. Such an attempt should fail.*
- *Test FCS_IPSEC_EXT.1.14:4: The evaluator shall attempt to establish an IKEv2 CHILD_SA for ESP (assumes the proper parameters were used to establish the IKEv2 IKE_SA) that selects an encryption algorithm that is not identified in [FCS_IPSEC_EXT.1.4](#). Such an attempt should fail.*

FCS_RB.G.2 Random Bit Generation (External Seeding)

The inclusion of this selection-based component depends upon selection in [FCS_RB.G.1.2](#).

FCS_RB.G.2.1

The TSF shall be able to accept a minimum input of [**assignment**: *minimum input length greater than zero*] from a TSF interface for the purpose of seeding.

Evaluation Activities ▾

[**FCS_RB.G.2.1**](#)

TSS

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

There are no test activities for this element.

FCS_RB.G.3 Random Bit Generation (Internal Seeding - Single Source)

The inclusion of this selection-based component depends upon selection in [FCS_RB.G.1.2](#).

FCS_RB.G.3.1

The TSF shall be able to seed the RBG using a [**selection**: *TSF software-based noise source, TSF hardware-based noise source*] with a minimum of [**assignment**: *number of bits*] bits of min-entropy.

Evaluation Activities ▾

FCS_RBG.3.1**TSS**

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

There are no test activities for this element.

FCS_RBG.4 Random Bit Generation (Internal Seeding - Multiple Sources)

The inclusion of this selection-based component depends upon selection in FCS_RBG.1.2.

FCS_RBG.4.1

The TSF shall be able to seed the RBG using [selection: [assignment: number] TSF software-based noise source(s), [assignment: number] TSF hardware-based noise source(s)].

Evaluation Activities ▼**FCS_RBG.4.1****TSS**

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

There are no test activities for this element.

FCS_RBG.5 Random Bit Generation (Combining Noise Sources Sources)

The inclusion of this selection-based component depends upon selection in FCS_RBG.1.2.

FCS_RBG.5.1

The TSF shall [assignment: combining operation] [selection: output from TSF noise source(s), input from TSF interface(s) for seeding] to create the entropy input into the derivation function as defined in [assignment: list of standards], resulting in a minimum of [assignment: number of bits] bits of min-entropy.

Evaluation Activities ▼**FCS_RBG.5.1****TSS**

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

There are no test activities for this element.

B.3 Identification and Authentication (FIA)**FIA_PMG_EXT.1 Password Management**

The inclusion of this selection-based component depends upon selection in FIA_UAU.5.1.

FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case characters, digits, and the following special characters:
[selection: "!", "@", "#", "\$", "%", "^", "&", "*", "(", ")"], [assignment: other characters]]
2. Minimum password length shall be configurable

3. Passwords of at least 15 characters in length shall be supported

Application Note: This SFR is included in the ST if the ST author selects 'authentication based on username and password' in [FIA_UAU.5.1](#).

The ST author selects the special characters that are supported by the TOE; they may optionally list additional special characters supported using the assignment. "Administrative passwords" refers to passwords used by administrators to gain access to the Management Subsystem.

Evaluation Activities ▼

[FIA_PMG_EXT.1.1](#)

TSS

There are no additional TSS evaluation activities for this element.

Guidance

The evaluator shall examine the operational guidance to determine that it provides guidance to security administrators in the composition of strong passwords, and that it provides instructions on setting the minimum password length.

Tests

The evaluator shall also perform the following test.

- Test FIA_PMG_EXT.1.1:1: The evaluator shall compose passwords that either meet the requirements, or fail to meet the requirements, in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible combinations of passwords, the evaluator shall ensure that all characters, rule characteristics, and a minimum length listed in the requirement are supported, and justify the subset of those characters chosen for testing.

[FIA_X509_EXT.4 Exceptions to X.509 Certificate Revocation Checking](#)

FIA_X509_EXT.4.1

The TSF shall provide alternate functionality to standard X.509 certificate revocation checking for the following exceptions: [selection: firmware checking of updates: invalidate automatic updates if the firmware certificate is compromised, [assignment: other exceptions and corresponding functionality]].

Evaluation Activities ▼

[FIA_X509_EXT.4.1](#)

TSS

The evaluator shall ensure the TSS describes, for each exception, the alternate functionality the TOE implements to handle the lack of certificate revocation. The description must be consistent with the selection in the requirement.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

- Test FIA_X509_EXT.4.1:1: For each exception, the evaluator shall configure the TSF as necessary to meet the exceptional condition described, and exercise the function using a certificate chain without revocation information. The evaluator shall attempt to examine TSF logging or behavior as described in the TSS to confirm the alternative action described is performed. For example, in the case of firmware updates that invalidate automatic updates, the evaluator shall invoke an automatic update and observe that the update is not performed. In other cases, the TSS describes the alternative action.

B.4 Protection of the TSF (FPT)

[FPT_TUD_EXT.2 Trusted Update Based on Certificates](#)

The inclusion of this selection-based component depends upon selection in [FPT_TUD_EXT.1.3](#).

FPT_TUD_EXT.2.1

The TSF shall not install an update if the code signing certificate is deemed invalid.

Application Note: Certificates may optionally be used for code signing of system software updates ([FPT_TUD_EXT.1.3](#)). This element must be included in the ST if certificates are used for validating updates. If "code signing for system

software updates" is selected in FIA_X509_EXT.2.1 from the Functional Package for X.509, version 1.0, [FTP_TUD_EXT.2](#) must be included in the ST.

Validity is determined by the certificate path, the expiration date, and the revocation status in accordance with FIA_X509_EXT.1 in the Functional Package for X.509, version 1.0.

Evaluation Activities ▼

[FTP_TUD_EXT.2.1](#)

TSS

There are no additional TSS evaluation activities for this element.

Guidance

There are no additional Guidance evaluation activities for this element.

Tests

The evaluation activity for this requirement is performed in conjunction with the evaluation activity for FIA_X509_EXT.1 and FIA_X509_EXT.2 in the Functional Package for X.509, version 1.0.

B.5 Trusted Path/Channel (FTP)

FTP_TRP.1 Trusted Path

The inclusion of this selection-based component depends upon selection in FMT_MOF_EXT.1.1, FTP_ITC_EXT.1.1.

FTP_TRP.1.1

The TSF shall **use a trusted channel as specified in [FTP_ITC_EXT.1](#) to provide a trusted communication path between itself and [remote] administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2

The TSF shall permit [remote **administrators**] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [*all remote administration actions*]].

Application Note: This SFR is included in the ST if "remote" is selected in [FMT_MOF_EXT.1.1](#).

Protocols used to implement the remote administration trusted channel must be selected in [FTP_ITC_EXT.1](#).

This requirement ensures that authorized remote administrators initiate all communication with the TOE via a trusted path, and that all communications with the TOE by remote administrators is performed over this path. The data passed in this trusted communication channel are encrypted as defined the protocol chosen in the first selection in [FTP_ITC_EXT.1](#). The ST author chooses the mechanism or mechanisms supported by the TOE, and then ensures that the detailed requirements in Appendix B corresponding to their selection are copied to the ST if not already present.

Evaluation Activities ▼

[FTP_TRP.1.1](#)

TSS

The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.

Guidance

The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.

Tests

The evaluator shall also perform the following tests:

- *Test FTP_TRP.1.1:1: The evaluators shall ensure that communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.*

- *Test FTP_TRP.1.1:2: For each method of remote administration supported, the evaluator shall follow the operational guidance to ensure that there is no available interface that can be used by a remote user to establish remote administrative sessions without invoking the trusted path.*
- *Test FTP_TRP.1.1:3: The evaluator shall ensure, for each method of remote administration, the channel data is not sent in plaintext.*
- *Test FTP_TRP.1.1:4: The evaluator shall ensure, for each method of remote administration, modification of the channel data is detected by the TOE.*

Additional evaluation activities are associated with the specific protocols.

Appendix C - Extended Component Definitions

This appendix contains the definitions for all extended requirements specified in the PP.

C.1 Extended Components Table

All extended components specified in the PP are listed in this table:

Table 10: Extended Component Definitions

Functional Class	Functional Components
Cryptographic Support (FCS)	FCS_ENT_EXT Entropy for Virtual Machines FCS_HTTPS_EXT HTTPS Protocol FCS_IPSEC_EXT IPsec Protocol
Identification and Authentication (FIA)	FIA_AFL_EXT Authentication Failure Handling FIA_PMG_EXT Password Management FIA_UIA_EXT Administrator Identification and Authentication FIA_X509_EXT X.509 Certificate
Protection of the TSF (FPT)	FPT_DDI_EXT Device Driver Isolation FPT_DVD_EXT Non-Existence of Disconnected Virtual Devices FPT_EEM_EXT Execution Environment Mitigations FPT_GVI_EXT guest VM Integrity FPT_HAS_EXT Hardware Assists FPT_HCL_EXT Hypercall Controls FPT_IDV_EXT Software Identification and Versions FPT_INT_EXT Support for Introspection FPT_ML_EXT Measured Launch of Platform and VMM FPT_RDM_EXT Removable Devices and Media FPT_TUD_EXT Trusted Updates FPT_VDP_EXT Virtual Device Parameters FPT_VIV_EXT VMM Isolation from VMs
Security Management (FMT)	FMT_MOF_EXT Management of Security Functions Behavior FMT_SMO_EXT Separation of Management and Operational Networks
Trusted Path/Channel (FTP)	FTP_ITC_EXT Trusted Channel Communications FTP_UIF_EXT User Interface
User Data Protection (FDP)	FDP_HBI_EXT Hardware-Based Isolation Mechanisms FDP_PPR_EXT Physical Platform Resource Controls FDP_RIP_EXT Residual Information in Memory FDP_VMS_EXT VM Separation FDP_VNC_EXT Virtual Networking Components

C.2 Extended Component Definitions

C.2.1 Cryptographic Support (FCS)

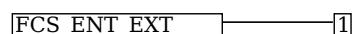
This PP defines the following extended components as part of the FCS class originally defined by CC Part 2:

C.2.1.1 FCS_ENT_EXT Entropy for Virtual Machines

Family Behavior

This family defines requirements for availability of entropy data generated or collected by the TSF.

Component Leveling



[FCS_ENT_EXT.1](#), Entropy for Virtual Machines, requires the TSF to provide entropy data to VMs in a specified manner.

Management: FCS_ENT_EXT.1

There are no management functions foreseen.

Audit: FCS_ENT_EXT.1

There are no audit events foreseen.

FCS_ENT_EXT.1 Entropy for Virtual Machines

Hierarchical to: No other components.

Dependencies to: [FCS_RBG.1](#) Cryptographic Operation (Random Bit Generation)

FCS_ENT_EXT.1.1

The TSF shall provide a mechanism to make available to VMs entropy that meets [FCS_RBG.1](#) through [selection: *hypervisor interface, virtual device interface, pass-through access to hardware entropy source*].

FCS_ENT_EXT.1.2

The TSF shall provide independent entropy across multiple VMs.

C.2.1.2 FCS_HTTPS_EXT HTTPS Protocol

Family Behavior

This family defines requirements for protecting remote management sessions between the TOE and a security administrator. This family describes how HTTPS will be implemented.

Component Leveling



[FCS_HTTPS_EXT.1](#), HTTPS Protocol, defines requirements for the implementation of the HTTPS protocol.

Management: FCS_HTTPS_EXT.1

There are no management functions foreseen.

Audit: FCS_HTTPS_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Failure to establish an HTTPS session.
- b. Establishment/termination of an HTTPS session.

FCS_HTTPS_EXT.1 HTTPS Protocol

Hierarchical to: No other components.

Dependencies to: [FCS_TLSC_EXT.1 TLS Client Protocol, or
FCS_TLSC_EXT.2 TLS Client Protocol with Mutual Authentication, or
FCS_TLSS_EXT.1 TLS Server Protocol, or
FCS_TLSS_EXT.2 TLS Server Protocol with Mutual Authentication]

FCS_HTTPS_EXT.1.1

The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2

The TSF shall implement HTTPS using TLS.

C.2.1.3 FCS_IPSEC_EXT IPsec Protocol

Family Behavior

This family defines requirements for protecting communications using IPsec.

Component Leveling



[FCS_IPSEC_EXT.1](#), IPsec Protocol, requires that IPsec be implemented as specified.

Management: FCS_IPSEC_EXT.1

There are no management functions foreseen.

Audit: FCS_IPSEC_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Failure to establish an IPsec SA.
- b. Establishment/Termination of an IPsec SA.

FCS_IPSEC_EXT.1 IPsec Protocol

Hierarchical to: No other components.

Dependencies to: [FCS_CKM.1](#) Cryptographic Key Generation
[FCS_CKM.2](#) Cryptographic Key Establishment
[FCS_COP.1](#) Cryptographic Operation

FCS_IPSEC_EXT.1.1

The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2

The TSF shall implement [**selection**: *transport mode, tunnel mode*].

FCS_IPSEC_EXT.1.3

The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4

The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [**assignment**: *cryptographic algorithms*] together with a Secure Hash Algorithm (SHA)-based HMAC.

FCS_IPSEC_EXT.1.5

The TSF shall implement the protocol:

[selection]:

- IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFC 2407, RFC 2408, RFC 2409, RFC 4109, [**selection**: no other RFCs for extended sequence numbers, RFC 4304 for extended sequence numbers], [**selection**: no other RFCs for hash functions, RFC 4868 for hash functions], and [**selection, choose one of**: support for XAUTH, no support for XAUTH]
- IKEv2 as defined in RFC 7296 (with mandatory support for NAT traversal as specified in section 2.23), RFC 8784, RFC 8247, and [**selection**: no other RFCs for hash functions, RFC 4868 for hash functions]

1.

FCS_IPSEC_EXT.1.6

The TSF shall ensure the encrypted payload in the [**selection**: *IKEv1, IKEv2*] protocol uses the cryptographic algorithms [**assignment**: *acceptable cryptographic algorithms*] and no other algorithm.

FCS_IPSEC_EXT.1.7

The TSF shall ensure that [**assignment**: *version(s) of IKE SA supported and the acceptable method(s) through which their lifetimes can be configured*].

FCS_IPSEC_EXT.1.8

The TSF shall ensure that all IKE protocols implement DH groups [**assignment**: *DH Groups*].

FCS_IPSEC_EXT.1.9

The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in $gx \bmod p$) using the random bit generator specified in FCS_RBG.1, and having a length of at least [**assignment**: *(one or more) number of bits that is at least twice the "bits of security" value associated with the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, Recommendation for Key Management - Part 1: General*] bits.

FCS_IPSEC_EXT.1.10

The TSF shall generate nonces used in IKE exchanges in a manner such that the probability that a specific nonce value will be repeated during the life of a specific IPsec SA is less than 1 in $2^{[\text{assignment}: (\text{one or more}) "bits of security" value associated with the negotiated Diffie-Hellman group as listed in Table 2 of NIST SP 800-57, Recommendation for Key Management - Part 1: General]}$.

FCS_IPSEC_EXT.1.11

The TSF shall ensure that the IKE protocol performs peer authentication using a [**selection**: *RSA, ECDSA*] that use X.509v3 certificates that conform to RFC 4945 and [**selection**: *Pre-shared Keys, no other method*].

FCS_IPSEC_EXT.1.12

The TSF shall not establish an SA if the [**assignment**: *specific certificate reference identifier*] and [**assignment**: *other certificate reference identifier type*] contained in a certificate does not match the expected value(s) for the entity attempting to establish a connection.

FCS_IPSEC_EXT.1.13

The TSF shall not establish an SA if the presented identifier does not match the configured reference identifier of the peer.

FCS_IPSEC_EXT.1.14

The [assignment: enforcing party] shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [assignment: version-specific term for initial SAs that protect protocol negotiation traffic] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [assignment: version-specific term for subsequent SAs that protect data traffic] connection.

C.2.2 Identification and Authentication (FIA)

This PP defines the following extended components as part of the FIA class originally defined by CC Part 2:

C.2.2.1 FIA_AFL_EXT Authentication Failure Handling

Family Behavior

This family defines requirements for detection and prevention of brute force authentication attempts.

Component Leveling



FIA_AFL_EXT.1, Authentication Failure Handling, requires the TSF to lock an administrator account when an excessive number of failed authentication attempts have been observed until some restorative event occurs to enable the account.

Management: FIA_AFL_EXT.1

The following actions could be considered for the management functions in FMT:

- Ability to configure lockout policy through unsuccessful authentication attempts.

Audit: FIA_AFL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Unsuccessful login attempts limit is met or exceeded.

FIA_AFL_EXT.1 Authentication Failure Handling

Hierarchical to: No other components.

Dependencies to: [FIA_UIA_EXT.1](#) Administrator Identification and Authentication
FMT_SMR.1 Security Roles

FIA_AFL_EXT.1.1

The TSF shall detect when [selection:

- [assignment: a positive integer number]
- an administrator configurable positive integer within a [assignment: range of acceptable values]

] unsuccessful authentication attempts occur related to administrators attempting to authenticate remotely using [selection: username and password, username and PIN].

FIA_AFL_EXT.1.2

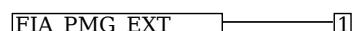
When the defined number of unsuccessful authentication attempts has been met, the TSF shall:
[selection: prevent the offending administrator from successfully establishing a remote session using any authentication method that involves a password or PIN until [assignment: action to unlock] is taken by an administrator, prevent the offending administrator from successfully establishing a remote session using any authentication method that involves a password or PIN until an administrator-defined time period has elapsed]

C.2.2.2 FIA_PMG_EXT Password Management

Family Behavior

This family defines requirements for the composition of administrator passwords.

Component Leveling



FIA_PMG_EXT.1, Password Management, requires the TSF to ensure that administrator passwords meet a defined password policy.

Management: FIA_PMG_EXT.1

The following actions could be considered for the management functions in FMT:

- Ability to configure administrator password policy, including the ability to change default authorization factors.

Audit: FIA_PMG_EXT.1

There are no audit events foreseen.

FIA_PMG_EXT.1 Password Management

Hierarchical to: No other components.

Dependencies to: [FIA_UIA_EXT.1](#) Administrator Identification and Authentication

FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case characters, digits, and the following special characters: [selection: "!", "@", "#", "\$", "%", "^", "&", "*", "(", ")", [assignment: other characters]]
2. Minimum password length shall be configurable
3. Passwords of at least 15 characters in length shall be supported

C.2.2.3 FIA_UIA_EXT Administrator Identification and Authentication

Family Behavior

This family defines requirements for ensuring that access to the TSF is not granted to unauthenticated subjects.

Component Leveling



[FIA_UIA_EXT.1](#), Administrator Identification and Authentication, requires the TSF to ensure that all subjects attempting to perform TSF-mediated actions are identified and authenticated prior to authorizing these actions to be performed.

Management: FIA_UIA_EXT.1

There are no management functions foreseen.

Audit: FIA_UIA_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Administrator authentication attempts.
- b. All use of the identification and authentication mechanism.
- c. Administrator session start time and end time.

FIA_UIA_EXT.1 Administrator Identification and Authentication

Hierarchical to: No other components.

Dependencies to: [FIA_UAU.5](#) Multiple Authentication Mechanisms

FIA_UIA_EXT.1.1

The TSF shall require administrators to be successfully identified and authenticated using one of the methods in [FIA_UAU.5](#) before allowing any TSF-mediated management function to be performed by that administrator.

C.2.2.4 FIA_X509_EXT X.509 Certificate

Family Behavior

This family defines requirements for the validation and use of X.509 certificates.

Component Leveling

C.2.3 Protection of the TSF (FPT)

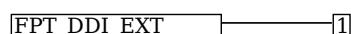
This PP defines the following extended components as part of the FPT class originally defined by CC Part 2:

C.2.3.1 FPT_DDI_EXT Device Driver Isolation

Family Behavior

This family defines requirements for isolation of device drivers

Component Leveling



[FPT_DDI_EXT.1](#), Device Driver Isolation, requires the TSF to isolate device drivers for physical devices from all virtual domains.

Management: FPT_DDI_EXT.1

There are no management functions foreseen.

Audit: FPT_DDI_EXT.1

There are no audit events foreseen.

FPT_DDI_EXT.1 Device Driver Isolation

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_DDI_EXT.1.1

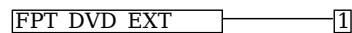
The TSF shall ensure that device drivers for physical devices are isolated from the VMM and all other domains.

C.2.3.2 FPT_DVD_EXT Non-Existence of Disconnected Virtual Devices

Family Behavior

This family defines requirements for ensuring that guest VMs cannot access the virtual hardware interfaces disabled or disconnected virtual devices.

Component Leveling



[FPT_DVD_EXT.1](#), Non-Existence of Disconnected Virtual Devices, requires the TSF to prevent guest VMs from accessing virtual devices that it is not configured to have access to.

Management: FPT_DVD_EXT.1

There are no management functions foreseen.

Audit: FPT_DVD_EXT.1

There are no audit events foreseen.

FPT_DVD_EXT.1 Non-Existence of Disconnected Virtual Devices

Hierarchical to: No other components.

Dependencies to: [FPT_VDP_EXT.1](#) Virtual Device Parameters

FPT_DVD_EXT.1.1

The TSF shall prevent guest VMs from accessing virtual device interfaces that are not present in the VM's current virtual hardware configuration.

C.2.3.3 FPT_EEM_EXT Execution Environment Mitigations

Family Behavior

This family defines requirements for the TOE's compatibility with platform mechanisms that prevent vulnerabilities that allow for the execution of unauthorized code or bypass of access restrictions on memory or storage.

Component Leveling



[FPT_EEM_EXT.1](#), Execution Environment Mitigations, requires the TSF to identify the execution environment-based protection mechanisms that it can use for self-protection.

Management: FPT_EEM_EXT.1

There are no management functions foreseen.

Audit: FPT_EEM_EXT.1

There are no audit events foreseen.

FPT_EEM_EXT.1 Execution Environment Mitigations

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_EEM_EXT.1.1

The TSF shall take advantage of execution environment-based vulnerability mitigation mechanisms supported by the Platform such as: **[selection]**:

- *Address space randomization*
- *Memory execution protection (e.g., DEP)*
- *Stack buffer overflow protection*
- *Heap corruption detection*
- **[assignment: other mechanisms]**
- *No mechanisms*

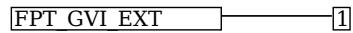
]

C.2.3.4 FPT_GVI_EXT guest VM Integrity

Family Behavior

This family defines requirements for the TOE to assert the integrity of guest VMs.

Component Leveling



FPT_GVI_EXT.1, guest VM Integrity, requires the TSF to specify the mechanisms it uses to verify the integrity of guest VMs.

Management: FPT_GVI_EXT.1

There are no management functions foreseen.

Audit: FPT_GVI_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Actions taken due to failed integrity check.

FPT_GVI_EXT.1 guest VM Integrity

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_GVI_EXT.1.1

The TSF shall verify the integrity of guest VMs through the following mechanisms: **[assignment: list of guest VM integrity mechanisms]**.

C.2.3.5 FPT_HAS_EXT Hardware Assists

Family Behavior

This family defines requirements for use of hardware-based virtualization assists as performance enhancements.

Component Leveling



FPT_HAS_EXT.1, Hardware Assists, requires the TSF to identify the hardware assists it uses to reduce TOE complexity.

Management: FPT_HAS_EXT.1

There are no management functions foreseen.

Audit: FPT_HAS_EXT.1

There are no audit events foreseen.

FPT_HAS_EXT.1 Hardware Assists

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_HAS_EXT.1.1

The VMM shall use **[assignment: list of hardware-based virtualization assists]** to reduce or eliminate the need for binary translation.

FPT_HAS_EXT.1.2

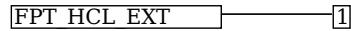
The VMM shall use **[assignment: list of hardware-based virtualization memory-handling assists]** to reduce or eliminate the need for shadow page tables.

C.2.3.6 FPT_HCL_EXT Hypercall Controls

Family Behavior

This family defines requirements for control of hypercall interfaces.

Component Leveling



[FPT_HCL_EXT.1](#), Hypercall Controls, requires the TSF to implement appropriate parameter validation to protect the VMM from unauthorized access through a hypercall interface.

Management: FPT_HCL_EXT.1

There are no management functions foreseen.

Audit: FPT_HCL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Invalid parameter to hypercall detected.
- b. Hypercall interface invoked when documented preconditions are not met.

FPT_HCL_EXT.1 Hypercall Controls

Hierarchical to: No other components.

Dependencies to: FMT_SMR.1 Security Roles

FPT_HCL_EXT.1.1

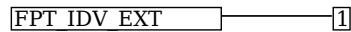
The TSF shall validate the parameters passed to hypercall interfaces prior to execution of the VMM functionality exposed by each interface.

C.2.3.7 FPT_IDV_EXT Software Identification and Versions

Family Behavior

This family defines requirements for the use of SWID tags to identify the TOE.

Component Leveling



[FPT_IDV_EXT.1](#), Software Identification and Versions, requires the TSF to identify itself using SWID tags.

Management: FPT_IDV_EXT.1

There are no management functions foreseen.

Audit: FPT_IDV_EXT.1

There are no audit events foreseen.

FPT_IDV_EXT.1 Software Identification and Versions

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_IDV_EXT.1.1

The TSF shall include software identification (SWID) tags that contain a SoftwareIdentity element and an Entity element as defined in ISO/IEC 19770-2:2009.

FPT_IDV_EXT.2

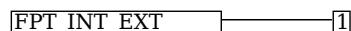
The TSF shall store SWIDs in a .swidtag file as defined in ISO/IEC 19770-2:2009.

C.2.3.8 FPT_INT_EXT Support for Introspection

Family Behavior

This family defines requirements for supporting VM introspection.

Component Leveling



[FPT_INT_EXT.1](#), Support for Introspection, requires the TSF to support introspection.

Management: FPT_INT_EXT.1

There are no management functions foreseen.

Audit: FPT_INT_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Introspection initiated/enabled.

FPT_INT_EXT.1 Support for Introspection

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_INT_EXT.1.1

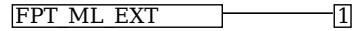
The TSF shall support a mechanism for permitting the VMM or privileged VMs to access the internals of another VM for purposes of introspection.

C.2.3.9 FPT_ML_EXT Measured Launch of Platform and VMM

Family Behavior

This family defines requirements for measured launch.

Component Leveling



[FPT_ML_EXT.1](#), Measured Launch of Platform and VMM, requires the TSF to support a measured launch of itself.

Management: FPT_ML_EXT.1

There are no management functions foreseen.

Audit: FPT_ML_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Integrity measurements collected.

FPT_ML_EXT.1 Measured Launch of Platform and VMM

Hierarchical to: No other components.

Dependencies to: No dependencies.

FPT_ML_EXT.1.1

The TSF shall support a measured launch of the virtualization system. Measured components of the VS shall include the static executable image of the hypervisor and: [selection:

- *Static executable images of the Management Subsystem*
- *[assignment: list of (static images of) Service VMs]*
- *[assignment: list of configuration files]*
- *no other components*

]

FPT_ML_EXT.1.2

The TSF shall make the measurements selected in [FPT_ML_EXT.1.1](#) available to the Management Subsystem.

C.2.3.10 FPT_RDM_EXT Removable Devices and Media

Family Behavior

This family defines requirements for enforcement of domain isolation when removable devices can be connected to a domain.

Component Leveling



[FPT_RDM_EXT.1](#), Removable Devices and Media, requires the TSF to ensure that VMs are not inadvertently given access to information in different domains because removable media is simultaneously accessible from separate domains.

Management: FPT_RDM_EXT.1

The following actions could be considered for the management functions in FMT:

- Ability to configure removable media policy.
- Ability to connect/disconnect removable devices to/from a VM.

Audit: FPT_RDM_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Connection/disconnection of removable media or device to/from a VM.
- b. Ejection/insertion of removable media or device from/to an already connected VM.

FPT_RDM_EXT.1 Removable Devices and Media

Hierarchical to: No other components.

Dependencies to: [FDP_VMS_EXT.1](#) VM Separation

FPT_RDM_EXT.1.1

The TSF shall implement controls for handling the transfer of virtual and physical removable media and virtual and physical removable media devices between information domains.

FPT_RDM_EXT.1.2

The TSF shall enforce the following rules when [**assignment**: *virtual or physical removable media and virtual or physical removable media devices*] are switched between information domains, then [**selection**]:

- *the administrator has granted explicit access for the media or device to be connected to the receiving domain*
- *the media in a device that is being transferred is ejected prior to the receiving domain being allowed access to the device*
- *the user of the receiving domain expressly authorizes the connection*
- *the device or media that is being transferred is prevented from being accessed by the receiving domain*

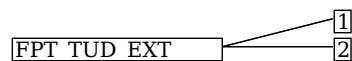
]

C.2.3.11 FPT_TUD_EXT Trusted Updates

Family Behavior

This family defines requirements for ensuring that updates to the TOE software and firmware are genuine.

Component Leveling



[FPT_TUD_EXT.1](#), Trusted Updates to the Virtualization System, requires the TSF to define the mechanism for applying and verifying TOE updates.

[FPT_TUD_EXT.2](#), Trusted Update Based on Certificates, requires the TSF to validate updates using a code signing certificate.

Management: FPT_TUD_EXT.1

The following actions could be considered for the management functions in FMT:

- a. Ability to update the virtualization system.

Audit: FPT_TUD_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Initiation of update.
- b. Failure of signature verification.

FPT_TUD_EXT.1 Trusted Updates to the Virtualization System

Hierarchical to: No other components.

Dependencies to: [FCS_COP.1](#) Cryptographic Operation

FPT_TUD_EXT.1.1

The TSF shall provide administrators the ability to query the currently executed version of the TOE firmware and software as well as the most recently installed version of the TOE firmware and software.

FPT_TUD_EXT.1.2

The TSF shall provide administrators the ability to manually initiate updates to TOE firmware and software and [**selection**: *automatic updates, no other update mechanism*].

FPT_TUD_EXT.1.3

The TSF shall provide means to authenticate firmware and software updates to the TOE using a [assignment: integrity action] prior to installing those updates.

Management: FPT_TUD_EXT.2

There are no management functions foreseen.

Audit: FPT_TUD_EXT.2

There are no audit events foreseen.

FPT_TUD_EXT.2 Trusted Update Based on Certificates

Hierarchical to: No other components.

Dependencies to: [FPT_TUD_EXT.1](#) Trusted Updates to the Virtualization System
FIA_X509_EXT.1 X.509 Validation
FIA_X509_EXT.2 X.509 Authentication

FPT_TUD_EXT.2.1

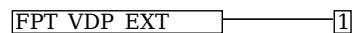
The TSF shall not install an update if the code signing certificate is deemed invalid.

C.2.3.12 FPT_VDP_EXT Virtual Device Parameters

Family Behavior

This family defines requirements for processing data transmitted to the TOE from a guest VM.

Component Leveling



[FPT_VDP_EXT.1](#), Virtual Device Parameters, requires the TSF to interface with guest VMs through virtual hardware abstractions so that any data transmitted to the TOE from a guest VM can be validated as well-formed.

Management: FPT_VDP_EXT.1

There are no management functions foreseen.

Audit: FPT_VDP_EXT.1

There are no audit events foreseen.

FPT_VDP_EXT.1 Virtual Device Parameters

Hierarchical to: No other components.

Dependencies to: [FPT_VIV_EXT.1](#) VMM Isolation from VMs

FPT_VDP_EXT.1.1

The TSF shall provide interfaces for virtual devices implemented by the VMM as part of the virtual hardware abstraction.

FPT_VDP_EXT.1.2

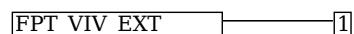
The TSF shall validate the parameters passed to the virtual device interface prior to execution of the VMM functionality exposed by those interfaces.

C.2.3.13 FPT_VIV_EXT VMM Isolation from VMs

Family Behavior

This family defines requirements for ensuring the TOE is logically isolated from its guest VMs

Component Leveling



[FPT_VIV_EXT.1](#), VMM Isolation from VMs, requires the TSF to ensure that there is no mechanism by which a guest VM can interface with the TOE, other VMs, or the hardware platform without authorization.

Management: FPT_VIV_EXT.1

There are no management functions foreseen.

Audit: FPT_VIV_EXT.1

There are no audit events foreseen.

FPT_VIV_EXT.1 VMM Isolation from VMs

Hierarchical to: No other components.

Dependencies to: [FDP_PPR_EXT.1](#) Physical Platform Resource Controls
[FDP_VMS_EXT.1](#) VM Separation

FPT_VIV_EXT.1.1

The TSF must ensure that software running in a VM is not able to degrade or disrupt the functioning of other VMs, the VMM, or the platform.

FPT_VIV_EXT.1.2

The TSF must ensure that a guest VM is unable to invoke platform code that runs at a privilege level equal to or exceeding that of the VMM without involvement of the VMM.

C.2.4 Security Management (FMT)

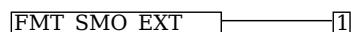
This PP defines the following extended components as part of the FMT class originally defined by CC Part 2:

C.2.4.1 FMT_SMO_EXT Separation of Management and Operational Networks

Family Behavior

This family defines requirements for separation of management and operational networks.

Component Leveling



[FMT_SMO_EXT.1](#), Separation of Management and Operational Networks, requires the TSF to separate its management and operational networks through a defined mechanism.

Management: FMT_SMO_EXT.1

There are no management functions foreseen.

Audit: FMT_SMO_EXT.1

There are no audit events foreseen.

FMT_SMO_EXT.1 Separation of Management and Operational Networks

Hierarchical to: No other components.

Dependencies to: No dependencies.

FMT_SMO_EXT.1.1

The TSF shall support the separation of management and operational network traffic through [**selection: separate physical networks, separate logical networks, trusted channels as defined in [FTP_ITC_EXT.1](#), data encryption using an algorithm specified in FCS_COP.1**].

C.2.4.2 FMT_MOF_EXT Management of Security Functions Behavior

Family Behavior

This family defines requirements for administrative management of the TOE.

Component Leveling



[FMT_MOF_EXT.1](#), Management of Security Functions Behavior, defines required management functions and responsibilities.

Management: FMT_MOF_EXT.1

There are no additional management functions beyond those already described in [FMT_MOF_EXT.1](#).

Audit: FMT_MOF_EXT.1

Success or failure of management function.

FMT_MOF_EXT.1 Management of Security Functions Behavior

Hierarchical to: No other components.

Dependencies to: No other dependencies.

FMT_MOF_EXT.1.1

The TSF shall be capable of supporting [**selection: local, remote**] administration.

FMT_MOF_EXT.1.2

The TSF shall be capable of performing the following management functions [**assignment**: *description of management functions*].

C.2.5 Trusted Path/Channel (FTP)

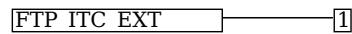
This PP defines the following extended components as part of the FTP class originally defined by CC Part 2:

C.2.5.1 FTP_ITC_EXT Trusted Channel Communications

Family Behavior

This family defines requirements for protection of data in transit between the TOE and its operational environment.

Component Leveling



[FTP_ITC_EXT.1](#), Trusted Channel Communications, requires the TSF to implement one or more cryptographic protocols to secure connectivity between the TSF and various external entities.

Management: FTP_ITC_EXT.1

There are no management functions foreseen.

Audit: FTP_ITC_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Initiation of the trusted channel.
- b. Termination of the trusted channel.
- c. Failures of the trusted path functions.

FTP_ITC_EXT.1 Trusted Channel Communications

Hierarchical to: No other components.

Dependencies to: [FAU_STG.1](#) External Audit Storage

FTP_ITC_EXT.1.1

The TSF shall use [**assignment**: *transport mechanism*] and [**assignment**: *authentication mechanism*] to provide a trusted communication channel between itself and

- audit servers (as required by [FAU_STG.1](#)) and

[**assignment**: *remote entities*] that is logically distinct from other communication paths and provides assured identification of its endpoints and protection of the communicated data from disclosure and detection of modification of the communicated data.

C.2.5.2 FTP_UIF_EXT User Interface

Family Behavior

This family defines requirements for unambiguously identifying the specific guest VM that a TOE user is interacting with at any given point in time.

Component Leveling



[FTP_UIF_EXT.1](#), User Interface: I/O Focus, requires the TSF to unambiguously identify the guest VM that has the current input focus for input peripherals.

[FTP_UIF_EXT.2](#), User Interface: Identification of VM, requires the TOE to perform power on self-tests to verify its functionality and the integrity of its stored executable code.

Management: FTP_UIF_EXT.1

There are no management functions foreseen.

Audit: FTP_UIF_EXT.1

There are no audit events foreseen.

FTP_UIF_EXT.1 User Interface: I/O Focus

Hierarchical to: No other components.

Dependencies to: No dependencies.

FTP_UIF_EXT.1.1

The TSF shall indicate to users which VM, if any, has the current input focus.

Management: FTP_UIF_EXT.2

There are no management functions foreseen.

Audit: FTP_UIF_EXT.2

There are no audit events foreseen.

FTP_UIF_EXT.2 User Interface: Identification of VM

Hierarchical to: No other components.

Dependencies to: No dependencies.

FTP_UIF_EXT.2.1

The TSF shall support the unique identification of a VM's output display to users.

C.2.6 User Data Protection (FDP)

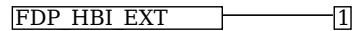
This PP defines the following extended components as part of the FDP class originally defined by CC Part 2:

C.2.6.1 FDP_HBI_EXT Hardware-Based Isolation Mechanisms

Family Behavior

This family defines requirements for isolation of guest VMs from the hardware resources of the physical device on which the guest VMs are deployed.

Component Leveling



[FDP_HBI_EXT.1](#), Hardware-Based Isolation Mechanisms, requires the TSF to identify the mechanisms used to isolate guest VMs from platform hardware resources.

Management: FDP_HBI_EXT.1

There are no management functions foreseen.

Audit: FDP_HBI_EXT.1

There are no audit events foreseen.

FDP_HBI_EXT.1 Hardware-Based Isolation Mechanisms

Hierarchical to: No other components.

Dependencies to: [FDP_VMS_EXT.1](#) VM Separation

FDP_HBI_EXT.1.1

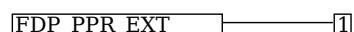
The TSF shall use [**selection**: no mechanism, [**assignment**: list of platform-provided, hardware-based mechanisms]] to constrain a guest VM's direct access to the following physical devices: [**selection**: no devices, [**assignment**: physical devices to which the VMM allows guest VMs physical access]].

C.2.6.2 FDP_PPR_EXT Physical Platform Resource Controls

Family Behavior

This family defines requirements for the physical resources that the TOE will allow or prohibit guest VMs to access.

Component Leveling



[FDP_PPR_EXT.1](#), Physical Platform Resource Controls, requires the TSF to define the hardware resources that guest VMs may always access, may never access, and may conditionally access based on administrative configuration.

Management: FDP_PPR_EXT.1

The following actions could be considered for the management functions in FMT:

- Ability to configure VM access to physical devices.

Audit: FDP_PPR_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Successful and failed VM connections to physical devices where connection is governed by configurable policy.
- b. Security policy violations.

FDP_PPR_EXT.1 Physical Platform Resource Controls

Hierarchical to: No other components.

Dependencies to: [FDP_HBI_EXT.1](#) Hardware-Based Isolation Mechanisms
[FMT_SMR.1](#) Security Roles

FDP_PPR_EXT.1.1

The TSF shall allow an authorized administrator to control guest VM access to the following physical platform resources: **[assignment]**: *list of physical platform resources the VMM is able to control access to*.

FDP_PPR_EXT.1.2

The TSF shall explicitly deny all guest VMs access to the following physical platform resources: **[selection]**: *no physical platform resources*, **[assignment]**: *list of physical platform resources to which access is explicitly denied*].

FDP_PPR_EXT.1.3

The TSF shall explicitly allow all guest VMs access to the following physical platform resources: **[selection]**: *no physical platform resources*, **[assignment]**: *list of physical platform resources to which access is always allowed*].

C.2.6.3 FDP_RIP_EXT Residual Information in Memory

Family Behavior

This family defines requirements for ensuring that allocation of data to a guest VM does not cause a disclosure of residual data from a previous VM.

Component Leveling



[FDP_RIP_EXT.1](#), Residual Information in Memory, requires the TSF to ensure that physical memory is cleared to zeros prior to its allocation to a guest VM.

[FDP_RIP_EXT.2](#), Residual Information on Disk, requires the TSF to ensure that physical disk storage is cleared upon allocation to a guest VM.

Management: FDP_RIP_EXT.1

There are no management functions foreseen.

Audit: FDP_RIP_EXT.1

There are no audit events foreseen.

FDP_RIP_EXT.1 Residual Information in Memory

Hierarchical to: No other components.

Dependencies to: No dependencies.

FDP_RIP_EXT.1.1

The TSF shall ensure that any previous information content of physical memory is cleared prior to allocation to a guest VM.

Management: FDP_RIP_EXT.2

There are no management functions foreseen.

Audit: FDP_RIP_EXT.2

There are no audit events foreseen.

FDP_RIP_EXT.2 Residual Information on Disk

Hierarchical to: No other components.

Dependencies to: No dependencies.

FDP_RIP_EXT.2.1

The TSF shall ensure that any previous information content of physical disk storage is cleared to zeros

upon allocation to a guest VM.

C.2.6.4 FDP_VMS_EXT VM Separation

Family Behavior

This family defines requirements for the logical separation of multiple guest VMs that are managed by the same virtualization system.

Component Leveling



[FDP_VMS_EXT.1](#), VM Separation, requires the TSF to maintain logical separation between guest VMs except through the use of specific configurable methods.

Management: FDP_VMS_EXT.1

The following actions could be considered for the management functions in FMT:

- a. Ability to configure inter-VM data sharing.

Audit: FDP_VMS_EXT.1

There are no audit events foreseen.

FDP_VMS_EXT.1 VM Separation

Hierarchical to: No other components.

Dependencies to: No dependencies.

FDP_VMS_EXT.1.1

The VS shall provide the following mechanisms for transferring data between guest VMs: [**selection**:

- *no mechanism*
- *virtual networking*
- [**assignment**: *other inter-VM data sharing mechanisms*]

].

FDP_VMS_EXT.1.2

The TSF shall by default enforce a policy prohibiting sharing of data between guest VMs.

FDP_VMS_EXT.1.3

The TSF shall allow administrators to configure the mechanisms selected in [FDP_VMS_EXT.1.1](#) to enable and disable the transfer of data between guest VMs.

FDP_VMS_EXT.1.4

The VS shall ensure that no guest VM is able to read or transfer data to or from another guest VM except through the mechanisms listed in [FDP_VMS_EXT.1.1](#).

C.2.6.5 FDP_VNC_EXT Virtual Networking Components

Family Behavior

This family defines requirements for configuration of virtual networking between guest VMs that are managed by the virtualization system.

Component Leveling



[FDP_VNC_EXT.1](#), Virtual Networking Components, requires the TSF to support the configuration of virtual networking between guest VMs.

Management: FDP_VNC_EXT.1

The following actions could be considered for the management functions in FMT:

- a. Ability to configure virtual networks including VM.

Audit: FDP_VNC_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a. Successful and failed attempts to connect VMs to virtual and physical networking components.
- b. Security policy violations.
- c. Administrator configuration of inter-VM communications channels between VMs.

FDP_VNC_EXT.1 Virtual Networking Components

Hierarchical to: No other components.

Dependencies to: [FDP_VMS_EXT.1](#) VM Separation
[FMT_SMR.1](#) Security Roles

FDP_VNC_EXT.1.1

The TSF shall allow administrators to configure virtual networking components to connect VMs to each other and to physical networks.

FDP_VNC_EXT.1.2

The TSF shall ensure that network traffic visible to a guest VM on a virtual network-or virtual segment of a physical network-is visible only to guest VMs configured to be on that virtual network or segment.

Appendix D - Implicitly Satisfied Requirements

This appendix lists requirements that should be considered satisfied by products successfully evaluated against this PP. These requirements are not featured explicitly as SFRs and should not be included in the ST. They are not included as standalone SFRs because it would increase the time, cost, and complexity of evaluation. This approach is permitted by [CC] Part 1, 8.3 Dependencies between components.

This information benefits systems engineering activities which call for inclusion of particular security controls. Evaluation against the PP provides evidence that these controls are present and have been evaluated.

Requirement Rationale for Satisfaction

FIA_UID.1 - Timing of Identification	FMT_SMR.2 has a dependency on FIA_UID.1. The extended SFR FIA_UID_EXT.1 expresses this dependency by also requiring user identification for use of the TOE.
FPT STM.1 - Reliable Time Stamps	FAU_GEN.1 has a dependency on FPT STM.1. While not explicitly stated in the PP, it is assumed that this will be provided by the underlying hardware platform on which the TOE is installed. This is because the TOE is installed as a software or firmware product that runs on general-purpose computing hardware so a hardware clock is assumed to be available.
FPT STM.1 - Reliable Time Stamps	FIA_X509_EXT.1 in the Functional Package for X.509, version 1.0 has a dependency on FPT STM.1. While not explicitly stated in the PP, it is assumed that this will be provided by the underlying hardware platform on which the TOE is installed. This is because the TOE is installed as a software or firmware product that runs on general-purpose computing hardware so a hardware clock is assumed to be available.

Appendix E - Entropy Documentation and Assessment

E.1 Design Description

Documentation shall include the design of the entropy source as a whole, including the interaction of all entropy source components. It will describe the operation of the entropy source to include how it works, how entropy is produced, and how unprocessed (raw) data can be obtained from within the entropy source for testing purposes. The documentation should walk through the entropy source design indicating where the random comes from, where it is passed next, any post-processing of the raw outputs (hash, XOR, etc.), if/where it is stored, and finally, how it is output from the entropy source. Any conditions placed on the process (e.g., blocking) should also be described in the entropy source design. Diagrams and examples are encouraged.

This design must also include a description of the content of the security boundary of the entropy source and a description of how the security boundary ensures that an adversary outside the boundary cannot affect the entropy rate.

E.2 Entropy Justification

There should be a technical argument for where the unpredictability in the source comes from and why there is confidence in the entropy source exhibiting probabilistic behavior (an explanation of the probability distribution and justification for that distribution given the particular source is one way to describe this). This argument will include a description of the expected entropy rate and explain how you ensure that sufficient entropy is going into the TOE randomizer seeding process. This discussion will be part of a justification for why the entropy source can be relied upon to produce bits with entropy.

E.3 Operating Conditions

Documentation will also include the range of operating conditions under which the entropy source is expected to generate random data. It will clearly describe the measures that have been taken in the system design to ensure the entropy source continues to operate under those conditions. Similarly, documentation shall describe the conditions under which the entropy source is known to malfunction or become inconsistent. Methods used to detect failure or degradation of the source shall be included.

E.4 Health Testing

More specifically, all entropy source health tests and their rationale will be documented. This will include a description of the health tests, the rate and conditions under which each health test is performed (e.g., at startup, continuously, or on-demand), the expected results for each health test, and rationale indicating why each test is believed to be appropriate for detecting one or more failures in the entropy source.

Appendix F - Equivalency Guidelines

F.1 Introduction

The purpose of equivalence in PP-based evaluations is to find a balance between evaluation rigor and commercial practicability--to ensure that evaluations meet customer expectations while recognizing that there is little to be gained from requiring that every variation in a product or platform be fully tested. If a product is found to be compliant with a PP on one platform, then all equivalent products on equivalent platforms are also considered to be compliant with the PP.

A Vendor can make a claim of equivalence if the Vendor believes that a particular instance of their Product implements PP-specified security functionality in a way equivalent to the implementation of the same functionality on another instance of their Product on which the functionality was tested. The Product instances can differ in version number or feature level (model), or the instances may run on different platforms. Equivalency can be used to reduce the testing required across claimed evaluated configurations. It can also be used during Assurance Maintenance to reduce testing needed to add more evaluated configurations to a certification.

These equivalency guidelines do not replace Assurance Maintenance requirements or NIAP Policy #5 requirements for CAVP certificates. Nor may equivalency be used to leverage evaluations with expired certifications.

This document provides guidance for determining whether Products and Platforms are equivalent for purposes of evaluation against the Protection Profile for Virtualization (VPP).

Equivalence has two aspects:

1. **Product Equivalence:** Products may be considered equivalent if there are no differences between Product Models and Product Versions with respect to PP-specified security functionality.
2. **Platform Equivalence:** Platforms may be considered equivalent if there are no significant differences in the services they provide to the Product--or in the way the platforms provide those services--with respect to PP-specified security functionality.

The equivalency determination is made in accordance with these guidelines by the Validator and Scheme using information provided by the Evaluator/Vendor.

F.2 Approach to Equivalency Analysis

There are two scenarios for performing equivalency analysis. One is when a product has been certified and the vendor wants to show that a later product should be considered certified due to equivalence with the earlier product. The other is when multiple product variants are going through evaluation together and the vendor would like to reduce the amount of testing that must be done. The basic rules for determining equivalence are the same in both cases. But there is one additional consideration that applies to equivalence with previously certified products. That is, the product with which equivalence is being claimed must have a valid certification in accordance with scheme rules and the Assurance Maintenance process must be followed. If a product's certification has expired, then equivalence cannot be claimed with that product.

When performing equivalency analysis, the Evaluator/Vendor should first use the factors and guidelines for Product Model equivalence to determine the set of Product Models to be evaluated. In general, Product Models that do not differ in PP-specified security functionality are considered equivalent for purposes of evaluation against the VPP.

If multiple revision levels of Product Models are to be evaluated--or to determine whether a revision of an evaluated product needs re-evaluation--the Evaluator/Vendor and Validator should use the factors and guidelines for Product Version equivalence to determine whether Product Versions are equivalent.

Having determined the set of Product Models and Versions to be evaluated, the next step is to determine the set of Platforms that the Products must be tested on.

Each non-equivalent Product for which compliance is claimed must be fully tested on each non-equivalent platform for which compliance is claimed. For non-equivalent Products on equivalent platforms, only the differences that affect PP-specified security functionality must be tested for each product.

If the set of equivalent Products includes only bare-metal installations, then the equivalency analysis is complete. But if any members of the set include hosted installations or installations that integrate with an existing host operating system or control domain, then software platform equivalence must be taken into consideration. The Evaluator/Vendor and Validator should use the factors and guidance for software platform equivalence to determine whether different models or versions of host or control domain operating systems require separate testing.

"Differences in PP-Specified Security Functionality" Defined

If PP-specified security functionality is implemented by the TOE, then differences in the actual implementation between versions or product models break equivalence for that feature. Likewise, if the TOE implements the functionality in one version or model and the functionality is implemented by the platform in another version or model, then equivalence is broken. If the functionality is implemented by the platform in multiple models or versions on equivalent platforms, then the functionality is considered different if the product invokes the platform differently to perform the function.

F.3 Specific Guidance for Determining Product Model Equivalence

Product Model equivalence attempts to determine whether different feature levels of the same product across a product line are equivalent for purposes of PP testing. For example, if a product has a "basic" edition and an

“enterprise” edition, is it necessary to test both models? Or does testing one model provide sufficient confidence that both models are compliant?

Table 11, below, lists the factors for determining Product Model equivalence.

Table 11: Factors for Determining Product Model Equivalence

Factor	Same/Different	Guidance
Target Platform	Different	Product Models that virtualize different instruction sets (e.g., x86, ARM, POWER, SPARC, MIPS) are not equivalent.
Installation Types	Different	If a Product can be installed either on bare metal or onto an operating system and the vendor wants to claim that both installation types constitute a single Model, then see the guidance for “PP-Specified Functionality,” below.
Software Platform	Different	Product Models that run on substantially different software environments, such as different host operating systems, are not equivalent. Models that install on different versions of the same software environment may be equivalent depending on the below factors.
PP-Specified Functionality	Same	If the differences between Models affect only non-PP-specified functionality, then the Models are equivalent.
	Different	If PP-specified security functionality is affected by the differences between Models, then the Models are not equivalent and must be tested separately. It is necessary to test only the functionality affected by the software differences. If only differences are tested, then the differences must be enumerated, and for each difference the Vendor must provide an explanation of why each difference does or does not affect PP-specified functionality. If the Product Models are fully tested separately, then there is no need to document the differences.

F.4 Specific Guidance for Determining Product Version Equivalence

In cases of version equivalence, differences are expressed in terms of changes implemented in revisions of an evaluated Product. In general, versions are equivalent if the changes have no effect on any security-relevant claims about the TOE or evaluation evidence. Non-security-relevant changes to TOE functionality or the addition of non-security-relevant functionality does not affect equivalence.

Table 12: Factors for Determining Product Version Equivalence

Factor	Same/Different	Guidance
Product Models	Different	Versions of different Product Models are not equivalent unless the Models are equivalent as defined in Section 3.
PP-Specified Functionality	Same	If the differences affect only non-PP-specified functionality, then the Versions are equivalent.
	Different	If PP-specified security functionality is affected by the differences, then the Versions are considered to be not equivalent and must be tested separately. It is necessary only to test the functionality affected by the changes. If only the differences are tested, then for each difference the Vendor must provide an explanation of why the difference does or does not affect PP-specified functionality. If the Product Versions are fully tested separately, then there is no need to document the differences.

F.5 Specific Guidance for Determining Platform Equivalence

Platform equivalence is used to determine the platforms that a product must be tested on. These guidelines are divided into sections for determining hardware equivalence and software (host OS/control domain) equivalence. If the Product is installed onto bare metal, then only hardware equivalence is relevant. If the Product is installed onto an OS—or is integrated into an OS—then both hardware and software equivalence are required. Likewise, if the Product can be installed either on bare metal or on an operating system, both hardware and software equivalence are relevant.

F.5.1 Hardware Platform Equivalence

If a Virtualization Solution runs directly on hardware without an operating system, then platform equivalence is based primarily on processor architecture and instruction sets.

Platforms with different processor architectures and instruction sets are not equivalent. This is probably not an issue because there is likely to be a different product model for different hardware environments.

Equivalency analysis becomes important when comparing platforms with the same processor architecture. Processors with the same architecture that have instruction sets that are subsets or supersets of each other

are not disqualified from being equivalent for purposes of a VPP evaluation. If the VS takes the same code paths when executing PP-specified security functionality on different processors of the same family, then the processors can be considered equivalent with respect to that application.

For example, if a VS follows one code path on platforms that support the AES-NI instruction and another on platforms that do not, then those two platforms are not equivalent with respect to that VS functionality. But if the VS follows the same code path whether or not the platform supports AES-NI, then the platforms are equivalent with respect to that functionality.

The platforms are equivalent with respect to the VS if the platforms are equivalent with respect to all PP-specified security functionality.

Table 13: Factors for Determining Hardware Platform Equivalence

Factor	Same/Different/None	Guidance
Platform Architectures	Different	Hardware platforms that implement different processor architectures and instruction sets are not equivalent.
PP-Specified Functionality	Same	For platforms with the same processor architecture, the platforms are equivalent with respect to the application if execution of all PP-specified security functionality follows the same code path on both platforms.

F.5.2 Software Platform Equivalence

If the Product installs onto or integrates with an operating system that is not installed with the product--and thus is not part of the TOE--then the Product must be tested on all non-equivalent Software Platforms.

The guidance for Product Model (Section 3) specifies that Products intended for use on substantially different operating systems (e.g., Windows vs. Linux vs. SunOS) are different Models. Therefore, platforms running substantially different operating systems are not equivalent. Likewise, operating systems with different major version numbers are not equivalent for purposes of this PP.

As a result, Software Platform equivalence is largely concerned with revisions and variations of operating systems that are substantially the same (e.g., different versions and revision levels of Windows or Linux).

Table 14: Factors for Determining Software Platform Equivalence

Factor	Same/Different/None	Guidance
Platform Type/Vendor	Different	Operating systems that are substantially different or come from different vendors are not equivalent.
Platform Versions	Different	Operating systems are not equivalent if they have different major version numbers.
PP-Specified Functionality	Same	If the differences between software platform models or versions affect only non-PP-specified functionality, then the software platforms are equivalent.
	Different	If PP-specified security functionality is affected by the differences between software platform versions or models, then the software platforms are not considered equivalent and must be tested separately. It is necessary only to test the functionality affected by the changes. If only the differences are tested, then for each difference the Vendor must provide an explanation of why the difference does or does not affect PP-specified functionality. If the Products are fully tested on each platform, then there is no need to document the differences.

F.6 Level of Specificity for Tested and Claimed Equivalent Configurations

In order to make equivalency determinations, the vendor and evaluator must agree on the equivalency claims. They must then provide the scheme with sufficient information about the TOE instances and platforms that were evaluated, and the TOE instances and platforms that are claimed to be equivalent.

The ST must describe all configurations evaluated down to processor manufacturer, model number, and microarchitecture version.

The information regarding claimed equivalent configurations depends on the platform that the VS was developed for and runs on.

Bare-Metal VS

For VSes that run without an operating system on bare-metal or virtual bare-metal, the claimed configuration must describe the platform down to the specific processor manufacturer, model number, and microarchitecture version. The Vendor must describe the differences in the TOE with respect to PP-specified security functionality and how the TOE operates differently to leverage platform differences (e.g., instruction set extensions) in the tested configuration versus the claimed equivalent configuration.

VS with OS Support

For VSes that run on an OS host or with the assistance of an OS, then the claimed configuration must describe the OS down to its specific model and version number. The Vendor must describe the differences in the TOE with respect to PP-specified security functionality and how the TOE functions differently to leverage platform differences in the tested configuration versus the claimed equivalent configuration.

Appendix G - Acronyms

Table 15: Acronyms

Acronym	Meaning
AES	Advanced Encryption Standard
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
DEP	Data Execution Prevention
DKM	Derived Keying Material
DSS	Digital Signature Standard
ECC	Elliptic Curve Cryptography
EP	Extended Package
FFC	Finite-Field Cryptography
FIPS	Federal Information Processing Standard
FP	Functional Package
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KDF	Key Derivation Function
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OE	Operational Environment
OS	Operating System
PKV	Public Key Verification
PP	Protection Profile
PP-Configuration	Protection Profile Configuration
PP-Module	Protection Profile Module
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SP	Special Publication
SPD	Security Policy Database
SSP	System Security Policy
ST	Security Target
SWID	Software Identification
TOE	Target of Evaluation
TPM	Trusted Platform Module
TSF	TOE Security Functionality
TSFI	TSF Interface

TSS	TOE Summary Specification
VM	Virtual Machine
VMM	Virtual Machine Manager
VS	Virtualization System

Appendix H - Bibliography

Table 16: Bibliography

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - <ul style="list-style-type: none">• Part 1: Introduction and general model, CCMB-2022-11-001, CC:2022, Revision 1, November 2022.• Part 2: Security functional requirements, CCMB-2022-11-002, CC:2022, Revision 1, November 2022.• Part 3: Security assurance requirements, CCMB-2022-11-003, CC:2022, Revision 1, November 2022.• Part 4: Framework for the specification of evaluation methods and activities, CCMB-2022-11-004, CC:2022, Revision 1, November 2022.• Part 5: Pre-defined packages of security requirements, CCMB-2022-11-005, CC:2022, Revision 1, November 2022.
[CEM]	Common Methodology for Information Technology Security Evaluation - <ul style="list-style-type: none">• Evaluation methodology, CCMB-2022-11-006, CC:2022, Revision 1, November 2022.