HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner

Assurance Activity Report

Version:	1.1
Date:	2023-11-14
Status:	RELEASE
Classification:	Public
Filename:	OCSI-CERT-ATS-02-2023_AAR_231114_v1.1
Product:	HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner
Sponsor:	HP Inc.
Evaluation Facility:	atsec information security srl
Certification ID:	OCSI-CERT-ATS-02-2023
Certification Body:	OCSI
Author(s):	Valerio Magliozzi
Quality Assurance:	Paolo Bernardon

atsec information security srl
Viale Regina Margherita, 302
00198 - Roma

Phone: +39-06-69758936
www.atsec.com

(Evaluation facility with accreditation number 10574 is accredited by SWEDAC as a Testing laboratory according to ISO/IEC 17025)

Classification Note

Public Information (public)

This classification level is for information that may be made available to the general public. No specific security procedures are required to protect the confidentiality of this information. Information classified “public” may be freely distributed to anyone inside or outside of atsec.

Information with this classification shall be clearly marked “public”, except that it is not required to mark “public” on printed marketing material obviously intended for publication.

Revision History

Version	Date	Author(s)	Changes to Previous Revision	Application Notes
1.0	2023-10-03	Valerio Magliozzi	First version	
1.1	2023-11-14	Valerio Magliozzi	First version	Addressed developer comments.

Table of Contents

List of Tables

1 Evaluation Basis and Documents

This evaluation is based on the "Common Criteria for Information Technology Security Evaluation" version 3.1 revision 5 [CC], the "Common Methodology for Information Technology Security Evaluation" [CEM] and the following extended methodologies:

- "CC and CEM addenda - Exact Conformance, Selection-Based SFRs, Optional SFRs" [CCDB-2017-05-17]; and
- "HardCopy Device Protection Profile" [HCDPPv1.0]

, as specified in the Security Target [ST].

The following scheme documents and interpretations have been considered:

- [CCEVS-TD0157]: "FCS_IPSEC_EXT.1.1 - Testing SPDs", version as of 2017-06-15.
- [CCEVS-TD0176]: "FDP_DSK_EXT.1.2 - SED Testing", version as of 2017-04-11.
- [CCEVS-TD0219]: "NIAP Endorsement of Errata for HCD PP v1.0", version as of 2017-07-07.
- [CCEVS-TD0253]: "Assurance Activities for Key Transport", version as of 2017-11-08.
- [CCEVS-TD0261]: "Destruction of CSPs in flash", version as of 2017-11-14.
- [CCEVS-TD0393]: "Require FTP_TRP.1(b) only for printing", version as of 2019-02-26.
- [CCEVS-TD0474]: "Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1", version as of 2019-12-04.
- [CCEVS-TD0494]: "Removal of Mandatory SSH Ciphersuite for HCD", version as of 2020-02-20.
- [CCEVS-TD0562]: "Test activity for Public Key Algorithms", version as of 2021-01-27.
- [CCEVS-TD0642]: "FCS_CKM.1(a) Requirement; P-384 keysize moved to selection", version as of 2022-06-17.
- [OCSI-NIS01]: "Scheme Information Notice No. 1/23 - Changes to LGP1", version 1.1 as of 2023-08-21.

- [OCSI-NIS02]: "Scheme Information Notice No. 2/23 - Changes to LGP2", version 1.1 as of 2023-08-21.
- [OCSI-NIS03]: "Scheme Information Notice No. 3/23 - Changes to LGP3", version 1.1 as of 2023-08-21.
- [OCSI-NIS04]: "Scheme Information Notice No. 4/23 - Assurance Continuity", version 1.1 as of 2023-08-21.
- [OCSI-NIS05]: "Scheme Information Notice No. 5/13 - Conditions for performing tests remotely in Common Criteria evaluations", version 1.1 as of 2023-08-21.

2 Evaluation Results

The evaluator work units have been performed, including: evaluator actions and analysis explicitly stated in the CEM; evaluator actions implicitly derived from developer action elements described in the CC Part 3; and evaluator confirmation that requirements for content and presentation of evidence elements described in the CC Part 3 have been met.

The evaluation was performed by informal analysis of the evidence provided by the sponsor.

2.1 Security Functional Requirements

2.1.1 Security audit (FAU)

2.1.1.1 Audit data generation (FAU_GEN.1)

TSS Assurance Activities

Assurance Activity AA-FAU_GEN.1-ASE-01

The evaluator shall check the TOE Summary Specification (TSS) to ensure that auditable events and its recorded information are consistent with the definition of the SFR.

Summary

The Security Target [ST] provides the TOE summary specification (TSS) in section 7 "TOE Summary Specification", describing how each security functional requirement (SFR) defined in section 6.1 "TOE Security Functional Requirements" of [ST] is addressed by the TOE.

The evaluator noted that the TSS provides Table 39 "TSS Index" and Table 40 "TOE SFR compliance rationale" where Table 39 provides a quick index to each SFR's entry described in Table 40.

Table 40 is a comprehensive nested table which provides for each SFR a corresponding TSS description and a mapping to applicable security objective(s).

Section 6.1.1.1 "Audit data generation (FAU_GEN.1)" of [ST] contains Table 20 "Auditable Events" listing the auditable events that the TOE generates which include those from [HCDPPv1.0] as well as additional ones from the vendor.

The evaluator found the description of FAU_GEN.1 is provided in the table entry "FAU_GEN.1 (Audit generation)" of Table 40. This table entry states that the TOE generates audit records for the audit events specified in [HCDPPv1.0] as well as additional vendor-specific audit events defined in Table 41 "TOE audit records". The evaluator compared Table 41 in the TSS to Table 20 in the FAU_GEN.1 definition and verified that Table 41 contains the same set of auditable events as well as their corresponding recorded information found in Table 20. Thus, the evaluator concluded that the TSS description is consistent with the definition of the SFR. Additionally, the evaluator notes that each auditable event listed in Table 41 of the TSS is mapped to the log message category and records described in the main guidance document Common Criteria Evaluated Configuration Guide, [CCECG]. For example, the auditable event "Job completion" is mapped to the "Job completion" category and a number of job (email job completion, save (scan) to SharePoint job completion, save (scan) to Network Folder job completion, job Notification completion) completion records that are described in detail in [CCECG].

Guidance Assurance Activities

Assurance Activity AA-FAU_GEN.1-AGD-01

The evaluator shall check the guidance documents to ensure that auditable events and its recorded information are consistent with the definition of the SFRs.

Summary

[CCECG] chapter 7 "Enhanced security event logging messages", section "Enhanced security event logging" provides relevant guidance for FAU_GEN.1. This section provides the following information:

- Outline of the format of syslog messages in Table 7-1 "Syslog message format for enhanced security event logging".
- Description of the common variables/parameters found in these logging messages in Table 7-2 "Variables within syslog messages for enhanced security event logging".
- Description of the logging messages specified in FAU_GEN.1.

The evaluator constructed the following table to determine whether the guidance documentation sufficiently describes the auditable events defined in FAU_GEN.1 (i.e., in Table 20 "Auditable Events") of [ST]. For each auditable event defined in Table 20 of [ST], the evaluator searched for relevant audit record description in [CCECG] section "Enhanced security event logging messages" and determined whether the description meets the general requirements of FAU_GEN.1 (e.g., user identity, timestamp) as well as the additional information specified in Table 20 of [ST].

Table 1: Auditable Events

Auditable events	Relevant SFR(s)	Additional information	Provided guidance [HCDPPv1.0]
Job completion	FDP_ACF.1	Type of job	The various audit records described in subsection "Job completion" contain all the information required by FAU_GEN.1. In particular, the audit records contain the "scanner" field which indicates the type of job that was completed. For example, the audit record for a scan to Email job shows the following: **Message:** `scanner: E-mail job completion; time="<timestamp>" user="<user>" outcome=canceled`
Unsuccessful user authentication	FIA_UAU.1	Required by [HCDPPv1.0]: - None	The audit records described in subsection "User authentication", which cover control panel sign in, EWS sign in and REST Web Services authentication, contain all the information required by FAU_GEN.1. In particular, the audit records have the "Variables" field which includes the user identity as follows: Control panel sign-in **Message:** `scanner: Control Panel Sign In Authentication; time="<timestamp>" sign-in_method=<sign-in method> user="<user>" outcome=failure` **Variables:** `<user> - Attempted user identity.`

Auditable events	Relevant SFR(s)	Additional information	Provided guidance [HCDPPv1.0]
			EWS sign-in **Message:** scanner: EWS Sign In Authentication; time="<timestamp>" sign-in_method=<sign-in method> user="<user>" outcome=failure **Variables:** <user> - Attempted user identity. REST Web Services authentication **Message:** scanner: WS Sign In Authentication; time="<timestamp>" sign-in_method=<sign-in method> user="<user>" source_IP="<client computer IP address>" outcome=failure **Variables:** <sign-in method> - Sign-in method that was used to perform authentication. Possible values are: • local_device • windows <user> - Attempted user identity.
Unsuccessful user identification	FIA_UID.1	Required by [HCDPPv1.0]: - None Added by vendor: - The attempted user identity	Please see assessment in the previous table entry.
Use of management functions	FMT_SMF.1	None	Aspects of the use of management functions are covered throughout the audit records described in subsection "Syslog messages" including the audit records for "NTP server settings", "Syslog settings", "Enhanced security event logging", "Control panel inactivity-timeout", "EWS session timeout", "Account lockout policy", "Minimum password length", etc. The evaluator examined the audit record descriptions and determined the claimed management function are sufficiently covered including the information required by FAU_GEN.1.
Modification to the group of Users that are part of a role	FMT_SMR.1	None	The audit records for "Custom permission sets", "Permissions set association", and "Permissions associated with permission sets" sufficiently demonstrate modification of user roles and permissions. The evaluator examined the description of these audit records and determined that they contain sufficient details as required by FAU_GEN.1.

Auditable events	Relevant SFR(s)	Additional information	Provided guidance [HCDPPv1.0]

Changes to the time	FPT_STM.1	Required by [HCDPPv1.0]:
		- None
		Added by vendor:
		- New date and time
		- Old date and time
			The audit records described in subsection "System time" describe time change. The "Variables" field of these audit records provides the old and new values for date and time as follows:
			`<value> - New system time.`
			`<old value> - Old system time.`

Failure to establish session	FTP_ITC.1, FTP_TRP.1(a)	Required by [HCDPPv1.0]: - Reason for failure Added by vendor: - Non-TOE endpoint of connection (e.g., IP address)	The audit records for "IKEv1 phase 1 negotiations" and "IKEv1 phase 2 negotiations" cover failure to establish a trusted session. In particular the "Variables" field includes description for reason for the failure and the IP address of the IPsec peer (i.e., non-TOE connection endpoint). Reason for failures are outlined in Table 7-3 "<reason for failure> variable contained within syslog messages".

Locking an account	FIA_AFL.1	User name associated with account	The audit records for "Account entered lockout (protected) mode" and "Account lockout policy" cover locking an account. The "account" attribute within the message of the Account lockout policy specifies the user who modified the account lockout policy.
			Message: `scanner: Account Lockout Policy setting modified; time="<timestamp>" account=local_administrator item=maximum_login_attempts value="<value>" old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success`
			Explanation: `The maximum attempts setting for the device administrator account lockout policy was modified.`
			Variables:
			`<value> - New setting value.`
			`<old value> - Old setting value.`

Unlocking an account	FIA_AFL.1	User name associated with account	The audit records for "Account exited lockout (protected) mode" and "Account lockout policy" cover locking an account. The "account" attribute within the message of the Account lockout policy specifies the user who modified the account lockout policy. **Message:** `scanner: Account Lockout Policy setting modified; time="<timestamp>" account=local_administrator item=counter_reset_time value="<value>"`

Auditable events	Relevant SFR(s)	Additional information	Provided guidance [HCDPPv1.0]
			old_value="<old value>" user="<user>" source_IP="<client computer IP address>" outcome=success **Explanation:** The reset lockout interval setting for the device administrator account lockout policy was modified. **Variables:** <value> - New setting value. <old value> - Old setting value.

Test Assurance Activities

Assurance Activity AA-FAU_GEN.1-ATE-01

The evaluator shall also perform the following tests:

The evaluator shall check to ensure that the audit record of each of the auditable events described in Table 1 of [HCDPPv1.0] *is appropriately generated.*

The evaluator shall check a representative sample of methods for generating auditable events, if there are multiple methods.

The evaluator shall check that FIA_UAU.1 events have been generated for each mechanism, if there are several different I&A mechanisms.

Summary

The evaluator performed several tests to verify that correct log events were recorded. The results are presented in the table below and cover Test 1, Test 2 and Test 3.

Table 2: Tests mapped to Auditable events

Auditable events	Test
Start-up and shutdown of the audit functions	The evaluator verified that appropriate log messages were generated when enabling and disabling the audit function.
Job completion	The evaluator verified that appropriate log messages were generated when job was completed for scanning.

Unsuccessful user authentication	The evaluator verified that appropriate log messages were generated for unsuccessful user authentication using the following interfaces:
	• Control Panel:
	  ○ Local Device sign in
	  ○ LDAP sign in
	  ○ Windows (Kerberos) sign in
	• Embedded Web Server (EWS):
	  ○ Local Device sign in
	  ○ LDAP sign in

Auditable events	Test
	○ Windows (Kerberos) sign in • REST: ○ Local Device sign in ○ Windows (Kerberos) sign in
Unsuccessful user identification	The evaluator verified that appropriate log message were generated for unsuccessful user identification using the following interfaces: • Control Panel: ○ Local Device sign in ○ LDAP sign in ○ Windows (Kerberos) sign in • Embedded Web Server (EWS): ○ Local Device sign in ○ LDAP sign in ○ Windows (Kerberos) sign in • REST: ○ Local Device sign in ○ Windows (Kerberos) sign in
Use of management functions	The evaluator verified that appropriate log message were generated for all management functionality specified in FMT_SMF.1.
Modification to the group of Users that are part of a role	The evaluator verified that appropriate log message were generated when adding and removing users from a group, both U.NORMAL and U.ADMIN.
Changes to the time	The evaluator verified that appropriate log message were generated when modifying the time including that the log message contained new and old date and time.
Failure to establish session	The evaluator verified that appropriate log message were generated when failing to establish IPsec connections using both PSK and certificates.
Locking an account	The evaluator verified that appropriate log message were generated when locking an account.
Unlocking an account	The evaluator verified that appropriate log message were generated when unlocking an account.

2.1.1.2 User identity association (FAU_GEN.2)

No assurance activities defined for this SFR.

2.1.1.3 Extended: External audit trail storage (FAU_STG_EXT.1)

TSS Assurance Activities

Assurance Activity AA-FAU_STG_EXT.1-ASE-01

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. Testing of the trusted channel mechanism will be performed as specified in the associated assurance activities for the particular trusted channel mechanism.

The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. 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.

Summary

The evaluator examined Table 40 of the TSS in which table entry "FAU_STG_EXT.1 (Audit trail storage)" describes FAU_STG_EXT.1. It states the following:

- The TOE connects and sends audit records to an external syslog server for long-term storage and audit review. It uses the syslog protocol to transmit the records over an IPsec channel. The IPsec channel provides protection of the transmitted data and assured identification of both endpoints.
- The TOE contains two in-memory audit record message queues. One queue is for network audit records (e.g., IPsec records) generated and maintained by the Jetdirect Inside Firmware and the other queue is for HCD audit records (e.g., Control Panel Sign In events) generated and maintained by the HCD System Firmware. These in-memory message queues are not accessible through any TOE interface and, thus, are protected against unauthorized access.
- The network queue holds up to 15 audit records. New audit records are discarded when the network queue becomes full. The HCD queue holds up to 1000 audit records. New audit records replace the oldest audit records when the HCD queue becomes full.
- The TOE establishes a persistent connection to the external syslog server. An audit record is generated, added to a queue, immediately sent from the queue to the syslog server, and then removed from the queue once the record has been successfully received by the syslog server.
- If the connection is interrupted (e.g., network outage), the TOE will make 5 attempts to reestablish the connection where each attempt lasts for approximately 30 seconds. If all attempts fail, the TOE will repeat the reestablishment process again when a new audit record is added to the HCD queue. Once the connection is reestablished, the records from both queues are immediately sent to the syslog server.
- If the TOE is powered off, any audit records remaining in the two in-memory messages queues at the time of power-off will be discarded.

The evaluator also examined the operational guidance [CCECG] to determine if it describes the relationship between the local audit data and the audit data that are sent to the audit log server. Section "Enhanced security event logging" states that there are two in-memory audit record message queues: one for network audit records and the other for HCD audit records. The HCD establishes a persistent connection to the external syslog server. When an audit record is generated, it is added to a queue and immediately sent from the queue to the syslog server. The record is then removed from the queue once it has been successfully received by the syslog server.

The evaluator thus considered the provided information to be clear and sufficient. Also, the evaluator determined that the description from the TSS and operational guidance are consistent.

Guidance Assurance Activities

Assurance Activity AA-FAU_STG_EXT.1-AGD-01

The evaluator shall also 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.

Summary

The evaluator examined [CCECG] chapter 5 "Configure the HCD" section "Enhanced security event logging" which provides relevant guidance for FAU_STG_EXT.1. It states that the TOE generates audit records for security-relevant events and sends them to a syslog server on the network. It provides step-by-step instructions to set up the secure connection to the syslog servers via the EWS interface. The instructions explicitly indicate the use of TCP/IP for the connection. Also, the instructions specify the maximum storage of the syslog server which is 1000 messages. The communication channel must be protected by IPsec, instructions to set up an IPsec chanel to the Syslog Server are provided in subsections in [CCECG] chapter 5, section "IPsec".

Test Assurance Activities

Assurance Activity AA-FAU_STG_EXT.1-ATE-01

The evaluator shall perform the following test for this requirement:

Test 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.

Summary

The TOE uses IPsec to protect communication between itself and Trusted IT Products, e.g. audit server. The evaluator configured the TOE to send logs to an audit server and configured IPsec to protect the transmitted data using the provided configuration guide. The evaluator then started Wireshark on the audit server to record the traffic on the network interface. He then logged in to the TOE and changed several settings so that log messages were created and sent to the audit server. Afterwards, the evaluator checked the Wireshark logs and verified that all non-broadcast traffic was encrypted using IPsec.

2.1.2 Cryptographic support (FCS)

2.1.2.1 Cryptographic key generation (for asymmetric keys) (FCS_CKM.1(a))

TSS Assurance Activities

Assurance Activity AA-FCS_CKM.1-A-ASE-01

The evaluator shall ensure that the TSS contains a description of how the TSF complies with 800-56A and/or 800-56B, depending on the selections made. This description shall indicate the sections in 800-56A and/or 800-56B that are implemented by the TSF, and the evaluator shall ensure that key establishment is among those sections that the TSF claims to implement.

Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described in the TSS.

The TSS may refer to the Key Management Description (KMD), described in Appendix F [of the PP], that may not be made available to the public.

Summary

The evaluator examined Table 40 of the TSS in which table entry "FCS_CKM.1(a) (Asymmetric key generation)" describes FCS_CKM.1(a). It states the following:

- For IPsec IKEv1 KAS FFC, the TOE uses DH with the DSA key pair generation algorithm to establish a protected communication channel.
- For KAS FFC, the TOE uses the DH ephemeral (dhEphem) scheme with SHA2-256 for key establishment as per the NIST SP [SP800-56A-Rev3] standard Section 5.5.1.1 "FFC Domain Parameter Generation" tests FB and FC, Section 5.6.1.1 "FFC Key-Pair Generation," and Section 6.1.2.1 "dhEphem, C(2e, 0s, FFC DH) Scheme." The DH/DSA key pair generation supports the following values as per the [FIPS186-4] standard.
  - L=2048, N=224
  - L=2048, N=256
  - L=3072, N=256
- For KAS FFC, any necessary key material is obtained using the QuickSec 5.1 CTR_DRBG(AES) defined in FCS_RBG_EXT.1.
- The TOE does not implement the key derivation function (KDF) defined in the NIST SP [SP800-56A-Rev3] standard. Instead, the TOE implements the IPsec IKEv1 KDF. The IKEv1 KDF was not tested through the CAVP as CAVP testing of this KDF was considered optional by NIAP at the time of this evaluation.
- The TOE uses RSA-based X509v3 certificates for IPsec/IKEv1 authentication using the IPsec IKEv1 digital signature authentication method. (See FCS_COP.1(b) for RSA digital signature generation and verification.) The TOE does not perform RSA key pair generation. Instead, the RSA certificates are generated by the Operational Environment and imported by the TOE. Therefore, RSA key pair generation is not claimed in FCS_CKM.1(a).

The evaluator noted that the TSS explicitly stated that there are no TOE-specific extensions.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

Assurance Activity AA-FCS_CKM.1-A-ATE-01

The evaluator shall use the key pair generation portions of "The FIPS 186-4 Digital Signature Algorithm Validation System (DSA2VS)", "The FIPS 186-4 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and "The 186-4 RSA Validation System (RSA2VS)" as a guide in testing the requirement above, depending on the selection performed by the ST author. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

Summary

This test is covered by CAVP tests and performed using the CAVP tool. Please see [CAVP_TEST] for references to the CAVP testing, [HP_CAVS], the description of the test and examination approach provided in ATE_IND.1-3 for more information.

2.1.2.2 Cryptographic key generation (symmetric keys) (FCS_CKM.1(b))

TSS Assurance Activities

Assurance Activity AA-FCS_CKM.1-B-ASE-01

The evaluator shall review the TSS to determine that it describes how the functionality described by FCS_RBG_EXT.1 is invoked.

Summary

The evaluator examined Table 40 of the TSS in which table entry "FCS_CKM.1(b) (Symmetric key generation)" describes FCS_CKM.1(b). It states the following:

> *The TOE uses HP FutureSmart OpenSSL FIPS Object Module 2.0.4 CTR_DRBG(AES) defined in FCS_RBG_EXT.1 to generate the key used for the SED's drive-lock password(BEV).*

The evaluator notes that the TSS references the Key Management Documentation [KMD] document for description on how the TOE invokes the DRBG. The evaluator reviewed this document and determined that it does contain description on how these DRBGs are invoked.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

No assurance activities defined.

Key Management Assurance Activities

Assurance Activity AA-FCS_CKM.1-B-AKM-01

If the TOE is relying on random number generation from a third-party source, the KMD needs to describe the function call and parameters used when calling the third-party DRBG function. Also, the KMD needs to include a short description of the vendor's assumption for the amount of entropy seeding the third-party DRBG. The evaluator uses the description of the RBG functionality in FCS_RBG_EXT or the KMD to determine that the key size being requested is identical to the key size and mode to be used for the encryption/decryption of the user data (FCS_COP.1(d)).

The KMD is described in Appendix F [of the PP].

Summary

It is clearly stated in the [KMD] that the TOE uses its own entropy source and does not rely on any third-party entropy sources. This work unit is therefore not applicable and considered satisfied. Confidential details are omitted in this public AAR document.

2.1.2.3 Cryptographic key destruction (FCS_CKM.4)

TSS Assurance Activities

Assurance Activity AA-FCS_CKM.4-ASE-01

[TD0261]

The evaluator shall verify the TSS provides a high level description of how keys and key material are destroyed.

If the ST makes use of the open assignment and fills in the type of pattern that is used, the evaluator examines the TSS to ensure it describes how that pattern is obtained and used. The evaluator shall verify that the pattern does not contain any CSPs.

The evaluator shall check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.

Summary

The evaluator examined Table 40 of the TSS in which table entry "FCS_CKM.4 (Key destruction)" describes FCS_CKM.4. This table entry provides in Table 44 "TOE key destruction" the keys and key materials and how they are destroyed when no longer in use. Table 44 is reproduced in the Assurance Activity for FCS_CKM_EXT.4 above.

The evaluator noted that [ST] neither makes use of the open assignment nor fills in the type of pattern that is used, thus no TSS description is required.

The evaluator also noted that the TSS does not identify any configurations or circumstances that may not strictly conform to the key destruction requirement. In other words, according to Table 44, all CSPs are destroyed upon power off.

Guidance Assurance Activities

Assurance Activity AA-FCS_CKM.4-AGD-01

[TD0261]

There are a variety of concerns that may prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS and any other relevant Required Supplementary Information. The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer and how such situations can be avoided or mitigated if possible.

Some examples of what is expected to be in the documentation are provided here.

When the TOE does not have full access to the physical memory, it is possible that the storage may be implementing wear-leveling and garbage collection. This may create additional copies of the key that are logically inaccessible but persist physically. In this case, to mitigate this the drive should support the TRIM command and implements garbage collection to destroy these persistent copies when not actively engaged in other tasks.

Drive vendors implement garbage collection in a variety of different ways, as such there is a variable amount of time until data is truly removed from these solutions. There is a risk that data may persist for a longer amount of time if it is contained in a block with other data not ready for erasure. To reduce this risk, the operating system and file system of the OE should support TRIM, instructing the non-volatile memory to erase copies via garbage collection upon their deletion. If a RAID array is being used, only set-ups that support TRIM are utilized. If the drive is connected via PCI-Express, the operating system supports TRIM over that channel.

The drive should be healthy and contains minimal corrupted data and should be end of lifed before a significant amount of damage to drive health occurs, this minimizes the risk that small amounts of potentially recoverable data may remain in damaged areas of the drive.

Summary

The evaluator examined the both the TSS of [ST] and guidance documentation and could not identify any configuration or circumstances that may not strictly conform to the key destruction requirement specified in [ST], thus relevant guidance documentation is not required.

Test Assurance Activities

Assurance Activity AA-FCS_CKM.4-ATE-01

[TD0261]

For these tests the evaluator shall utilize appropriate development environment (e.g. a Virtual Machine) and development tools (debuggers, simulators, etc.) to test that keys are cleared, including all copies of the key that may have been created internally by the TOE during normal cryptographic processing with that key.

Test 1: Applied to each key held as in volatile memory and subject to destruction by overwrite by the TOE (whether or not the value is subsequently encrypted for storage in volatile or non-volatile memory). In the case where the only selection made for the destruction method key was removal of power, then this test is unnecessary. The evaluator shall:

1. *Record the value of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Cause the TOE to stop the execution but not exit.*
5. *Cause the TOE to dump the entire memory of the TOE into a binary file.*
6. *Search the content of the binary file created in Step #5 for instances of the known key value from Step #1.*

Steps 1-6 ensure that the complete key does not exist anywhere in volatile memory. If a copy is found, then the test fails.

Test 2: Applied to each key help in non-volatile memory and subject to destruction by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to ensure the tests function as intended.

1. *Identify the purpose of the key and what access should fail when it is deleted. (e.g. the data encryption key being deleted would cause data decryption to fail.)*
2. *Cause the TOE to clear the key.*
3. *Have the TOE attempt the functionality that the cleared key would be necessary for. The test succeeds if step 3 fails.*

Test 3: Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location:

1. *Record the value of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Search the non-volatile memory the key was stored in for instances of the known key value from Step #1. If a copy is found, then the test fails.*

Test 4: Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator shall use special tools (as needed), provided by the TOE developer if necessary, to view the key storage location:

1. *Record the storage location of the key in the TOE subject to clearing.*
2. *Cause the TOE to perform a normal cryptographic processing with the key from Step #1.*
3. *Cause the TOE to clear the key.*
4. *Search the storage location in Step #1 of non-volatile memory to ensure the appropriate pattern is utilized.*

The test succeeds if correct pattern is used to overwrite the key in the memory location. If the pattern is not found the test fails.

Summary

[ST] SFR FCS_CKM.4 selects only “For volatile memory, the destruction shall be executed by a removal of power to the memory".

[HCDPPv1.0] 4.5.4 "FCS_CKM.4 Cryptographic key destruction" states under "Test":

> "*There is no test for keys in volatile memory, since they are destroyed by powering down the TOE.*"

In addition the evaluator noted that also TD0261 is not applicable. Test 1 refers to keys held in volatile memory, but destroyed by the TOE by overwriting, Test 2 instead applies to keys held in non-volatile memory. Therefore, the evaluator determined this work unit as not applicable.

Key Management Assurance Activities

Assurance Activity AA-FCS_CKM.4-AKM-01

[TD0261]

The evaluator examines the KMD to ensure it describes how the keys are managed in volatile memory. This description includes details of how each identified key is introduced into volatile memory (e.g. by derivation from user input, or by unwrapping a wrapped key stored in non-volatile memory) and how they are overwritten.

The evaluator shall check to ensure the KMD lists each type of key that is stored in non-volatile memory, and identifies the memory type (volatile or non-volatile) where key material is stored.

The KMD identifies and describes the interface(s) that is used to service commands to read/write memory. The evaluator examines the interface description for each different media type to ensure that the interface supports the selection(s) made by the ST Author.

Summary

This work unit covers key destruction (FCS_CKM.4). [ST] section 6.1.2.4 "Cryptographic key destruction (FCS_CKM.4)" has only selected key destruction for volatile memory, and that keys should be destroyed by a removal of power to the memory.

The evaluator examined [KMD] and analyzed how the keys are managed in RAM, EEPROM, SPI flash and SED. The generation, memory location and destruction of different keys are included in the analysis. All keys stored in volatile memory (RAM) are destroyed when the HCD is powered off.

[KMD] also identifies and describes the interfaces that are used to service commands to read and write memory. There are four areas where keys are used: Storage encryption (Drive-lock password for SEDs), IPsec (PSK, RSA key pair, Session keys and intermediate key material), Trusted Update and TSF Testing.

The evaluator determined that the interfaces described in [KMD] that the administrator can use to access keys commensurate with the information provided in [ST].

The evaluator determined that [KMD] contains all necessary information to satisfy the requirements for this Work Unit.

2.1.2.4 Extended: Cryptographic key material destruction (FCS_CKM_EXT.4)

TSS Assurance Activities

Assurance Activity AA-FCS_CKM_EXT.4-ASE-01

The evaluator shall verify the TSS provides a high level description of what it means for keys and key material to be no longer needed and when then should be expected to be destroyed.

Summary

The evaluator examined Table 40 of the TSS in which table entry "FCS_CKM_EXT.4 (Key material destruction)" describes FCS_CKM_EXT.4. FCS_CKM_EXT.4 table entry refers to TSS for FCS_CKM.4. Table entry FCS_CKM.4 refers to Table 44 "TOE key destruction" which outlines the keys and key materials and how they are destroyed when no longer in use. Table 44 is reproduced below:

Table 3: TOE key destruction

Secret type	Usage	Storage location	No longer needed	When destroyed	Destruction algorithm
IPsec Diffie-Hellman (DH) private exponent	The private exponent used in DH exchange (generated by the TOE)	RAM	After DH shared secret generation	Power off	Power loss
IPsec DH shared secret	Shared secret generated by the DH key exchange (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec SKEYID	Value derived from the shared secret within IKE exchange (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec IKE session encrypt key	The IKE session encrypt key (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec IKE session authentication key	The IKE session authentication key (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec pre-shared key	The key used to generate the IKE SKEYID during pre-shared key authentication (entered by the administrator)	RAM	After SKEYID generation	Power off	Power loss
IPsec IKE RSA private key	RSA private key for IKE authentication	RAM	After session establishment	Power off	Power loss
IPsec encryption key	The IPsec encryption key (generated by the TOE)	RAM	Session termination	Power off	Power loss
IPsec authentication key	The IPsec authentication key	RAM	Session termination	Power off	Power loss

Secret type	Usage	Storage location	No longer needed	When destroyed	Destruction algorithm
Drive-lock password (BEV)	The SED password. Generated by the TOE.	RAM	After boot	Power off	Power loss

The table entry for FCS_CKM.4 also explains why the keys stored in nonvolatile memory do not need to be destroyed.

- The drive-lock password is generated once and stored in non-field replaceable nonvolatile memory (SPI flash and EEPROM) and does not get destroyed because it is always needed and also it is not accessible by any TOE user even administrators.
- Pre-shared keys and RSA private keys for IPsec stored on the SED are not destroyed since they are stored as ciphertext and not plaintext.

The evaluator verified that the TSS provides the necessary information about keys and key materials as well as their usage and destruction.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

No assurance activities defined.

Key Management Assurance Activities

Assurance Activity AA-FCS_CKM_EXT.4-AKM-01

The evaluator shall verify the Key Management Description (KMD) includes a description of the areas where keys and key material reside and when the keys and key material are no longer needed.

The evaluator shall verify the KMD includes a key lifecycle, that includes a description where key material reside, how the key material is used, how it is determined that keys and key material are no longer needed, and how the material is destroyed once it is not needed and that the documentation in the KMD follows FCS_CKM.4 for the destruction.

Summary

The evaluator reviewed [KMD] chapter 1 "Introduction" and could find four areas where keys are used:

- Storage encryption (Drive-lock password for SEDs)
- IPsec (Pre-shared keys, IPsec RSA private keys (X.509v3), Session keys and intermediate key material)
- Trusted Update (RSA 2048-bit public code signing key)
- TSF Testing (RSA 2048-bit X.509v3 public certificate)

For each of these areas, [KMD] describes how the keys are used, stored, protected, and destroyed.

The evaluator verified that the [KMD] contains a description of the areas where the keys and key material reside and when the keys and key material are no longer needed. The evaluator verified that it includes a lifecycle for the keys and how they are destroyed. The evaluator also verified that the description of key destruction is consistent with the SFR FCS_CKM.4 in [ST].

2.1.2.5 Cryptographic operation (symmetric encryption/decryption) (FCS_COP.1(a))

TSS Assurance Activities

No assurance activities defined.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

Assurance Activity AA-FCS_COP.1-A-ATE-01

The evaluator shall use tests appropriate to the modes selected in the above requirement from "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (these documents are available from http://csrc.nist.gov/groups/STM/cavp/index.html) as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

Summary

This test is covered by CAVP tests and performed using the CAVP tool. Please see [CAVP_TEST] for references to the CAVP testing, [HP_CAVS], the description of the test and examination approach provided in ATE_IND.1-3 for more information.

2.1.2.6 Cryptographic operation (for signature generation/verification) (FCS_COP.1(b))

TSS Assurance Activities

No assurance activities defined.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

Assurance Activity AA-FCS_COP.1-B-ATE-10

The evaluator shall use the signature generation and signature verification portions of "The Digital Signature Algorithm Validation System" (DSA2VS), "The Elliptic Curve Digital Signature Algorithm Validation System" (ECDSA2VS), and "The RSA Validation System" RSA2VS as a guide in testing the requirement above. The Validation System used shall comply with the conformance standard identified in the ST (i.e., FIPS PUB 186-4). This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

Summary

This test is covered by CAVP tests and performed using the CAVP tool. Please see [CAVP_TEST] for references to the CAVP testing, [HP_CAVS], the description of the test and examination approach provided in ATE_IND.1-3 for more information.

2.1.2.7 Cryptographic operation (hash algorithm) (FCS_COP.1(c))

TSS Assurance Activities

Assurance Activity AA-FCS_COP.1-C-ASE-10

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.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_COP.1(c) (SHS)" describes FCS_COP.1(c). It states the following:

- IKE supports the conditioning of text-based pre-shared keys using SHA-1, SHA2-256, and SHA2-512 hash algorithms as specified in FIA_PSK_EXT.1. IKE supports SHA2-256 for KAS FFC as specified in FCS_CKM.1(a). IKE supports SHA2-256, SHA2-384, and SHA2-512 for RSA signature generation and SHA-1, SHA2-256, SHA2-384, and SHA2-512 for RSA signature verification as specified in FCS_COP.1(b). Also, IKE supports HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 which use SHA2-256, SHA2-384, and SHA2-512, respectively. IKE uses the HP FutureSmart QuickSec 5.1 implementation for these algorithms.
- IPsec supports HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512 which use SHA-1, SHA2-256, SHA2-384, and SHA2-512, respectively. IPsec uses the HP FutureSmart QuickSec 5.1 implementation for these algorithms.
- The TOE's trusted update function uses the SHA2-256 algorithm for digital signature verification. This function uses the HP FutureSmart Rebex Total Pack 2017 R1 2470159 implementation of the SHA2-256 algorithm.
- The TOE's TSF testing (Whitelisting) functions use the SHA2-256 algorithm for RSA digital signature verification which is implemented by the HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937.

The evaluator therefore determined that the TSS documents the association of the hash function with other TSF cryptographic functions.

Guidance Assurance Activities

Assurance Activity AA-FCS_COP.1-C-AGD-01

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

Summary

[CCECG] chapter 5 "Configure the HCD", section "IPsec", subsection "IKE requirements" provides related guidance for text-based pre-shared keys. Table 5-3 and Table 5-4 of [CCECG] list the hash sizes supported in the evaluated configuration for IKEv1 phase 1 and phase 2, respectively. The instructions provided in section "Create an IKEv1 IPsec/Firewall template" contains a step to specify the hash value (if the hash option is selected) which must be one of the options specified in Table 5-3 for phase 1 and Table 5-4 for phase 2. The evaluator also verified the supported algorithms listed in Table 5-3 and Table 5-4 match with those specified in the SFR FCS_COP.1(c) from [ST]. In section “Certificates”, the [CCECG] provides also information for the SHA algorithms supported for signature verification of X.509 certificates during IPsec authentication, matching those specified in [ST].

Test Assurance Activities

Assurance Activity AA-FCS_COP.1-C-ATE-01

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 mode.

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.

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.

Summary

This test is covered by CAVP tests and performed using the CAVP tool. Please see [CAVP_TEST] for references to the CAVP testing, [HP_CAVS], the description of the test and examination approach provided in ATE_IND.1-3 for more information.

Assurance Activity AA-FCS_COP.1-C-ATE-02

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.

Summary

This test is covered by CAVP tests and performed using the CAVP tool. Please see [CAVP_TEST] for references to the CAVP testing, [HP_CAVS], the description of the test and examination approach provided in ATE_IND.1-3 for more information.

Assurance Activity AA-FCS_COP.1-C-ATE-03

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. For SHA-256, the length of the i-th message is 512 + 99*i, where 1 <= i <= m. For SHA-512, the length of the i-th message is 1024 + 99*i, where 1 <= i <= 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.*

Summary

This test is covered by CAVP tests and performed using the CAVP tool. Please see [CAVP_TEST] for references to the CAVP testing, [HP_CAVS], the description of the test and examination approach provided in ATE_IND.1-3 for more information.

Assurance Activity AA-FCS_COP.1-C-ATE-04

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. For SHA-256, the length of the i-th message is 512 + 8*99*i, where 1 <= i <= m/8. For SHA-512, the length of the i-th message is 1024 + 8*99*i, where 1 <= i <= 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.*

Summary

This test is covered by CAVP tests and performed using the CAVP tool. Please see [CAVP_TEST] for references to the CAVP testing, [HP_CAVS], the description of the test and examination approach provided in ATE_IND.1-3 for more information.

Assurance Activity AA-FCS_COP.1-C-ATE-05

Pseudorandomly Generated Messages Test

This test is for byteoriented 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 The Secure Hash Algorithm Validation System (SHAVS). The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.

Summary

This test is covered by CAVP tests and performed using the CAVP tool. Please see [CAVP_TEST] for references to the CAVP testing, [HP_CAVS], the description of the test and examination approach provided in ATE_IND.1-3 for more information.

2.1.2.8 Cryptographic operation (for keyed-hash message authentication) (FCS_COP.1(g))

TSS Assurance Activities

No assurance activities defined.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

Assurance Activity AA-FCS_COP.1-G-ATE-01

The evaluator shall use "The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)" as a guide in testing the requirement above. This will require that the evaluator have a reference implementation of the algorithms known to be good that can produce test vectors that are verifiable during the test.

Summary

This test is covered by CAVP tests and performed using the CAVP tool. Please see [CAVP_TEST] for references to the CAVP testing, [HP_CAVS], the description of the test and examination approach provided in ATE_IND.1-3 for more information.

2.1.2.9 Extended: IPsec selected (FCS_IPSEC_EXT.1)

FCS_IPSEC_EXT.1.1

TSS Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.1-ASE-01

The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the algorithm used to process the packet. 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 those rules and actions form the SPD in terms of the 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.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_IPSEC_EXT.1 (IPsec)" describes FCS_IPSEC_EXT.1. It states the following:

- The TOE's IPsec processes packets following the policy order defined in the Security Policy Database (SPD). The first matching policy is used to process the packet. The final policy in the SPD matches all unmatched packets and causes the TOE to discard the packet.
- The TOE processes incoming packets as follows:
  - When the TOE receives an incoming packet, it determines whether or not the packet is destined for the TOE. If not destined for the TOE, the packet is discarded. If destined for the TOE, the firewall rules are applied. The firewall rules map address templates to service templates. In essence, the rules map IP addresses to ports. The default rule is to discard (i.e., drop) all packets that do not match a firewall rule. This default rule can be modified by an administrator. Also, if the packet is not an IPsec protected packet, the packet is discarded except for the DHCPv4/BOOTP, DHCPv6, ICMPv4, and ICMPv6 service packets which are bypassed. The TOE's simplicity of the rule configuration helps to avoid overlapping rules, but if one or more overlapping rules exist, the first matching rule is the rule that is enforced. Administrators can add, delete, enable, and disable rules as well as modify the processing order of existing rules.
  - If the packet is a request for a new connection, then the IKE negotiation is performed to establish SAs based on the connection rules in the SPD. This negotiation supports both pre- shared keys and certificates. Next, the packet is compared against the set of known SAs. If the packet fails to match an SA, the packet is discarded. The SA is checked to ensure that the SA's lifetime has not expired and that the amount of data allowed by the SA has not been exceeded. If any of these checks fail, the packet is discarded. If all the checks succeed, the IPsec portion of the packet processing is considered complete and the packet is processed as part of the connection's flow.
- The TOE processes outgoing packets as follows:

- The TOE originates packets over established IPsec connections. Because of this, only protected (encrypted) packets are sent from the TOE to connected IT entities. The exceptions being for the DHCPv4/BOOTP, DHCPv6, ICMPv4, and ICMPv6 service packets which are bypassed. The TOE does not forward packets received from other devices.
- Protected packets being transmitted are compared to the SPD rules for that interface. Again, the first matching rule applies. Packets matching an SPD rule are encrypted and sent to the IT entity. All other packets are discarded. If this is the first transmission, an SA is created based on the SPD connection rules.

Guidance Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.1-AGD-01

The evaluator shall examine the guidance documentation 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 guidance documentation is consistent with the description in the TSS, and that the level of detail in the guidance documentation 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.

Summary

[CCECG] chapter 5 "Configure the HCD" section "IPsec" provides related guidance on IPsec. Subsection "Configure IPsec/Firewall rules" contains instructions for how to create (including setting the ordering of rules) IPsec/Firewall rules on the TOE (via the EWS) including rules for DISCARD, BYPASS and PROTECT. In particular the instructions for defining the DROP action for the TOE states that when incoming or outgoing traffic does not match any of the user-defined IPsec/Firewall rules, the traffic is processed by the default IPsec/Firewall rule. In the evaluated configuration, the action-on-match for the default IPsec/Firewall rule must be set to drop traffic. Likewise, the instructions for defining the BYPASS action states that in the evaluated configuration, the traffic for DHCPv4/BOOTP, DHCPv6, ICMPv4, and ICMPv6 services must be allowed to bypass the IPsec/Firewall policy. The traffic for all other services must be processed using the rules in the IPsec/Firewall policy.

The information is found to be consistent with the description of the TSS. In particular both documents explicitly specify that only DHCPv4/BOOTP, DHCPv6, ICMPv4, and ICMPv6 services are permitted to bypass the IPsec/Firewall policy. Also, the evaluator found the instructions to be very detailed and clear which includes cautions to the reader with respect to the evaluated configuration, such as:

In the evaluated configuration, the following rules must be created:

- *One rule for the Administrative Computer*
- *At least one rule for the Trusted IT Products*

Assurance Activity AA-FCS_IPSEC_EXT.1.1-AGD-02

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 DISCARD, BYPASS and PROTECT.

Summary

[CCECG] chapter 5 "Configure the HCD" section "IPsec" provides related guidance on IPsec. It contains instructions for how to create, modify the order, disable, enable, and delete IPsec/Firewall rules on the TOE (via the EWS) including rules for DISCARD, BYPASS and PROTECT. In particular,

subsections "Set the action for the default IPsec/Firewall rule to drop traffic" and "Configure broadcast and multicast bypass options" describes how to define/select the DROP and BYPASS actions for the TOE to take when traffic matches the criteria in the IPsec/Firewall rules. Also, this section explicitly specify that only DHCPv4/BOOTP, DHCPv6, ICMPv4, and ICMPv6 services are permitted to bypass.

Test Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.1-ATE-01

[TD0157] The evaluator uses the operational guidance to configure the TOE to carry out the following tests:

1. *Test 1: The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and (if configurable) 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.*
2. *Test 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 must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and guidance documentation. 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 guidance documentation.*

Summary

Test 1 and 2

The evaluator set up Wireshark on a computer and recorded all network traffic. The TOE supports dropping a packet and encrypting a packet. The evaluator first sent correct traffic matching IPsec rules and traffic was not dropped, since a SA has been established. He then sent incorrect traffic that not match any IPsec rule and the traffic was dropped, since no SA has been established. He then repeated the test when computer had matching IPsec rules, the traffic was not dropped. He then tried to send traffic from TOE to computer when computer did not have matching IPsec rules, the traffic was dropped. The evaluator also tested overlapping IP ranges and sent traffic from computer to the TOE. The TOE responded correctly and accepted valid traffic. Relevant logs, e.g. IKEv1 Phase 1 SA and Phase 2 SA were also recorded in the audit server, for more information see [ManualTestResults].

FCS_IPSEC_EXT.1.2

TSS Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.2-ASE-01

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

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_IPSEC_EXT.1 (IPsec)" describes FCS_IPSEC_EXT.1. It states that the VPN operates in transport mode only in the evaluated configuration. The evaluator found this description consistent with FCS_IPSEC_EXT.1.2 which specifies transport mode.

Guidance Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.2-AGD-01

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

Summary

[CCECG] chapter 5, "Configure the HCD", section "IPsec", subsection "Configure IPsec/Firewall templates" provides related guidance on IPsec. The instructions for creating a IPsec/Firewall policy (via the EWS interface) includes a step to select the transport mode as defined in FCS_IPSEC_EXT.1.2 of [ST].

Test Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.2-ATE-02

The evaluator shall perform the following test(s) based on the selections chosen:

1. *(conditional): If tunnel mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in tunnel mode and also configures an IPsec Peer to operate in tunnel mode. The evaluator configures the TOE and the IPsec 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 client to connect to the IPsec Peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.*
2. *(conditional): If transport mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in transport mode and also configures an IPsec Peer to operate in transport mode. The evaluator configures the TOE and the IPsec 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 to connect to the IPsec Peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.*

Summary

TOE supports only transport mode, therefore the test for tunnel mode is not applicable.

The evaluator configured the TOE to use IPsec using the provided guidance. He then configured IPsec on the following computers:

Table 4: IPsec configured computers

Computer Name	Role
Windows 7/10 Computer	Administrative. This computer provides access to TOE bios.
Windows Server 2016	Trusted IT product.
Debian Linux Computer	Administrative, Trusted IT product. This computer provides access to bios.

and successfully established a connection from the TOE to the computer. For more information about the computers in the VTL, please see [VTL].

FCS_IPSEC_EXT.1.3

TSS Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.3-ASE-01

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.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_IPSEC_EXT.1 (IPsec)" describes FCS_IPSEC_EXT.1. It states that packets are processed following the policy order defined in the SPD. The first matching policy is used to process the packet. The final policy in the SPD matches all unmatched packets and causes the TOE to discard the packet.

Guidance Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.3-AGD-01

The evaluator checks that the operational guidance provides instructions on how to construct the SPD and uses the guidance to configure the TOE for the following tests.

Summary

Per the Evaluation Activity, the operational guidance must provide instructions to configure the SPD such that it has entries that contain operations that DISCARD, BYPASS, and PROTECT network packets. The evaluator examined [CCECG] chapter 5 "Configure the HCD" section "IPsec" which provides related guidance on IPsec. The instructions for creating IPsec/Firewall rules via the EWS interface contains a step which is to select a radio button corresponding to the action/operation the TOE will take when traffic matches the criteria in the service templates. The options are as follows:

- When incoming or outgoing traffic does not match any of the user-defined IPsec/Firewall rules, the traffic is processed by the default IPsec/Firewall rule. In the evaluated configuration, the action-on-match for the default IPsec/Firewall rule must be set to drop traffic.
- In the evaluated configuration, the traffic for DHCPv4/BOOTP, DHCPv6, ICMPv4, and ICMPv6 services must be allowed to bypass the IPsec/Firewall Policy. The traffic for all other services must be processed using the rules in the IPsec/Firewall policy.

Test Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.3-ATE-03

The evaluator shall perform the following test:

The evaluator shall configure the SPD such that it has entries that contain operations that DISCARD, BYPASS, and PROTECT 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.

Summary

TD0157 modifies this work unit to remove the requirement to test BYPASS since many devices do not support a BYPASS function. The TOE only supports BYPASS for a few specific broadcast protocols: DHCPv4/BOOTP, DHCPv6, ICMPv4, and ICMPv6, as described in the Guidance Assurance Activity for FCS_IPSEC_EXT.1.1. Therefore the evaluator determined these tests are not applicable to the TOE.

FCS_IPSEC_EXT.1.4

TSS Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.4-ASE-01

The evaluator shall examine the TSS to verify that the symmetric encryption algorithms selected (along with the SHA-based HMAC algorithm, if AES-CBC is selected) are described. If selected, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1(g) Cryptographic Operations (for keyed-hash message authentication).

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_IPSEC_EXT.1 (IPsec)" describes FCS_IPSEC_EXT.1. It specifies the following symmetric encryption and HMAC algorithms:

- AES-CBC-128 and AES-CBC-256
- HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512

The evaluator found the above description to be consistent with FCS_COP.1(a) and FCS_COP.1(g), respectively. FCS_COP.1(a) ([ST] section 6.1.2.5) specifies data encryption and decryption algorithms for IKE and IPsec as follows: AES in CBC mode with key size 128 bits and 256 bits for symmetric data encryption and decryption. FCS_COP.1(g) ([ST] section 6.1.2.8) specifies HMAC-SHA1-96, HMAC-SHA2-256, HMAC-SHA2-384, and HMAC-SHA2-512.

Guidance Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.4-AGD-01

The evaluator checks the operational guidance to ensure it provides instructions on how to configure the TOE to use the algorithms selected by the ST author.

Summary

Per the definition of FCS_IPSEC_EXT.1.4, the ST selects the following algorithms:

- AES-CBC-128 with SHA-based HMAC
- AES-CBC-256 with SHA-based HMAC

The evaluator examined [CCECG] chapter 5 "Configure the HCD" section "IPsec" which provides related guidance on IPsec. The instructions for creating a IPsec/Firewall policy (via the EWS interface) is provided in subsection "Create an IKEv1 IPsec/Firewall template" which includes steps 20 and 26 according to the supported parameters listed in Table 5-3 for IKEv1 phase 1 and Table 5-4 for IKEv1 phase 2. The evaluator also verified the supported algorithms listed in these tables match with those specified in the SFR FCS_IPSEC_EXT.1.4 from [ST].

Test Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.4-ATE-01

The evaluator shall also perform the following tests:

The evaluator shall configure the TOE as indicated in the operational guidance configuring the TOE to using each of the selected algorithms, and attempt to establish a connection using ESP. The connection should be successfully established for each algorithm.

Summary

In [ST] 6.1.2.9 "Extended: IPsec selected (FCS_IPSEC_EXT.1)", FCS_IPSEC_EXT.1.4 states that the TOE supports the following cryptographic algorithms for IPsec ESP:

- AES-CBC-128 together with a Secure Hash Algorithm (SHA)-based HMAC
- AES-CBC-256 together with a Secure Hash Algorithm (SHA)-based HMAC

The TOE was configured to support AES-CBC-128, AES-CBC-256, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-384 and HMAC-SHA2-512 for IPsec ESP. The evaluator first configured the admin computer to use AES-CBC-128 together with HMAC-SHA1 and successfully established a connection to the TOE. Next, he configured the admin computer to use AES-CBC-128 together with HMAC-SHA256 and successfully connected to the TOE. After that, he configured the admin computer to use AES-CBC-256 together with HMAC-SHA-384 and successfully connected to the TOE. As the last step, he configured the admin computer to use AES-CBC-128 together with HMAC-SHA-512 and successfully connected to the TOE.

FCS_IPSEC_EXT.1.5

TSS Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.5-ASE-01

The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_IPSEC_EXT.1 (IPsec)" describes FCS_IPSEC_EXT.1. It explicitly indicates that only IKEv1 is supported. The evaluator found this description consistent with FCS_IPSEC_EXT.1.5 which specifies IKEv1.

Guidance Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.5-AGD-01

The evaluator shall check the operational guidance to ensure it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and uses the guidance to configure the TOE to perform NAT traversal for the following test if IKEv2 is selected.

Summary

[CCECG] chapter 5, "Configure the HCD", section "IPsec" provides related guidance on IPsec. The instructions for creating a IPsec/Firewall policy (via the EWS interface) includes a step to select IKEv1 for the evaluated configuration. Per the definition of FCS_IPSEC_EXT.1.5 of [ST], the TOE only supports IKEv1 thus no guidance on how to configure the TOE to perform NAT traversal is required.

Test Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.5-ATE-01

(conditional): If IKEv2 is selected, the evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 5996, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed.

Summary

IKEv2 is not supported in the evaluated configuration.

FCS_IPSEC_EXT.1.6

TSS Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.6-ASE-01

The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified, and if others are chosen in the selection of the requirement, those are included in the TSS discussion.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_IPSEC_EXT.1 (IPsec)" describes FCS_IPSEC_EXT.1. It explicitly states only AES-CBC-128 and AES-CBC-256 are used for encrypting the payload. The evaluator found this description to be consistent with FCS_IPSEC_EXT.1.6 which specifies IKEv1 using AES-CBC-128 and AES-CBC-256 and no other algorithm.

Guidance Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.6-AGD-01

The evaluator ensures that the operational guidance describes the configuration of the mandated algorithms, as well as any additional algorithms selected in the requirement. The guidance is then used to configure the TOE to perform the following test for each ciphersuite selected.

Summary

Per the definition of FCS_IPSEC_EXT.1.6, the ST selects the following algorithms:

- AES-CBC-128
- AES-CBC-256

The evaluator examined [CCECG] chapter 5 "Configure the HCD" section "IPsec" which provides related guidance on IPsec. The instructions for creating a IPsec/Firewall policy (via the EWS interface) in subsection "Create an IKEv1 IPsec/Firewall template" includes steps to specify the supported payload encryption algorithms (in the "Encryption" area) which must be one of the options specified in Table 5-3 for phase 1. The evaluator also verified the supported algorithms listed in Table 5-3 match with those specified in the SFR FCS_IPSEC_EXT.1.6 from [ST].

Test Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.6-ATE-01

The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv1 and/or 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.

Summary

In [ST] 6.1.2.9 "Extended: IPsec selected (FCS_IPSEC_EXT.1)", FCS_IPSEC_EXT.1.6 states that the TOE supports the following cryptographic algorithms for IKEv1:

- AES-CBC-128 as specified in RFC 3602
- AES-CBC-256 as specified in RFC 3602

The evaluator first configured the TOE to use AES-CBC-128 by following the instructions in the operational guidance. He then configured the admin computer to only support AES-CBC-128 and successfully established a connection to the TOE. Next, he configured TOE to use AES-CBC-256 by following the instructions in the operational guidance and configured the admin computer to only support AES-CBC-256, and successfully established a connection to the TOE.

FCS_IPSEC_EXT.1.7

TSS Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.7-ASE-01

The evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol supported by the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. It may be that this is a configurable option.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_IPSEC_EXT.1 (IPsec)" describes FCS_IPSEC_EXT.1. It explicitly states that the TOE's IKEv1 uses only Main Mode for Phase 1 exchanges and that Aggressive Mode is not supported and is not a configurable option. The evaluator found this description consistent with FCS_IPSEC_EXT.1.7 which specifies that the TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

Guidance Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.7-AGD-01

If the mode requires configuration of the TOE prior to its operation, the evaluator shall check the operational guidance to ensure that instructions for this configuration are contained within that guidance.

Summary

For FCS_IPSEC_EXT.1.7, [ST] specifies that the TOE shall ensure that IKEv1 Phase 1 exchanges use only Main mode, because Aggressive Mode is not supported and is not a configurable option.

The evaluator examined [CCECG] chapter 5 "Configure the HCD" section "IPsec" and noted that there is no reference for the configuration of IKEv1 phase 1 as Main mode is set automatically and Aggressive Mode is not selectable.

Test Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.7-ATE-01

The evaluator shall also perform the following test:

(conditional): The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported. This test is not applicable if IKEv1 is not selected above in the FCS_IPSEC_EXT.1.5 protocol selection.

Summary

The evaluator configured TOE and the admin computer according to guidance and was able to establish an IPsec connection. He then configured the admin computer to use aggressive mode and the connection failed.

FCS_IPSEC_EXT.1.8

TSS Assurance Activities

No assurance activities defined.

Guidance Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.8-AGD-01

The evaluator verifies that the values for SA lifetimes can be configured and that the instructions for doing so are located in the operational guidance. If time-based limits are supported, the evaluator ensures that the values allow for Phase 1 SAs values for 24 hours and 8 hours for Phase 2 SAs. Currently there are no values mandated for the number of packets or number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.

When testing this functionality, the evaluator needs to ensure that both sides are configured appropriately. From the RFC "A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. 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."

Summary

Per the definition of FCS_IPSEC_EXT.1.8, the SA lifetime can be established based on length of time where the time values is 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

[CCECG] chapter 5 "Configure the HCD" section "IPsec" provides related guidance on IPsec. The instructions for creating an IKEv1 IPsec/Firewall template (via the EWS interface) includes step 22 to specify a value for SA Lifetime for IKEv1 Phase 1 which must be 85500 seconds (23.75 hours) and step 28 for SA Lifetime for IKEv1 Phase 2 which must be 28800 seconds (8 hours).

Test Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.8-ATE-01

Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection:

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 renegotiated.*

2. *(Conditional): The evaluator shall construct a test where a Phase 1 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.*
3. *(Conditional): The evaluator shall perform a test similar to Test 1 for Phase 2 SAs, except that the lifetime will be 8 hours instead of 24.*

Summary

Test 1

Not applicable since allowed number (#) of packets (or bytes) was not selected in [ST] for this SFR.

Test 2

The evaluator configured the TOE according to operational guidance and the admin computer to use 40 hours for IKEv1 Phase 1 SA. He then initiated an IPsec connection and regularly sent traffic within the IPsec connection to maintain it. The evaluator observed a rekey before the 24h limit.

Test 3

The evaluator configured the TOE according to operational guidance and the admin computer to use 20 hours for IKEv1 Phase 2 SA. He then initiated an IPsec connection and regularly sent traffic within the connection to maintain it. The evaluator observed a rekey before the 8h limit.

FCS_IPSEC_EXT.1.9

TSS Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.9-ASE-01

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.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_IPSEC_EXT.1 (IPsec)" describes FCS_IPSEC_EXT.1. It states that the TOE's IKEv1 supports the following DH Groups. The DH groups are specified using a defined group description as specified in [RFC3526].

- DH Group 14 (2048-bit MODP)
- DH Group 15 (3072-bit MODP)
- DH Group 16 (4096-bit MODP)
- DH Group 17 (6144-bit MODP)
- DH Group 18 (8192-bit MODP)

The evaluator found this description to be consistent with FCS_IPSEC_EXT.1.9 ([ST] section 6.1.2.9) which specifies the following DH groups:

- DH Group 14 (2048-bit MODP),
- DH Group 15 (3072-bit MODP),
- DH Group 16 (4096-bit MODP),
- DH Group 17 (6144-bit MODP),

- DH Group 18 (8192-bit MODP).

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.9-ATE-01

> *The evaluator shall also perform the following test (this test may be combined with other tests for this component, for instance, the tests associated with FCS_IPSEC_EXT.1.1):*
>
> *For each supported DH group, the evaluator shall test to ensure that all IKE protocols can be successfully completed using that particular DH group.*

Summary

The evaluator notes that only IKEv1 and the following DH groups have been selected in [ST]:

- DH Group 14 (2048-bit MODP)
- DH Group 15 (3072-bit MODP)
- DH Group 16 (4096-bit MODP)
- DH Group 17 (6144-bit MODP)
- DH Group 18 (8192-bit MODP)

The evaluator set up Wireshark on the computer used to connect to the TOE and recorded all network traffic. The TOE was configured to support the above listed DH. The evaluator then configured the computer to use DH Group 14 and successfully connected to the TOE. He then verified in the network traffic logs that DH Group 14 was used during the initiation of the connection. The evaluator then repeated this for each DH Group. The test passed for each DH Group.

FCS_IPSEC_EXT.1.10

TSS Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.10-ASE-01

> *The evaluator shall check that the TSS contains a description of the IKE peer authentication process used by the TOE, and that this description covers the use of the signature algorithm or algorithms specified in the requirement.*

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_IPSEC_EXT.1 (IPsec)" describes FCS_IPSEC_EXT.1. It states that for IKEv1, the TOE supports peer authentication using either RSA-based digital signatures (RSA 2048-bit and 3072-bit) or pre-shared keys. The evaluator found this description consistent with FCS_IPSEC_EXT.1.10 which specifies RSA and pre-shared keys for peer authentication.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

Assurance Activity AA-FCS_IPSEC_EXT.1.10-ATE-01

The evaluator shall also perform the following test:

For each supported signature algorithm, the evaluator shall test that peer authentication using that algorithm can be successfully achieved and results in the successful establishment of a connection.

Summary

The evaluator configured the TOE and the admin computer to use certificate-based authentication (RSA algorithm) for IPsec and successfully established an IPsec connection between the TOE and the admin computer. He then configured the TOE and the admin computer to use Pre-shared Keys (PSK) and successfully established an IPsec connection between the TOE and the admin computer.

2.1.2.10 Extended: Key chaining (FCS_KYC_EXT.1)

TSS Assurance Activities

Assurance Activity AA-FCS_KYC_EXT.1-ASE-01

The evaluator shall verify the TSS contains a high-level description of the BEV sizes - that it supports BEV outputs of no fewer 128 bits for products that support only AES-128, and no fewer than 256 bits for products that support AES-256.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_KYC_EXT.1 (Key chaining)" describes FCS_KYC_EXT.1.

It states that the TOE uses a 256-bit drive-lock password (a.k.a BEV) to unlock the TOE's field-replaceable SED. The BEV is generated in accordance to the DRBG specified in FCS_RBG_EXT.1 and stored as a key chain of one in a SPI flash and EEPROM located inside the TOE. The evaluator verified that the TSS contains a high-level description of the BEV sizes, i.e. that it supports BEV outputs of no fewer than 256 bits as the product supports AES-256.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

No assurance activities defined.

Key Management Assurance Activities

Assurance Activity AA-FCS_KYC_EXT.1-AKM-01

The evaluator shall examine the KMD to ensure that it describes a high level description of the key hierarchy for all accepted BEVs. The evaluator shall examine the KMD to ensure it describes the key chain in detail. The description of the key chain shall be reviewed to ensure it maintains a chain of keys using key wrap, submask combining, or key encryption.

The evaluator shall examine the KMD to ensure that it describes how the key chain process functions, such that it does not expose any material that might compromise any key in the chain. (e.g. using a key directly as a compare value against a TPM) This description must include a diagram illustrating the key hierarchy implemented and detail where all keys and keying material is stored or what it is derived from. The evaluator shall examine the key hierarchy to ensure that at no point the chain could be broken without a cryptographic exhaust or the initial authorization value and the effective strength of the BEV is maintained throughout the Key Chain.

The evaluator shall verify the KMD includes a description of the strength of keys throughout the key chain.

Summary

The evaluator verified that the [KMD] includes descriptions of the key hierarchy for the BEV and the key chain. The evaluator also verified that the management of keys and key material will not expose any information that might compromise any key. It is clear how keys were generated and where they were stored. No point of failure was identified.

2.1.2.11 Extended: Cryptographic operation (random bit generation) (FCS_RBG_EXT.1)

TSS Assurance Activities

Assurance Activity AA-FCS_RBG_EXT.1-ASE-01

For any RBG services provided by a third party, the evaluator shall ensure the TSS includes a statement about the expected amount of entropy received from such a source, and a full description of the processing of the output of the third-party source. The evaluator shall verify that this statement is consistent with the selection made in FCS_RBG_EXT.1.2 for the seeding of the DRBG. If the ST specifies more than one DRBG, the evaluator shall examine the TSS to verify that it identifies the usage of each DRBG mechanism.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FCS_RBG_EXT.1 (DRBG)" describes FCS_RBG_EXT.1. It states the following DRBG mechanisms and their usage:

- IPsec uses the CTR_DRBG(AES) DRBG algorithm from HP FutureSmart QuickSec 5.1 to generate key and key material.
- The SED drive-lock password generation mechanism uses the CTR_DRBG(AES) algorithm from the HP FutureSmart OpenSSL FIPS Object Module 2.0.4 to generate the password (BEV).
- Both DRBGs are seeded by a hardware-based entropy noise source. This entropy source provides at least 256 bits of minimum entropy.

The evaluator determined that the above statements are consistent with the algorithm, noise source and minimum entropy specified in FCS_RBG_EXT.1. The TOE does not use any third-party RBG services, as stated in section 1 "Introduction" of [ST], the TOE is an entire device which comes with the HP FutureSmart QuickSec 5.1 crypto library and OpenSSL FIPS Object Module 2.0.4. Thus, the TSS does not make any statement about third-party source as it is not applicable.

Guidance Assurance Activities

Assurance Activity AA-FCS_RBG_EXT.1-AGD-01

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected DRBG mechanism(s), if necessary.

Summary

For FCS_RBG_EXT.1, [ST] lists the following supported DRBG mechanisms:

- CTR_DRBG(AES) provided by the HP FutureSmart QuickSec 5.1 for IKE/IPsec
- CTR_DRBG(AES) provided by HP FutureSmart OpenSSL FIPS Object Module 2.0.4 for generating the Drive-lock password (BEV).

Per [ST], these are the only DRBG mechanisms supported by the TOE in the evaluated configuration. In other words, they are the default DRBG mechanisms used by the TOE as there are no other mechanisms available. In [CCECG], subsection "Drive-lock password" states that in the evaluated configuration, a new random drive-lock password must be generated. The CTR_DRBG(AES) in the HP FutureSmart OpenSSL FIPS Object Module 2.0.4 is used in order to generate the drive-lock password.

Test Assurance Activities

Assurance Activity AA-FCS_RBG_EXT.1-ATE-01

The evaluator shall perform 15 trials for the RBG implementation. If the RBG is configurable by the TOE, the evaluator shall perform 15 trials for each configuration. The evaluator shall verify that the instructions in the operational guidance for configuration of the RBG are valid.

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 SP800-90A).

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 Derivation Function 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 support, 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.

Summary

This test is covered by CAVP tests and performed using the CAVP tool. Please see [CAVP_TEST] for references to the CAVP testing, [HP_CAVS], the description of the test and examination approach provided in ATE_IND.1-3 for more information.

Entropy Assurance Activities

Assurance Activity AA-FCS_RBG_EXT.1-AEN-01

The evaluator shall ensure the Entropy Description provides all of the required information as described in Appendix E [of the PP]. The evaluator assesses the information provided and ensures the TOE is providing sufficient entropy when it is generating a Random Bit String.

Summary

Appendix E "Entropy Documentation and Assessment"of [HCDPPv1.0] puts forth requirements on supplementary information for each entropy source with respect to design description, entropy justification, operating conditions and health testing. The evaluator analysed this information as follows.

E.1 Design Description

The evaluator went through the requirements on design description of entropy source in Appendix E.1 of [HCDPPv1.0] and found the answers in the [EAR]:

- *Design of each entropy source as a whole, including the interaction of all entropy source components:* the design of the hardware entropy source is described as a whole in [EAR] chapter 2 "Hardware entropy source", from the energization of ring oscillators, to the collection of raw data from ring oscillators, then to health testing and conditioning, and finally to the output of noise data. The interactions between the components are included in this description.
- *Operation of the entropy source:* the operation of the hardware entropy source is described in [EAR] chapter 2 "Hardware entropy source".
- *How entropy is produced:* section 2.1 "Design overview" in the [EAR] describes in detail the hardware entropy source, which consists of 5 hardware ring oscillators.
- *How uncompressed (raw) data can be obtained from within the entropy source for testing purposes:* as described in the [EAR] section 2.5 "KernelIoControl()", the KernelIoControl() call can output both unconditioned noise data (uncompressed raw data) and conditioned noise data.
- *Where the randomness comes from, where it is passed next:* the operation of the hardware entropy source is described in chapter 2 "Hardware entropy source" in the [EAR], and the operation of the software DRBGs is described in chapter 3 "DRBGs".
- *Any post-processing of the raw output:* as described in the [EAR] section 2.4 "Conditioning", the noise source firmware can add post-processing on the raw noise data.
- *If and where the output is stored:* the output is not stored anywhere. Random data is freshly gathered for every request. However, section 3.1.2 "InitRNG function" of [EAR] specifies how bytes of data are written and where they are stored.
- *How it is output from the entropy source:* as described in the [EAR] section 2.5 "KernelIoControl()", the entropy is output from the entropy source using a *KernelIoControl()* call, which gathers data from the ring oscillators.
- *Any conditions placed on the process, e.g., blocking:* as described in [EAR] section 3.1.2.2 "Handling of failure to obtain random data from the hardware entropy source" describes how the health test fails, stopping the gathering process and hanging the system, which means that it either does not boot or ceases to operate.
- *Content of the security boundary:* as described in the [EAR] section 2.1 "Design overview", the security boundary of the entropy source is the HCD itself.
- *How the security boundary ensures any adversary outside cannot affect the entropy rate:* the [EAR] chapter 6 "Mapping to the validator entropy spreadsheet" rationalizes that the ring oscillators and noise source firmware are located on the HP device, which are physically protected. This ensures that any adversary outside the boundary cannot affect the entropy rate.
- *How third-party applications can add entropy to the RBG:* the [EAR] chapter 3 "DRBGs" describes the third-party applications. However, the third-party applications cannot add entropy to the entropy source.

- *Any RBG state saving performed between power cycles:* as described in [EAR] section 2.2 "Noise source firmware" and 2.3 "Health testing", the ring oscillator are only energized when the crypto libraries (QuickSec or OpenSSL) call for random data. Entropy source state is not saved between power cycles.

E.2 Entropy Justification

The evaluator went through the requirements on entropy justification in Appendix E.2 of the [HCDPPv1.0] and found the answers in the [EAR]:

- *Where the unpredictability of the entropy source comes from:* [EAR] chapter 6 "Mapping to the validator entropy spreadsheet" rationalizes that the unpredictability of the noise source comes from the ring oscillators, their numbers, and frequency which is variable. Chapter 2 "Hardware entropy source" describes how the frequency of the ring oscillators varies and they are read in a random order, causing unpredictability of the result.
- *Why there is confidence the entropy source exhibits probabilistic behavior:* [EAR] chapter 6 "Mapping to the validator entropy spreadsheet" rationalizes that the statistical testing shows that the min-entropy combined with an over-sampling of the data to seed the DRBGs is compliant with SP 800-90A.
- *Expected entropy rate:* chapter 5 "Conclusion" in the [EAR] describes that the most conservative entropy estimate has enough bits of data per byte.
- *How TOE ensures sufficient entropy is received:* [EAR] chapter 4 "Min-entropy estimation for hardware entropy source" and chapter 5 "Conclusion" in the [EAR] rationalizes that the libraries (QuickSec and OpenSSL) seed their DRBG with sufficient entropy. Furthermore, health tests are performed on the raw noise data, as described in the [EAR] section 2.3 "Health Testing".

E.3 Operating Conditions

The evaluator went through the requirements on operating conditions in Appendix E.3 of [HCDPPv1.0] and found the answers in the [EAR]:

- *Range of operating conditions under which the source is expected to perform:* [EAR] section 4.2 "Operating environment settings" describes the 5 operating environment settings for testing. These were derived from an analysis of the recommended and allowed ranges for temperature and relative humidity for all product families listed in [EAR] Table 1-1 "HCD product models" to provide the most coverage.
- *Conditions under which the entropy source is no longer guaranteed to provide sufficient entropy:* it is rationalized in chapter 6 "Mapping to the validator entropy spreadsheet" of [EAR] that the HCD will operate within normal temperature and humidity ranges, and that statistical testing has been performed at high/low temperature and humidity, which does not significantly impact the entropy.
- *Methods to detect failure or degradation of the source:* it is rationalized in [EAR] chapter 6 "Mapping to the validator entropy spreadsheet" that the health test is performed on HCD boot and is constantly performed on the data being returned to the caller, which will detect failure or degradation of the source.

E.4 Health Testing

The evaluator went through the requirements on health testing in [HCDPPv1.0] and found the answers in the [EAR]:

- *Description of the health tests:* as described in chapter 6 "Mapping to the validator entropy spreadsheet" of [EAR], both software libraries (QuickSec and OpenSSL) performed their own self-tests internally on the AES-256 DRBG (continuous test on the output). The hardware entropy source performs the self-tests, as described in Section 2.3 "Health testing".

- *Rate and conditions under which each test is performed (e.g., at startup, continuously, or on-demand):* as described in chapters 2 "Hardware entropy source" and 3 "DRBGs" in the [EAR], the hardware ring oscillators are only energized when the crypto libraries (QuickSec or OpenSSL) call for random data. Health tests are performed on all the raw noise data collected from the ring oscillators. Therefore, the health testing can be considered as a continuous activity.
- *Expected results of each test:* section 2.3 "Health testing" in the [EAR] describes two health tests (repetitive count test and adaptive proportion test) with its parameters (expected results).
- *TOE behavior upon entropy source failure:* as described in section 2.5 "KernelIoControl()" of the [EAR] that the KernelIoControl() call returns zero bytes if the health tests fail, which is passed to the crypto libraries. The crypto libraries are described in chapter 3 "DRBGs" in the [EAR].
- *Rationale for why each test is appropriate for detecting failure:* as described in section 2.3 "Health testing" in the [EAR], the two health tests performed are the ones defined in the SP 800-90B standard.

The evaluator examined the Entropy Assessment Report (provided by the developer) and determined that it contains the information required by [HCDPPv1.0] on the design description, entropy justification and health testing. The CTR_DRBG is implemented according to SP 800-90A. Also, the evaluator determined that the information required by [HCDPPv1.0] on operating conditions is described in the provided Entropy Assessment Report.

In summary, the evaluator concluded that the entropy description provided by the developer contains all of the required information as described in Appendix E in [HCDPPv1.0]. The evaluator assessed the information provided and ensures the TOE is providing sufficient entropy when it is generating a Random Bit String. Confidential details are omitted in this public AAR document.

2.1.3 User data protection (FDP)

2.1.3.1 Subset access control (FDP_ACC.1)

TSS Assurance Activities

Assurance Activity AA-FDP_ACC.1-ASE-01

> *It is covered by assurance activities for FDP_ACF.1.*

Summary

This assurance activity is performed in conjunction with FDP_ACF.1.

Guidance Assurance Activities

Assurance Activity AA-FDP_ACC.1-AGD-01

> *It is covered by assurance activities for FDP_ACF.1.*

Summary

This assurance activity is performed in conjunction with the Evaluation Activity for FDP_ACF.1, AA-FDP_ACF.1-AGD-01.

Test Assurance Activities

Assurance Activity AA-FDP_ACC.1-ATE-01

It is covered by assurance activities for FDP_ACF.1.

Summary

Please see tests for FDP_ACF.1.

2.1.3.2 Security attribute based access control (FDP_ACF.1)

TSS Assurance Activities

Assurance Activity AA-FDP_ACF.1-ASE-01

The evaluator shall check to ensure that the TSS describes the functions to realize SFP defined in Table 2 and Table 3 of [HCDPPv1.0].

Summary

The evaluator checked Table 40 of the TSS in which table entry "FDP_ACF.1 (Security attribute based access control)" describes FDP_ACF.1.

First off, this table entry references Table 28 "D.USER.DOC Access Control SFP" and Table 29 "D.USER.JOB Access Control SFP" specified in FDP_ACF.1 ([ST] section 6.1.3.2). It describes access control for the following categories:

- Scan Create/Read/Modify/Delete D.USER.DOC in Table 28
- Scan Create/Read/Modify/Delete(Cancel) D.USER.JOB in Table 29

For each category, the TSS identifies the appropriate subject and object, the allowed operation(s), and the applicable interface(s), and authentication method, if any. The evaluator found the description very detailed and covers all the definitions of FDP_ACF.1 provided in Table 28 and Table 29 of [ST].

Guidance Assurance Activities

Assurance Activity AA-FDP_ACF.1-AGD-01

The evaluator shall check to ensure that the operational guidance contains a description of the operation to realize the SFP defined in Table 2 and Table 3 of [HCDPPv1.0]*, which is consistent with the description in the TSS.*

Summary

[CCECG] chapter 5 "Configure the HCD", section "System and network settings (excluding IPsec)", subsection "Access control" provides related guidance on access control. In particular subsection "Configure permission sets" describes access control policies (represented in the form of permission sets). Access types/levels and user roles are outlined in Table 5-2 "Permissions configuration for control panel realm". The evaluator analyzed these tables for consistency against Table 28 "D.USER.DOC Access Control SFP" and Table 29 "D.USER.JOB Access Control SFP" of [ST] which are drawn from Table 2 and Table 3 of [HCDPPv1.0]. The evaluator determined that the tables are consistent with one another.

Test Assurance Activities

Assurance Activity AA-FDP_ACF.1-ATE-01

The evaluator shall perform tests to confirm the functions to realize the SFP defined in Table 2 and Table 3 of [HCDPPv1.0] *with each type of interface (e.g., operation panel, Web interfaces) to the TOE.*

The evaluator testing should include the following viewpoints:

- *representative sets of the operations against representative sets of the object types defined in Table 2 and Table 3 of* [HCDPPv1.0] *(including some cases where operations are either permitted or denied)*
- *representative sets for the combinations of the setting for security attributes that are used in access control*

Summary

The evaluator performed several tests to confirm the functions defined in Table 2 and Table 3 in [HCDPPv1.0].

Table 5: Tests mapped to functions and interfaces

Function	Interface	Test
Scan	Control Panel	Authenticated as U.NORMAL and initiated a scan to network folder job, then signed out and signed in as another U.NORMAL and verified that the user could not read, modify or delete scan job. Then authenticated as Scan owner and verified that user could read and delete scan job. Then authenticated as U.ADMIN and verified that user could both view scan log and delete the scan job.
	EWS	Please note that only administrator has access to this interface. Authenticated as U.ADMIN and was able to view scan log.
	REST	Scan jobs cannot be accessed using this interface.

2.1.3.3 Extended: Protection of data on disk (FDP_DSK_EXT.1)

TSS Assurance Activities

Assurance Activity AA-FDP_DSK_EXT.1-ASE-01

[TD0176] If the self-encrypting device option is selected, the device must be certified in conformance to the current Full Disk Encryption Protection Profile. The tester shall confirm that the specific SED is listed in the TSS, documented and verified to be CC certified against the FDE EE cPP.

The evaluator shall examine the TSS to ensure that the description is comprehensive in how the data is written to the Device and the point at which the encryption function is applied.

For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes the interface(s) used by the TOE to invoke this functionality.

The evaluator shall verify that the TSS describes the initialization of the Device at shipment of the TOE, or by the activities the TOE performs to ensure that it encrypts all the storage devices entirely when a user or administrator first provisions the Device. The evaluator shall verify the TSS describes areas of the Device that it does not encrypt (e.g., portions that do not contain confidential data boot loaders, partition tables, etc.). If the TOE supports multiple Device encryptions, the evaluator shall examine the administration guidance to ensure the initialization procedure encrypts all Devices.

Summary

[ST] section 6.1.3.3 "Extended: Protection of Data on Disk (FDP_DSK_EXT.1)" defines FDP_DSK_EXT.1 which states that the TOE uses self-encrypting Field-Replaceable Nonvolatile Storage Devices that are separately CC certified to conform to the FDE EE cPP.

The evaluator checked Table 40 of the TSS in which table entry "FDP_DSK_EXT.1 (Disk data protection)" describes FDP_DSK_EXT.1. It describes that the TOE contains one field-replaceable, nonvolatile storage device that is a disk-based self-encrypting drive (SED), and states the following:

> [HCDPPv1.0] *states that SEDs must be CC certified using the Full Disk Encryption (FDE) Encryption Engine (EE) collaborative PP (cPP). The field-replaceable SED model used by TOE models is CC certified using the FDE EE cPP.*

The following is the product name, model, hardware version, and firmware version for the SED:

- Name: Seagate Secure TCG SSC SED
- Model: ST500LM033
- Hardware version: 1RD17D
- Firmware version: RTE2

The SED is CC certified and the following is the information for the CC certification:

- NIAP: VID11209
- Security Target: Version 1.2, May 20, 2022

The TSS also states that the SED performs all of the storage encryption and decryption internally without any external intervention (i.e., the encryption and decryption feature is built into the SED). The TOE provides an SED drive-lock password (BEV) to the SED which in turn uses it to decrypt the symmetric key it uses to encrypt and decrypt the data on the SED. The TOE generates the initial drive-lock password when the TOE is initialized and stores it in the TOE's internal non-field replaceable nonvolatile storage (SPI flash and EEPROM). This password is never changed and is not accessible by any user.

The TOE does not rely on any cryptographic services from the operational environment. The TSS in table entry "FCS_KYC_EXT.1 (Key chaining)" does state that the TOE generates the BEV by requesting a 256-bits of data from the OpenSSL FIPS Object Module 2.0.4 DRBG specified in FCS_RBG_EXT.1.

Furthermore, the SEDs typically have a small portion of space on the drive that is not encrypted. This unencrypted space which is used by the drive to store its own key chain needed to encrypt and decrypt the rest of the storage. This key chain is encrypted and decrypted using the BEV. The TOE has no control over this unencrypted space.

The evaluator notes that neither the specification of FDP_DSK_EXT.1 nor the TSS indicates the TOE supports multiple device encryptions.

Guidance Assurance Activities

Assurance Activity AA-FDP_DSK_EXT.1-AGD-20

> *The evaluator shall review the AGD guidance to determine that it describes the initial steps needed to enable the Device encryption function, including any necessary preparatory steps. The guidance shall provide instructions that are sufficient to ensure that all Devices will be encrypted when encryption is enabled or at shipment of the TOE.*

Summary

[CCECG] chapter 5 "Configure the HCD", section "System and network settings (excluding IPsec)", section "Drive-lock password" provides guidance on a self-encrypting drive (SED). It states that the HCD contains a self-encrypting drive (SED) that is locked to the HCD using a drive-lock password.

In addition, it states that as part of achieving the evaluated configuration, a new, random drive-lock password must be generated. This section provides step-by-step instructions to generate a new drive-lock password with the following note:

> "***IMPORTANT**: After achieving the evaluated configuration, the drive-lock password must not be changed.*"

The evaluator determined that the provided guidance contains the necessary instructions to configure/enable the device encryption function.

Test Assurance Activities

Assurance Activity AA-FDP_DSK_EXT.1-ATE-01

The evaluator shall perform the following tests:

> *Test 1. Write data to Storage device: Perform writing to the storage device with operating TSFI which enforce write process of User documents and Confidential TSF data.*
>
> *Test 2. Confirm that written data are encrypted: Verify there are no plaintext data present in the encrypted range written by Test 1; and, verify that the data can be decrypted by proper key and key material.*

All TSFIs for writing User Document Data and Confidential TSF data should be tested by above Test 1 and Test 2.

Summary

6.1.3.3 "Extended: Protection of Data on Disk (FDP_DSK_EXT.1)" has selected in the SFR FDP_DSK_EXT.1 the following:

> "*use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP.*"

NIAP has released the technical decision TD0176 which states that

> *The TSS, KMD, and test sections only apply to parts of the TOE which fall under the selection "perform encryption in accordance with FCS_COP.1(d)".*

which the ST has not selected.

The evaluator therefore consider this requirement as not applicable.

Key Management Assurance Activities

Assurance Activity AA-FDP_DSK_EXT.1-AKM-10

The evaluator shall verify the KMD includes a description of the data encryption engine, its components, and details about its implementation (e.g. for hardware: integrated within the device's main SOC or separate co-processor, for software: initialization of the Device, drivers, libraries (if applicable), logical interfaces for encryption/decryption, and areas which are not encrypted (e.g. boot loaders, portions that do not contain confidential data, partition tables, etc.)). The evaluator shall verify the KMD provides a functional (block) diagram showing the main components (such as memories and processors) and the data path between, for hardware, the Device's interface and the Device's persistent media storing the data, or for software, the initial steps needed to the activities the TOE performs to ensure it encrypts the storage device entirely when a user or administrator first provisions the product. The hardware encryption diagram shall show the location of the data encryption engine within the data path. The evaluator shall validate that the hardware encryption diagram contains enough detail showing the main components within the data path and that it clearly identifies the data encryption engine.

The evaluator shall verify the KMD provides sufficient instructions to ensure that when the encryption is enabled, the TOE encrypts all applicable Devices. The evaluator shall verify that the KMD describes the data flow from the interface to the Device's persistent media storing the data. The evaluator shall verify that the KMD provides information on those conditions in which the data bypasses the data encryption engine (e.g. read-write operations to an unencrypted area).

The evaluator shall verify that the KMD provides a description of the boot initialization, the encryption initialization process, and at what moment the product enables the encryption. If encryption can be enabled and disabled, the evaluator shall validate that the product does not allow for the transfer of confidential data before it fully initializes the encryption. The evaluator shall ensure the software developer provides special tools which allow inspection of the encrypted drive either in-band or out-of-band, and may allow provisioning with a known key.

Summary

The evaluator analysed the various subsections of [KMD] and confirmed that the hardware encryption diagrams contain enough detail showing the main components within the data path and that they clearly identify the data encryption engines and their location. The evaluator confirmed that the diagrams also explain all the steps on how data encryption/decryption takes place, including a description of the boot initialization, the encryption initialization process, and at what moment the product enables the encryption. Moreover, the evaluator determined that the [KMD] describes the storage location of all keys stored in nonvolatile memory and how they are protected. The evaluator therefore considered the requirements for this work unit fulfilled.

2.1.3.4 Subset residual information protection (image overwrite) (FDP_RIP.1(a))

TSS Assurance Activities

Assurance Activity AA-FDP_RIP.1-A-ASE-01

The evaluator shall examine the TSS to ensure that the description is comprehensive in describing where image data is stored and how and when it is overwritten.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FDP_RIP.1(a) (Document erase)" describes FDP_RIP.1(a). It states the following:

- User document data are stored on a field-replaceable nonvolatile storage devices, specifically a disk drive that is also an SED. This user document data is stored in the form of job files. When a job file is deleted (either automatically by the system or by request of a user), the TOE will overwrite the file. The overwriting is performed by the feature "Managing Temporary Job Files" which implement the following two (administrator-selected) options allowed in the evaluated configuration:
  - Secure Fast Erase overwrites a job file once using a static byte value of 0x48. Then the file is unlinked (deallocated) from the file system and the disk blocks comprising the file reassigned to free space in the file system.
  - Secure Sanitize Erase overwrites a job file three times. The first pass uses a static byte value of 0x48. The second pass uses a static byte value of 0xB7. The third pass uses pseudo-random values. Then the file is unlinked (deallocated) from the file and the disk blocks comprising the file reassigned to free space in the file system.

The evaluator determined that the TSS provides sufficient description of where image data is stored and how it is overwritten upon deletion.

Guidance Assurance Activities

Assurance Activity AA-FDP_RIP.1-A-AGD-01

The evaluator shall check to ensure that the operational guidance contains instructions for enabling the Image Overwrite function.

Summary

The evaluator checked [CCECG] chapter 5 "Configure the HCD" section "Managing temporary job files" which provides related guidance for FDP_RIP.1. According to the guidance, the file erase mode must be configure to erase temporary job files using either the Secure Fast Erase or Secure Sanitize Erase mode. The configuration is as follows:

1. Open the **Security** tab of the EWS.
2. Select the **Protect Stored Data** menu item.
3. In the **Managing Temporary Job Files** section, select either the **Secure Fast Erase (Overwrite 1 time)** or **Secure Sanitize Erase (Overwrite 3 times)** radio button.
4. Click **Apply**.

The evaluator verified that the guidance contains instructions for enabling the Image Overwrite function.

Test Assurance Activities

Assurance Activity AA-FDP_RIP.1-A-ATE-01

The evaluator shall include tests related to this function in the set of tests performed in FMT_SMF.1.

Summary

Please see tests for FMT_SMF.1 as stated in [HCDPPv1.0].

2.1.4 Identification and authentication (FIA)

2.1.4.1 Authentication failure handling (FIA_AFL.1)

TSS Assurance Activities

Assurance Activity AA-FIA_AFL.1-ASE-40

The evaluator shall check to ensure that the TSS contains a description of the actions in the case of authentication failure (types of authentication events, the number of unsuccessful authentication attempts, actions to be conducted), which is consistent with the definition of the SFR.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FIA_AFL.1 (Authentication failure handling)" describes FIA_AFL.1. The description addresses the Local Device Sign In mechanism (used by the Control Panel, EWS, and REST interfaces) which uses the Device Administrator account. The lockout mechanism uses three control values: account lockout maximum attempts, account lockout interval, account reset lockout counter interval.

The account lockout maximum attempts which is between 3 and 10 can be configured by the administrator. When the maximum attempts are reached, the account is locked for the amount of time specified by the account lockout internal value which is between 60 seconds (1 minute) and 1800 seconds (30 minutes). The account reset lockout counter interval value allows an administrator

to specify the time (in seconds) in which the failed login attempts must occur before the account lockout maximum attempts counter is reset to zero. This value must be equal to or greater than the account lockout interval value.

The evaluator verified the TSS description with the definition of FIA_AFL.1 ([ST] section 6.1.4.1 "Authentication failure handling (FIA_AFL.1)" and found them to be consistent. FIA_AFL.1 specifically lists the authentication mechanisms and the applicable interfaces and specifies the configurable unsuccessful authentication attempts to be between 3 to 10.

Guidance Assurance Activities

Assurance Activity AA-FIA_AFL.1-AGD-01

The evaluator shall check to ensure that the administrator guidance describes the setting for actions to be taken in the case of authentication failure, if any are defined in the SFR.

Summary

[ST] section "Authentication failure handling (FIA_AFL.1)" defines FIA_AFL.1 in which FIA_AFL.1.2 states that when the defined number of unsuccessful authentication attempts has been met, the TSF shall lock the account.

[CCECG], chapter 5 "Configure the HCD", section "System and network settings", subsection "Account policy" provides guidance for configuring account policy settings including setting the maximum login attempts and account lockout. The instructions include steps for enabling account lockout for the local administrator account, entering a value in the range of 3-10 in the maximum attempts field, as specified in the SFR FIA_AFL.1 from [ST].

Test Assurance Activities

Assurance Activity AA-FIA_AFL.1-ATE-01

The evaluator shall also perform the following tests:

1. *The evaluator shall check to ensure that the subsequent authentication attempts do not succeed by the behavior according to the actions defined in the SFR when unsuccessful authentication attempts reach the status defined in the SFR.*
2. *The evaluator shall check to ensure that authentication attempts succeed when conditions to re-enable authentication attempts are defined in the SFR and when the conditions are fulfilled.*
3. *The evaluator shall perform the tests 1 and 2 described above for all the targeted authentication methods when there are multiple Internal Authentication methods (e.g., password authentication, biometric authentication).*
4. *The evaluator shall perform the tests 1 and 2 described above for all interfaces when there are multiple interfaces (e.g., operation panel, Web interfaces) that implement authentication attempts.*

Summary

Table 6: Tests mapped to interfaces

Test Number	Interface	Test description
Test 1	Control Panel	The lockout-policy was configured to three attempts. The evaluator then entered wrong password three times on the Control Panel and the account became locked. Then checked logs that showed that account was locked. Then tried to log in with correct password using Control Panel and EWS, and failed as expected.

Test Number	Interface	Test description
	EWS	The lockout-policy was configured to three attempts. The evaluator then entered wrong password three times using EWS interface (web GUI) and the account became locked. He then checked the logs and saw that the account had been locked. Afterwards, the evaluator tried to authenticate with the correct password and failed since the account was locked, as expected.
	REST	The lockout-policy was configured to three attempts. The evaluator then sent commands to the REST interface using different (wrong) passwords three times. He then observed that the syslog recorded that user account had been locked. Afterwards, the evaluator tried to authenticate with the correct password and failed since the account was locked, as expected.
Test 2	Control Panel	The evaluator configured the account lockout timer to 60 seconds, then entered wrong password three times on the Control Panel which locked the account. He then waited 60 seconds and entered the correct password and successfully logged into the system.
	EWS	The evaluator configured the account lockout timer to 60 seconds, then entered wrong password three times using EWS interface (web GUI) which locked the account. He then waited 60 seconds and entered the correct password and successfully logged into the system.
	REST	The evaluator configured the account lockout timer to 60 seconds, then sent three commands to the REST interface, each using a different (wrong) password. He then observed that the syslog recorded that user account had been locked. After 60 seconds, the evaluator sent a new command using the correct password and the command was successfully executed.
Test 3	Not applicable since no extra authentication has been selected in [ST].	
Test 4	Please see Test 1 and Test 2.	

2.1.4.2 User attribute definition (FIA_ATD.1)

TSS Assurance Activities

Assurance Activity AA-FIA_ATD.1-ASE-01

The evaluator shall check to ensure that the TSS contains a description of the user security attributes that the TOE uses to implement the SFR, which is consistent with the definition of the SFR.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FIA_ATD.1 (User attribute definition)" describes FIA_ATD.1. The description covers Control Panel users, EWS users, and REST users, all of which are specified in the definition of FTA_ATD.1 ([ST] section 6.1.4.2). To verify the consistency the evaluator constructed the following table listing the user types and security attributes specified in FIA_ATD.1 and the corresponding description in the TSS.

Table 7: User Security Attribute and TSS Description

User	Authentication Mechanism	Security Attribute	TSS Description	Consistent?
Control Panel users	Internal Authentication (Local Device Sign In)	Identifier: Display name Authenticator: Password PS: Device Administrator PS	*For Internal Authentication (i.e., the Local Device Sign In method), only one account exists in the evaluated configuration: Device Administrator. This account is a built-in account and is permanently assigned the Device Administrator PS which makes its role U.ADMIN. The user identifier is the Display name and the authenticator is a password.*	Yes. The TSS description mentions all the user security attributes specified in the SFR.
	External Authentication (LDAP Sign In and Windows Sign In)	PS: Network user PS	*For each External Authentication method (i.e., LDAP Sign In and Windows Sign In), the user identifiers and passwords are stored on and verified by the External Authentication server. Also, the network group memberships are stored on the External Authentication server. Because these security attributes are not stored on and maintained by the TOE, they are not listed in FIA_ATD.1. User accounts from External Authentication methods are known as network user accounts. Each network user account can have zero or one PS (i.e., network user PS) associated with it that is used in calculating the user's session PS (i.e., the user's role). These PSs are stored on and maintained by the TOE.*	Yes. The TSS description mentions the user security attribute (i.e., network user PS)
ESW user	Internal Authentication (Local Device Sign In)	Identifier: Display name Authenticator: Password Role: (implied U.ADMIN)	*For Internal Authentication (i.e., the Local Device Sign In method), only one account exists in the evaluated configuration: Device Administrator. This account is a built-in account and is permanently assigned the Device Administrator PS which makes its role U.ADMIN. It contains a user identifier known*	Yes. The TSS description mentions all the user security attributes specified in the SFR.

User	Authentication Mechanism	Security Attribute	TSS Description	Consistent?
			as the Display name and a password known as the Device Administrator Password.	
	External Authentication (LDAP Sign In and Windows Sign In)	Role: (implied U.ADMIN)	*The EWS authentication works very similarly to the Control Panel authentication* which implies it has the same security attributes.	Yes. The TSS description mentions all the user security attributes specified in the SFR.
REST users	Internal Authentication (Local Device Sign In)	Identifier: Display name Authenticator: Password Role: (implied U.ADMIN)	*For Internal Authentication, the REST interface supports the Local Device Sign In method which requires the administrator to authenticate using the Device Administrator account. The Display name is used as the identifier and password is used as the authenticator.*	Yes. The TSS description mentions all the user security attributes specified in the SFR.
	External Authentication (Windows Sign In)	Role: (implied U.ADMIN)	*For External Authentication, the REST interface supports the Windows Sign In method which requires the user to be associated with the Device Administrator permission set.*	Yes. The TSS description mentions all the user security attributes specified in the SFR.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

No assurance activities defined.

2.1.4.3 Extended: Password management (FIA_PMG_EXT.1)

TSS Assurance Activities

No assurance activities defined.

Guidance Assurance Activities

Assurance Activity AA-FIA_PMG_EXT.1-AGD-01

> *The evaluator shall examine the operational guidance to determine that it provides guidance to security administrators on the composition of passwords, and that it provides instructions on setting the minimum password length.*

Summary

The evaluator examined the following subsections of [CCECG] chapter 5, section Section "System and network settings (excluding IPsec)" for related guidance for FIA_PMG_EXT.1:

Subsection "Account policy"

It provides instructions to set the password complexity for the local administrator password via the EWS interface as follows:

- Open the **Security** tab of the EWS.
- Select the **Account Policy** menu item.
- In the **Local Administrator Password** area, check the **Enable password complexity** check box.
- Click **Apply**.

It provides instructions to set the minimum password length for the local administrator password via the EWS interface as follows:

- Open the **Security** tab of the EWS.
- Select the **Account Policy** menu item.
- In the **Local Administrator Password** area, enter a value in the range of 8-16 in the the **Minimum password length**.
- Click **Apply**.

Subsection "Local administrator password"

It provides instructions for password composition including password strength via the EWS interface as follows:

- Open the **Security** tab of the EWS.
- Select the **General Security** menu item.
- Under the **Set the Local Administrator Password** are, in the **New Password** field, enter a password that is at least eight characters long and contains characters from three of the four following categories: uppercase letters, lowercase letters, numbers, and special characters ("!", "@", "#", "$", "%", "^", "&", "*", "(", ")", """, "'", "+", ",", "-", ".", ":", ";", "<", "=", ">", "?", "[", "/", "\", "]", "_", "`", "|", "~", "{", "}").
- In the **Verify Password** field, re-enter the password.
- Click **Apply**.

Test Assurance Activities

Assurance Activity AA-FIA_PMG_EXT.1-ATE-01

The evaluator shall also perform the following test:

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 compositions 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.

Summary

The evaluator performed several tests, both negative and positive tests, including password lengths, password complexity, and all special characters defined in [ST]. The tests covered "Device Administrator Password".

2.1.4.4 Extended: Pre-shared key composition (FIA_PSK_EXT.1)

TSS Assurance Activities

Assurance Activity AA-FIA_PSK_EXT.1-ASE-01

The evaluator shall examine the TSS to ensure that it states that text-based pre-shared keys of 22 characters are supported, and that the TSS states the conditioning that takes place to transform the text-based pre-shared key from the key sequence entered by the user (e.g., ASCII representation) to the bit string used by IPsec, and that this conditioning is consistent with the first selection in the FIA_PSK_EXT.1.3 requirement. If the assignment is used to specify conditioning, the evaluator will confirm that the TSS describes this conditioning.

If "bit-based pre-shared keys" is selected, the evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both). The evaluator shall also examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.

Summary

[ST] section 6.1.4.4 "Pre-shared key composition (FIA_PSK_EXT.1)" defines FIA_PSK_EXT.1 which states the following:

- The TOE is capable of accepting text-based pre-shared keys between 22 to 128 characters.
- The TOE conditions text-based pre-shared keys using SHA-1, SHA2-256, or SHA2-512.
- The TOE is capable of accepting bit-based pre-shared keys.

The evaluator checked Table 40 of the TSS in which table entry "FIA_PSK_EXT.1 (Pre-shared key composition) describes FIA_PSK_EXT.1. It states that the TOE supports text-based pre-shared keys and accepts bit-based pre-shared keys for IPsec. Text-based keys can be between 22 to 128 characters in length, and are conditioned using SHA-1, SHA2-256, or SHA2-512 which is consistent with the definition of FIA_PSK_EXT.1.3 outlined above.

The evaluator noted that the assignment was not used in FIA_PSK_EXT.1.3 to specify conditioning, thus the TSS is not required to describe such conditioning. The evaluator also noted that according to the definition of FIA_PSK_EXT.1.3, the TOE is capable of accepting bit-based pre-shared keys. In regard to this, the TSS states that the TOE does accept bit-based pre-shared keys generated outside of the TOE. The TOE does not generate bit-based pre-shared keys by itself. It allows administrator to enter a hexadecimal bit-based pre-shared key. The evaluator also examined the operational guidance [CCECG] and confirmed that section "Configure IPsec/Firewall templates" contains instructions for entering bit-based pre-shared keys.

Based on the findings above, the evaluator determined that the TSS description is consistent with the definition of FIA_PSK_EXT.1 in [ST] section 6.1.4.4.

Guidance Assurance Activities

Assurance Activity AA-FIA_PSK_EXT.1-AGD-01

The evaluator shall examine the operational guidance to determine that it provides guidance on the composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the merits of shorter or longer pre-shared keys. The guidance must specify the allowable characters for pre-shared keys, and that list must be a super-set of the list contained in FIA_PSK_EXT.1.2.

Summary

[CCECG] chapter 5 "Configure the HCD" section "IPsec" provides guidance for pre-shared keys. Pre-shared keys can be configured via the EWS interface. Step-by-step instructions are provided in subsection "Create an IKEv1 IPsec/Firewall template" (step 15) which states the following:

The HCD supports text-based pre-shared keys and accepts bit-based pre-shared keys.

The text-based keys can be from 22 characters to 128 characters in length and be composed of any combination of upper and lower case letters, numbers, and special characters that include the characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". The text-based keys are conditioned using SHA-1, SHA2-256, or SHA2-512 hash algorithms.

The HCD accepts bit-based pre-shared keys generated outside of the HCD. It allows the user to enter a hexadecimal bit-based pre-shared key.

a. If a text-based pre-shared key is to be used, perform the following:
   i. Select the **Pre-Shared Key** radio button.
   ii. Check the **Hash** check box.
   iii. If another hash algorithm other than **SHA1** is to be used to condition the test-based key, select either the **SHA-256** or **SHA-512** radio button.
   iv. In the field, enter a text-based key that is at least 22 characters long.

b. If a bit-based pre-shared key is to be used, perform the following:
   i. Select the **Pre-Shared Key** radio button.
   ii. Select the **Hex** radio button.
   iii. In the field, enter a bit-based key in hexadecimal form that is at least 22 characters long.

Test Assurance Activities

Assurance Activity AA-FIA_PSK_EXT.1-ATE-01

The evaluator shall also perform the following tests:

1. *The evaluator shall compose at least 15 pre-shared keys of 22 characters that cover all allowed characters in various combinations that conform to the operational guidance, and demonstrates that a successful protocol negotiation can be performed with each key.*
2. *[conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall repeat Test 1 using the minimum length; the maximum length; and an invalid length. The minimum and maximum length tests should be successful, and the invalid length must be rejected by the TOE.*
3. *[conditional]: If the TOE supports bit-based pre-shared keys but does not generate such keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.*
4. *[conditional]: If the TOE supports bit-based pre-shared keys and does generate such keys, the evaluator shall generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.*

Summary

Test 1

The evaluator composed 15 different pre-shared keys with 22 characters, using upper and lower case letters, numbers, and all special characters listed in [ST] for this SFR.

Test 2

The evaluator composed several different pre-shared keys, using minimum length, maximum length, and invalid length. The valid pre-shared keys was successfully created and the pre-shared keys with invalid length was rejected by TOE.

Test 3

The TOE supports bit-based pre-shared keys but does not generate such keys. Therefore, the evaluator generated a bit-based key outside of the TOE and entered it according to the instructions in operational guidance. He then successfully initiated an IPsec connection with another device using the entered PSK.

Test 4

Generation of bit-based pre-shared keys is not selected in [ST]. Therefore, this test is not applicable.

2.1.4.5 Timing of authentication (FIA_UAU.1)

TSS Assurance Activities

Assurance Activity AA-FIA_UAU.1-ASE-01

The evaluator shall check to ensure that the TSS describes all the identification and authentication mechanisms that the TOE provides (e.g., Internal Authentication and authentication by external servers).

The evaluator shall check to ensure that the TSS identifies all the interfaces to perform identification and authentication (e.g., identification and authentication from operation panel or via Web interfaces).

The evaluator shall check to ensure that the TSS describes the protocols (e.g., LDAP, Kerberos, OCSP) used in performing identification and authentication when the TOE exchanges identification and authentication with External Authentication servers.

The evaluator shall check to ensure that the TSS contains a description of the permitted actions before performing identification and authentication, which is consistent with the definition of the SFR.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FIA_UAU.1 (Timing of authentication)" describes FIA_UAU.1. The TSS description covers the following interfaces that perform identification and authentication (I&A):

- Control Panel
- Network interfaces
  - EWS
  - REST

Control Panel

The Control Panel supports both Internal Authentication and External Authentication methods. Users select the authentication mechanism (i.e., the sign in method) from a menu of sign in methods. Internal Authentication is provided through the Local Device Sign In method and External Authentication through either the LDAP Sign In or Windows Sign In (via Kerberos) method.

The Local Device Sign In method requires a username and password. The TOE in its evaluated configuration comes with only one account which is the built-in Device Administrator account.

The LDAP Sign In method uses an external LDAP server (e.g., Microsoft Active Directory server) for I&A. The TOE uses LDAP version 3 protocol over IPsec to communicate with the LDAP server. A valid LDAP account is required for this method. The Windows Sign In method uses an external Windows domain server for I&A. The TOE uses Kerberos version 5 protocol over IPsec to communicate with the Windows domain server. A valid Windows domain account is required for this method.

Prior to successful authentication, the user is allowed to perform the following actions via the Control Panel:

- View the Welcome message
- Reset the session
- Select the Sign In button
- Select a sign-in method from Sign In screen
- View the device status information
- Change the display language for the session
- Place the device into sleep mode
- View the network connectivity status information
- View help information
- View the system time

Network interfaces

Most of the client network interfaces protected by IPsec perform authentication. Table 50 "IPsec client interfaces" of the TSS provides a list of the available IPsec client interfaces to the TOE, whether or not there is an authentication mechanism associated with the client interface, and a list of TSF-mediated actions prior to authentication, if any.

EWS over IPsec

This interface which is connected over IPsec is used by the Administrative Computer (via a web browser) for managing the TOE. This interface requires the administrator to sign in using the same sign in method menu options as provided by the Control Panel.

According to Table 50 "IPsec client interfaces" of the TSS, prior to successful authentication, the administrator is only allowed to select a sign in method.

REST over IPsec

This is an administrative interface used to manage the TOE over IPsec. This interface supports the Local Device Sign In method which requires the administrator to authenticate using the Device Administrator account. It also supports the Windows Sign In method which requires the user to be associated with the Device Administrator permission set.

According to Table 50 "IPsec client interfaces" of the TSS, this interface allows the following actions prior to successful authentication:

- Discover a subset of the Web Services
- Obtain the X.509v3 certificate on the print engine
- Obtain the secure configuration settings on the print engine
- Obtain list of installed licenses
- Install a digitally signed license
- Delete a license (if the license in the payload of the request is digitally signed)
- Obtain Web Services registration status

The evaluator verified that ALL the permitted actions before successful identification and authentication described in the TSS are consistent with the definition of FIA_UAU.1 in [ST] section 6.1.4.5 and the definition of FIA_UID.1 in section 6.1.4.7.

Guidance Assurance Activities

Assurance Activity AA-FIA_UAU.1-AGD-01

The evaluator shall check to ensure that the administrator guidance contains descriptions of identification and authentication methods that the TOE provides (e.g., External Authentication, Internal Authentication) as well as interfaces (e.g., identification and authentication from operation panel or via Web interfaces), which are consistent with the ST (TSS).

Summary

The TSS of [ST] provides Table 40 "TOE SFR compliance rationale" in which table entry "FIA_UAU.1 (Timing of authentication)" describes the authentication methods as follows:

- Control Panel which supports both Internal Authentication (via Local Device Sign In) and External Authentication (via LDAP Sign In and Windows Sign In)
- Network interfaces which includes the EWS and REST, and all of which are over IPsec.

[CCECG] chapter 5 "Configure the HCD" section "Access Control" identifies the following authentication (sign-in) methods supported in the evaluated configuration:

- Local Device - This sign-in method uses an authentication database stored on the HCD's storage drive to authenticate users. In the evaluated configuration, only the local administrator account is supported.
- LDAP - This sign-in method depends on an LDAP server on the network to authenticate users.
- Windows - This sign-in method depends on a Windows Active Directory domain on the network to authenticate users.

This section also states the following:

- The Local Device sign-in method is always available and does not require any configuration.
- The LDAP sign-in method and Windows sign-in method must be configured and enabled before they can be used.
- In the evaluated configuration, at least one of the sign-in methods that depends on an authentication server (e.g., LDAP server) must be configured and enabled.

The evaluator examined step-by-step instructions on how to configure via the EWS interface the LDAP Sign In and Windows (Kerberos) Sign In, for user authentication. The instructions are determined to be sufficiently detailed and easy to follow.

For IPsec configuration, the evaluator examined section "IPsec" which provides a great level of details for configuring IPsec.

The evaluator's findings are supported by the assessments performed in other evaluation activities where the evaluator examined these sections for the subject matter. Thus, the evaluator concluded that the provided guidance contains sufficient information with regard to user authentication. In addition, the evaluator found the guidance description to be consistent with the TSS description of FIA_UAU.1.

Test Assurance Activities

Assurance Activity AA-FIA_UAU.1-ATE-01

The evaluator shall also perform the following tests:

1. *The evaluator shall check to ensure that identification and authentication succeeds, enabling the access to the TOE when using authorized data.*
2. *The evaluator shall check to ensure that identification and authentication fails, disabling the access to the TOE afterwards when using unauthorized data.*

The evaluator shall perform the tests described above for each of the authentication methods that the TOE provides (e.g., External Authentication, Internal Authentication) as well as interfaces (e.g., identification and authentication from operation panel or via Web interfaces).

Summary

Interface: Control Panel

- I&A mechanism: Local Device Authentication
  The evaluator successfully signed into the TOE using correct user name and password when using Local Device Authentication. He then logged out and tried to log in with the same account, but with wrong password, and failed, as expected. He then tried to sign into the TOE using incorrect user name, but correct password, and failed, as expected.
- I&A mechanism: LDAP
  The evaluator successfully logged in to the TOE using correct user name and password when using LDAP. He then logged out and tried to log in with the same account, but with wrong password, and failed, as expected. He then tried to sign into the TOE using incorrect user name, but correct password, and failed, as expected.
- I&A mechanism: Kerberos
  The evaluator successfully logged in to the TOE using correct user name and password when using Kerberos. He then logged out and tried to log in with same account, but with wrong password, and failed, as expected. He then tried to sign into the TOE using incorrect user name, but correct password, and failed, as expected.

Interface: EWS

- I&A mechanism: Local Device Authentication
  The evaluator successfully logged in to the TOE using correct user name and password when using Local Device Authentication. He then logged out and tried to log in with the same account, but with wrong password, and failed, as expected. He then tried to sign into the TOE using incorrect user name, but correct password, and failed, as expected.
- I&A mechanism: LDAP
  The evaluator successfully logged in to the TOE using correct user name and password when using LDAP. He then logged out and tried to log in with the same account, but with wrong password, and failed, as expected. He then tried to sign into the TOE using incorrect user name, but correct password, and failed, as expected.
- I&A mechanism: Kerberos
  The evaluator successfully logged in to the TOE using correct user name and password when using Kerberos. He then logged out and tried to log in with same account, but with wrong password, and failed, as expected. He then tried to sign into the TOE using incorrect user name, but correct password, and failed, as expected.

Interface: REST

- I&A mechanism: Local Device Authentication
  The evaluator sent a command to the REST interface on the TOE using correct credentials and command was executed on the TOE. He then sent a command using the correct user name and wrong password and the command was not executed, as expected. He then sent a command using wrong user name and correct password and the command was not executed, as expected.
- I&A mechanism: Kerberos

The evaluator sent a command to the REST interface on the TOE using correct Kerberos credentials and command was executed on the TOE. He then sent a command using the correct user name and wrong password and the command was not executed, as expected. He then sent a command using wrong user name and correct password and the command was not executed, as expected.

2.1.4.6 Protected authentication feedback (FIA_UAU.7)

TSS Assurance Activities

Assurance Activity AA-FIA_UAU.7-ASE-01

The evaluator shall check to ensure that the TSS contains a description of the authentication information feedback provided to users while the authentication is in progress, which is consistent with the definition of the SFR.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FIA_UAU.7 (Protected authentication feedback)" describes FIA_UAU.7. It states that the Control Panel (for Internal and External Authentication methods) and EWS (for Internal and External Authentication methods) display a dot for each password character typed by the user. This description is found to be consistent with the definition of FIA_UAU.7 ([ST] section 6.1.4.6) which states that the TSF shall provide only dots to the user while the authentication is in progress.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

Assurance Activity AA-FIA_UAU.7-ATE-01

The evaluator shall also perform the following tests:

1. *The evaluator shall check to ensure that only the information defined in the SFR is provided for feedback by attempting identification and authentication.*
2. *The evaluator shall perform the test 1 described above for all the interfaces that the TOE provides (e.g., operation panel, identification and authentication via Web interface).*

Summary

Interface: Control Panel

The evaluator selected Local Device Authentication and entered the password for the admin account. Each character was masked after being selected and/or entered. He then repeated the test using LDAP sign in and Kerberos (Windows) sign in.

Interface: EWS

The evaluator selected Local Device Authentication and entered the password for the admin account. Each character was masked after being entered. He then repeated the test using LDAP sign in and Kerberos (Windows) sign in.

2.1.4.7 Timing of identification (FIA_UID.1)

TSS Assurance Activities

Assurance Activity AA-FIA_UID.1-ASE-01

It is covered by assurance activities for FIA_UAU.1.

Summary

This assurance activity was performed in conjunction with FIA_UAU.1.

Guidance Assurance Activities

Assurance Activity AA-FIA_UID.1-AGD-01

It is covered by assurance activities for FIA_UAU.1.

Summary

This assurance activity is performed in conjunction with AA-FIA_UAU.1-AGD-01.

Test Assurance Activities

Assurance Activity AA-FIA_UID.1-ATE-01

It is covered by assurance activities for FIA_UAU.1.

Summary

Interface: Control Panel

- I&A mechanism: Local Device Authentication
  The evaluator successfully signed into the TOE using correct user name and password when using Local Device Authentication. He then logged out and tried to log in with the same account, but with wrong password, and failed, as expected. He then tried to sign into the TOE using incorrect user name, but correct password, and failed, as expected.
- I&A mechanism: LDAP
  The evaluator successfully logged in to the TOE using correct user name and password when using LDAP. He then logged out and tried to log in with the same account, but with wrong password, and failed, as expected. He then tried to sign into the TOE using incorrect user name, but correct password, and failed, as expected.
- I&A mechanism: Kerberos
  The evaluator successfully logged in to the TOE using correct user name and password when using Kerberos. He then logged out and tried to log in with same account, but with wrong password, and failed, as expected. He then tried to sign into the TOE using incorrect user name, but correct password, and failed, as expected.

Interface: EWS

- I&A mechanism: Local Device Authentication
  The evaluator successfully logged in to the TOE using correct user name and password when using Local Device Authentication. He then logged out and tried to log in with the same account, but with wrong password, and failed, as expected. He then tried sign into the TOE using incorrect user name, but correct password, and failed, as expected.

- I&A mechanism: LDAP
  The evaluator successfully logged in to the TOE using correct user name and password when using LDAP. He then logged out and tried to log in with the same account, but with wrong password, and failed, as expected. He then tried to sign into the TOE using incorrect user name, but correct password, and failed, as expected.
- I&A mechanism: Kerberos
  The evaluator successfully logged in to the TOE using correct user name and password when using Kerberos. He then logged out and tried to log in with same account, but with wrong password, and failed, as expected. He then tried to sign into the TOE using incorrect user name, but correct password, and failed, as expected.

Interface: REST

- I&A mechanism: Local Device Authentication
  The evaluator sent a command to the REST interface on the TOE using correct credentials and command was executed on the TOE. He then sent a command using the correct user name and wrong password and the command was not executed, as expected. He then sent a command using wrong user name and correct password and the command was not executed, as expected.
- I&A mechanism: Kerberos
  The evaluator sent a command to the REST interface on the TOE using correct Kerberos credentials and command was executed on the TOE. He then sent a command using the correct user name and wrong password and the command was not executed, as expected. He then sent a command using wrong user name and correct password and the command was not executed, as expected.

2.1.4.8 User-subject binding (FIA_USB.1)

TSS Assurance Activities

Assurance Activity AA-FIA_USB.1-ASE-01

The evaluator shall check to ensure that the TSS contains a description of rules for associating security attributes with the users who succeed identification and authentication, which is consistent with the definition of the SFR.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FIA_USB.1 (User-subject binding)" describes FIA_USB.1. The TSS description explains how the TOE associate security attributes as follows:

Control Panel users:

Upon successful sign in, a username and role are bound to the subject on behalf of that user. If the user signs in via the Local Device Sign In method then the bound username would be the Display name. If the user signs in via the LDAP/Windows Sign In method then the bound username will be the user's LDAP/Windows username.

The Control Panel user's role is determined by the user's session permission set (PS). There is one PS per user for the Internal Authentication method while the External Authentication methods have one PS per authentication method, zero or more PS per user, and zero or one PS per network group to which the user belongs. The Device Administrator account (for Local Device Sign In) always has the role U.ADMIN, while for the External Authentication methods the role can be either U.ADMIN or U.NORMAL, which is determined by combinations of PSs as described in great detail in the TSS description.

Remote users

Upon successful authentication, the client's IP address is the client's user identifier. For EWS users, the identity binding is the same as for Control Panel users. As to REST users, the user identity is the Display name when authenticating via the Local Sign In method and the Windows username when authenticating via the Windows Sign In method.

The user role is determined by the login account for EWS and REST.

The evaluator checked the TSS description against the definition of FIA_USB.1 ([ST] section 6.1.4.8) and determined they are consistent.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

Assurance Activity AA-FIA_USB.1-ATE-01

The evaluator shall also perform the following test:

The evaluator shall check to ensure that security attributes defined in the SFR are associated with the users who succeed identification and authentication (it is ensured in the tests of FDP_ACF) for each role that the TOE supports (e.g., User and Administrator).

Summary

1. User identifier

Control Panel users

- Local Device Sign In method: Display name
  Evaluator verified Display name (local username) was associated with the user.
- LDAP Sign In method: LDAP username
  Evaluator verified LDAP username was associated with the user.
- Windows Sign In method: Windows username
  Evaluator verified Windows username was associated with the user.

EWS users

- Local Device Sign In method: Display name
  Evaluator verified Display name (local username) was associated with the user.
- LDAP Sign In method: LDAP username
  Evaluator verified LDAP username was associated with the user.
- Windows Sign In method: Windows username
  Evaluator verified Windows username was associated with the user.

REST users

- Local Device Sign In method: Display name
  Evaluator verified Display name (local username) was associated with the user.
- Windows Sign In method: Windows username
  Evaluator verified Windows username was associated with the user.

2.1.5 Security management (FMT)

2.1.5.1 Management of security functions behavior (FMT_MOF.1)

TSS Assurance Activities

Assurance Activity AA-FMT_MOF.1-ASE-01

The evaluator shall check to ensure that the TSS contains a description of the management functions that the TOE provides as well as user roles that are permitted to manage the functions, which is consistent with the definition of the SFR.

The evaluator shall check to ensure that the TSS identifies interfaces to operate the management functions.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FMT_MOF.1 (Management of functions)" describes FMT_MOF.1. The TSS description covers the following management functions:

Allow users to choose alternate sign-in methods at the product control panel
This function which is restricted to U.ADMIN can be enabled or disabled by the administrator via the EWS interface. When this function is disabled, the user is required to sign in using the sign-in method associated with the selected application in order to access that application.

Control Panel Mandatory Sign-in
This function is restricted to U.ADMIN and can be enabled or disabled by the administrator via the EWS interface.

Windows Sign In
This function is restricted to U.ADMIN and is used to enable and disable the Windows Sign In method via the EWS interface.

LDAP Sign In
This function is restricted to U.ADMIN and is used to enable and disable the LDAP Sign In method via the EWS interface.

Account Lockout
This function is restricted to U.ADMIN and is used to enable/disable Device Administrator account lockout via the EWS interface.

Enhanced security event logging
This function is restricted to U.ADMIN and is used to enable and disable the generation of additional security events via the EWS interface.

Managing Temporary Job Files
This function is restricted to U.ADMIN and is used to manage the image overwrite function via the EWS interface.

IPsec
This function is restricted to U.ADMIN and is used to enable and disable IPsec via the EWS interface.

Automatically synchronize with a Network Time Service:
This function is restricted to U.ADMIN and is used to enable and disable the automatic synchronization of NTS via the EWS interface.

The evaluator verified the above listing and found it to be consistent with the definition of FMT_MOF.1 (Table 30 "Management of functions" in [ST] section 6.1.5.1). Each management function listed in Table 30 is sufficiently covered in the TSS.

Guidance Assurance Activities

Assurance Activity AA-FMT_MOF.1-AGD-01

The evaluator shall check to ensure that the administrator guidance describes the operation methods for users of the given roles defined in the SFR to operate the management functions.

Summary

The definition of FMT_MOF.1 provided in section 6.1.5.1 "Management of security functions behaviour (FMT_MOF.1)" of [ST] specifies the actions/functions restricted to the U.ADMIN role (i.e., administrators). This section provides Table 30 "Management of functions" outlining the actions limited to administrators.

[CCECG] chapter 6 "Operational guidance", section "Manage the HCD security" provides guidance for security management. This section provides Table 6-6 "Operational guidance index for management functions claimed in FMT_SMF.1" mapping each management functions with corresponding guidance provided within [CCECG].

Using the information outlined above from [ST] and [CCECG], the evaluator constructed the table below mapping the actions from Table 30 of [ST] to corresponding provided guidance in [CCECG].

Table 8: Management Functions and Guidance

Function	Actions	Provided Guidance	Evaluator's Comment
Allow users to choose alternate sign-in methods at the product control panel	Enable, disable	[CCECG] chapter 5 "Configure the HCD" section "Access control".	The evaluator determined that per the guidance description, the enabling/disabling of this method can be done by check/uncheck the **Allow users to choose alternate sign-in methods at the product control panel** checkbox on the EWS interface.
Control Panel Mandatory Sign-in	Enable, disable	[CCECG] chapter 5 "Configure the HCD" section "Access control"	The evaluator determined that per the guidance description, the enabling/disabling of **Control Panel Mandatory Sign-in** can be configured via the EWS interface as described subsection "Configure permission sets" of section "Access control" which states: "***NOTE:*** *Control Panel Mandatory Sign-in is enabled when all permissions in the Device Guest permission are configured to deny access.*"
Windows Sign In	Enable, disable	[CCECG] chapter 5 "Configure the HCD" section "Access control"	The evaluator determined that per the guidance description, the enabling/disabling of **Windows Sign In** can be configured via the EWS interface as described in subsection "Configure and enable Windows sign-in method" of section "Access control".

Function	Actions	Provided Guidance	Evaluator's Comment
LDAP Sign In	Enable, disable	[CCECG] chapter 5 "Configure the HCD" section "Access control"	The evaluator determined that per the guidance description, the enabling/disabling of **LDAP Sign In** can be configured via the EWS interface as described in subsection "Configure and enable LDAP sign-in method" of section "Access control".
Account lockout	Enable, disable	[CCECG] chapter 5 "Configure the HCD" section "Account policy"	The evaluator determined that per the guidance description, the enabling/disabling of **Account lockout** can be configured via EWS interface (for local administrator account) as described in subsection "Local administrator account" of section "Account policy".
Enhanced security event logging	Enable, disable	[CCECG] chapter 5 "Configure the HCD" section "Enhanced security event logging"	The evaluator determined that per the guidance description, the enabling/disabling of **Enhanced security event logging** can be configured via EWS interface as described in section "Enhanced security event logging" (i.e., by checking/unchecking the checkbox available on the EWS interface).
Managing Temporary Job Files (i.e., image overwrite)	Determine the behavior of, modify the behavior of	[CCECG] chapter 5 "Configure the HCD" section "Managing temporary job files"	The evaluator determined that per the guidance description, the image overwrite can be managed via the EWS interface as described in section "**Managing temporary job files**", i.e., by selecting either Secure Fast Erase (Overwrite 1 time) or Secure Sanitize Erase (Overwrite 3 times) radio button available from the EWS interface.
IPsec	Enable, disable	[CCECG] chapter 5 "Configure the HCD" section "IPsec"	The evaluator determined that per the guidance description, the enabling/disabling of IPsec can be configured via EWS interface as described in subsection "Configure IPsec on the HCD" of section "IPsec" which involves selecting the **IPsec/Firewall** from the EWS menu, then configuring address templates, service templates, IPsec/Firewall templates, and IPsec/Firewall rules. This section provides detailed instructions on how to create these requirements.
Automatically synchronize with a Network Time Service	Enable, disable	[CCECG] chapter 5 "Configure the HCD" section "Date and time"	The evaluator determined that per the guidance description, the enabling/disabling of this method can be configured via EWS interface as described in subsection "Date and time"

Function	Actions	Provided Guidance	Evaluator's Comment
			of section "System and network settings (excluding IPsec)" which involves selecting the **Date/Time Settings** then from the EWS menu, then checking/unchecking the **Automatically synchronize with a Network Time Server** checkbox in the **Network Time Server** available on the EWS interface.

In preparing the table above, the evaluator determined that appropriate guidance was provided for the management functions defined in FMT_MOF.1.

Test Assurance Activities

Assurance Activity AA-FMT_MOF.1-ATE-01

The evaluator shall also perform the following tests:

1. *The evaluator shall check to ensure that users of the given roles defined in the SFR can operate the management functions in accordance with the operation methods specified in the administrator guidance.*
2. *The evaluator shall check to ensure that the operation results are appropriately reflected.*
3. *The evaluator shall check to ensure that U.NORMAL is not permitted to operate the management functions.*

Summary

The evaluator performed several tests where he checked that U.ADMIN as defined in [ST] could perform the management functions listed in [ST] for the SFR FMT_MOF.1.1 and that the operation results were appropriately reflected. Please see the list below for more detailed information.

- **Function: Allow users to choose alternate sign-in methods at the product control panel**
  The evaluator signed in as administrator and configured to allow alternative sign-in methods and verified that users could choose alternative sign-in methods in the control panel. He then disabled the option and verified that users could not choose alternative sign-in methods.
- **Function: Control Panel Mandatory Sign-in**
  Not applicable since the "Control Panel Mandatory Sign-in" must be enabled, which is done during the initial configuration of the TOE.
- **Function: Windows Sign In**
  The evaluator successfully disabled and enabled Windows Sign In when logged in as administrator.
- **Function: LDAP Sign In**
  The evaluator successfully disabled and enabled LDAP Sign In when logged in as administrator.
- **Function: Account lockout**
  The evaluator enabled and disabled account lockout for Device Administrator account, which is specified in the SFR (table 32) in the [ST].
- **Function: Enhanced security event logging**
  Not applicable since the "Enhanced security event logging" must be enabled, which is done during the initial configuration of the TOE.
- **Function: Managing Temporary Job Files (i.e., image overwrite)**

The evaluator successfully changed the Erasure method to "Secure Fast Erase", then "Secure Sanitize Erase", and finally "Non-Secure Fast Erase".

- **Function: IPsec**
  Not applicable since the "IPsec" must be enabled, which is done during the initial configuration of the TOE.
- **Function: Automatically synchronize with a Network Time Service**
  Not applicable since the "NTS" must be enabled, which is done during the initial configuration of the TOE.

The evaluator also performed several test for each Administrator management interface and verified that only U.ADMIN could access them (not unauthenticated users or U.NORMAL).

2.1.5.2 Management of security attributes (FMT_MSA.1)

TSS Assurance Activities

Assurance Activity AA-FMT_MSA.1-ASE-01

The evaluator shall check to ensure that the TSS contains a description of possible operations for security attributes and given roles to those security attributes, which is consistent with the definition of the SFR.

Summary

The definition of FMT_MSA.1 is provided in [ST] section 6.1.5.2, in particular Table 31 "Management of security attributes" which lists for each security attribute the available operations and roles allowed to perform them.

For each security attribute listed in this table, a corresponding description is provided in the TSS in table entry "FMT_MSA.1 (Management of attributes)" of Table 40. The following list provides a summary of the coverage in the TSS:

- The security attribute "Account identity" (for both Internal and External Authentication mechanisms) has no possible operations available.
- The security attribute "Device Administrator permission set permissions" can be viewed and is restricted to U.ADMIN role.
- The security attribute "Device User and Device Guest permission set permissions" can be modified and viewed and restricted to the U.ADMIN role.
- The security attribute "Custom permission set permissions" can be created, modified, deleted, and viewed and is restricted to the U.ADMIN role.

The evaluator determined that the TSS description is consistent with the definition of FMT_MSA.1.

Guidance Assurance Activities

Assurance Activity AA-FMT_MSA.1-AGD-30

The evaluator shall check to ensure that the administrator guidance contains a description of possible operations for security attributes and given roles to those security attributes, which is consistent with the definition of the SFR.

The evaluator shall check to ensure that the administrator guidance describes the timing of modified security attributes.

Summary

[ST] section 6.1.5.2 "Management of security attributes (FMT_MSA.1)" provides Table 33 "Management of security attributes" of [ST] outlining the allowable operations for security attributes with specific roles.

The evaluator noted that all the security attributes are restricted to the role U.ADMIN. The evaluator created the table below to determine whether corresponding guidance is provided for each security attribute listed in Table 33 of [ST].

Table 9: Management Functions and Guidance

Security Attribute	Operations	Provided Guidance	Evaluator's Comment
Device Administrator permission set permissions	View	[CCECG] chapter 5 "Configure the HCD" section "Access control"	The evaluator determined that per the guidance description, permission sets for Device Administrator can be viewed via the EWS as described in section "Configure permission sets". The HCD contains the following built-in permission set: • Device Administrator - This permission set is granted to administrators (U.ADMIN). This permission set's permissions are not configurable. All permissions in this permission set are hardcoded to grant access. The evaluator noted that the permission set for Administrators are not managed as they are built-in and is not configurable. In addition, the permissions contained in the Device Administrator permission set can also be viewed in the Sign-In and Permissions Policies section.
Device User and Device Guest permission set permissions	Modify, view	[CCECG] chapter 5 "Configure the HCD" section "Access control".	The evaluator determined that per the guidance description, permission sets for Device User and Device Guest can be managed via the EWS as described in section "Configure permission sets", subsection "Configure permissions for control panel realm". Step-by-step instructions are provided to view and configure the Control Panel permissions for each the Device Guest permission set, and Device User permission set to adhere the following requirements: • Device Guest - This permission set is automatically applied to all users. This permission set's permissions are configurable. In the evaluated configuration, all permissions in this permission set must be configured to deny access. • Device User - This permission set is granted to non-administrative users (U.NORMAL). This permission

Security Attribute	Operations	Provided Guidance	Evaluator's Comment
			set’s permissions are configurable. In the evaluated configuration, the permissions in this permission set must be configured to grant access to non-administrative functions and configured to deny access to administrative functions. The table 5-2 "Permissions configuration for control panel realm" lists the permissions configuration for the control panel realm that must be adhered to in the evaluated configuration. The evaluator noted that the Control Panel Mandatory Sign-in is enabled when all permissions in the Device Guest permission are configured to deny access.
Custom permission set permissions	Create, modify, delete, view	[CCECG] chapter 5 "Configure the HCD" section "Access control".	The evaluator determined that per the guidance description, custom permission sets can be managed via EWS interface as described in the subsection "Configure custom permission sets". Step-by-step instructions are provided to create, modify, delete, and view a custom permission set.

Test Assurance Activities

Assurance Activity AA-FMT_MSA.1-ATE-01

The evaluator shall also perform the following tests:

1. *The evaluator shall check to ensure that users of the given roles defined in the SFR can perform operations to the security attributes in accordance with the operation methods specified in the administrator guidance.*
2. *The evaluator shall check to ensure that the operation results are appropriately reflected as specified in the administrator guidance.*
3. *The evaluator shall check to ensure that a user that is not part of an authorized role defined in the SFR is not permitted to perform operations on the security attributes.*

Summary

Table 10: Tests mapped to TOE Components and Security attributes

TOE Component	Security attribute	Test description
Control Panel and EWS subject attributes	Account identity (Internal Authentication mechanism)	Not applicable since [ST] states that "Authorized identified roles" is n/a and "Available operations" is None.

TOE Component	Security attribute	Test description
	Account identity (External Authentication mechanisms)	Not applicable since [ST] states that "Authorized identified roles" is n/a and "Available operations" is None.
	Device Administrator permission set permissions	The evaluator signed in as Device Administrator and that permissions can be viewed.
	Device User and Device Guest permission set permissions	The evaluator signed in as administrator and could performed the tasks specified in the SFR for U.ADMIN.
	Custom permission set permissions	The evaluator signed in as administrator and could performed the tasks specified in the SFR for U.ADMIN.

The evaluator observed the results for each testing activity above and confirmed that the results matched what is presented in the administrator guidance.

The evaluator also verified that U.NORMAL could not access the administrator interfaces except the Control Panel. He then logged in as U.NORMAL in the Control Panel and verified that the user could not access any management functions.

2.1.5.3 Static attribute initialization (FMT_MSA.3)

TSS Assurance Activities

Assurance Activity AA-FMT_MSA.3-ASE-01

The evaluator shall check to ensure that the TSS describes mechanisms to generate security attributes which have properties of default values, which are defined in the SFR.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FMT_MSA.3 (Initialization of attributes)" describes FIA_MSA.3 which refers to the TSS description of FMT_MSA.1.

The TSS description covers two categories of security attributes:

- Control Panel and EWS identities
- Control Panel and EWS roles

Control Panel and EWS identities

For Internal Authentication mechanism, the TOE comes with a built-in Device Administrator account which has a Display name that is considered as a subject identity. This account is granted administrative access by default and the TOE does not provide any management operations for this account's identity. In other words, the Device Administrator account is predefined whose default values cannot be overwritten.

For External Authentication mechanism, the subjects as well as their security attributes are maintained by the External Authentication mechanism and thus the TOE does not provide the capability to overwrite their default values.

Control Panel and EWS roles

Roles are determined by permission sets which consists of Device Administrator permission set, Device User and Device Guest permission set, and Custom permission set (defined at creation). These permission sets are predefined whose default values cannot be modified.

The evaluator verified the above description and found it to be consistent with the definitions of FMT_MSA.1 and FMT_MSA.3.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

Assurance Activity AA-FMT_MSA.3-ATE-60

If U.ADMIN is selected, then testing of this SFR is performed in the tests of FDP_ACF.1.

Summary

The evaluator notes that a refinement has been performed to the SFR which references the selection to the roles defined in FMT_MSA.1.1. U.ADMIN is defined for most roles and therefore the evaluator considered this assurance activity fulfilled by tests for FDP_ACF.1.

2.1.5.4 Management of TSF data (FMT_MTD.1)

TSS Assurance Activities

No assurance activities defined.

Guidance Assurance Activities

Assurance Activity AA-FMT_MTD.1-AGD-01

The evaluator shall check to ensure that the administrator guidance identifies the management operations and authorized roles consistent with the SFR.

The evaluator shall check to ensure that the administrator guidance describes how the assignment of roles is managed.

The evaluator shall check to ensure that the administrator guidance describes how security attributes are assigned and managed.

The evaluator shall check to ensure that the administrator guidance describes how the security-related rules (.e.g., access control rules, timeout, number of consecutive logon failures,) are configured.

Summary

This assurance activity was performed in conjunction with AA-FMT_SMF.1-AGD-01. In that assurance activity, the evaluator verified that the sufficient guidance is provided for the claimed management functions, including guidance for configuring/managing access control rules, timeout, and authentication mechanisms. While analyzing the provided guidance for adequate coverage of

management functions, the evaluator also took into account the associated security attributes. Thus, for this assurance activity, the evaluator focused on analyzing the provided guidance with regard to the management of applicable TSF data.

[ST] section 6.1.5.4 "Management of TSF data (FMT_MTD.1)" provides Table 32 "Management of TSF Data" of [ST] outlining the TSF data and which role manages them. All TSF data listed in Table 32 are managed by the U.ADMIN (i.e., administrator) role.

Guidance for management of TSF data is spread throughout chapter 5 "Configure the HCD" of [CCECG]. The evaluator constructed the following table mapping the managed TSF data listed in Table 32 of [ST] to the corresponding description provided in the guidance.

Table 11: Managed TSF data and Guidance

Managed TSF data	Management operation	Provided Guidance	Evaluator's Comment
Device Administrator password	Change	[CCECG] chapter 5 "Configure the HCD" section "Local administrator password" for Device Administrator Password.	The provided guidance is sufficient.
Permission set associations (except on the Device Administrator account)	Add, delete, view	[CCECG] chapter 5 "Configure the HCD" section "Access control".	The provided guidance is sufficient.
Permission set associations (only on the Device Administrator account)	View	[CCECG] chapter 5 "Configure the HCD" section "Access control".	The provided guidance is sufficient.
IPsec CA and identify certificates	Import, delete	[CCECG] chapter 5 "Configure the HCD" section "Certificates"	The provided guidance is sufficient.
IPsec pre-shared keys	Set, change	[CCECG] chapter 5 "Configure the HCD" section "IPsec"	The provided guidance is sufficient.
NTS server configuration data	Change	[CCECG] chapter 5 "Configure the HCD" section "Date and time"	The provided guidance is sufficient.
Minimum password length	Change	[CCECG] chapter 5 "Configure the HCD" section "Account policy".	The provided guidance is sufficient.
Account lockout maximum attempts	Change	[CCECG] chapter 5 "Configure the HCD" section "Account policy"	The provided guidance is sufficient.
Account lockout interval	Change	[CCECG] chapter 5 "Configure the HCD" section "Account policy"	The provided guidance is sufficient.
Account reset lockout counter interval	Change	[CCECG] chapter 5 "Configure the HCD" section "Account policy"	The provided guidance is sufficient.

Managed TSF data	Management operation	Provided Guidance	Evaluator's Comment
Session inactivity timeout	Change	[CCECG] chapter 5 "Configure the HCD" section "Control panel inactivity timeout" (for the Control Panel) and section "EWS session timeout" (for EWS).	The provided guidance is sufficient.

Test Assurance Activities

Assurance Activity AA-FMT_MTD.1-ATE-01

The evaluator shall perform the following tests:

1. *The evaluator shall check to ensure that users of the given roles defined in the SFR can perform operations to TSF data in accordance with the operation methods specified in the administrator guidance.*
2. *The evaluator shall check to ensure that the operation results are appropriately reflected as specified in the administrator guidance.*
3. *The evaluator shall check to ensure that no users other than users of the given roles defined in the SFR can perform operations to TSF data.*

Summary

Test 1 and Test 2

Test 1 and Test 2 are covered by the tests described in the table below:

Table 12: Tests mapped to Data, Operation and Authorized role

Data	Operation	Authorized role	Test description
List of TSF Data not owned by U.NORMAL			
Device Administrator password	Change	U.ADMIN	The evaluator verified when signed in as U.ADMIN that the administrator could change the Device password.
Permission set associations (except on the Device Administrator account)	Add, delete, view	U.ADMIN	The evaluator verified when signed in as U.ADMIN that the administrator could add, delete and change Permission set associations. However, the evaluator could not add or delete permission set associations for Device Administrator account, as expected.
Permission set associations (only on the Device Administrator account)	View	U.ADMIN	The evaluator verified when signed in as U.ADMIN that the administrator could view Permission set associations for Device Administrator.
List of software, firmware, and related configuration data			

Data	Operation	Authorized role	Test description
IPsec CA and identity certificates	Import, delete	U.ADMIN	The evaluator verified when signed in as U.ADMIN that the administrator could import and delete IPsec CA and identity certificates.
IPsec pre-shared keys	Set, change	U.ADMIN	The evaluator verified when signed in as U.ADMIN that the administrator could set and change IPsec pre-shared keys.
NTS server configuration data	Change	U.ADMIN	The evaluator verified when signed in as U.ADMIN that the administrator could change the NTS server settings.
Minimum password length	Change	U.ADMIN	The evaluator verified when signed in as U.ADMIN that the administrator could change the minimum password length for Device Administrator Password.
Account lockout maximum attempts	Change	U.ADMIN	The evaluator verified when signed in as U.ADMIN that the administrator could change the Account lockout maximum attempts for Local Device Sign In.
Account lockout interval	Change	U.ADMIN	The evaluator verified when signed in as U.ADMIN that the administrator could change the Account lockout interval for Local Device Sign In.
Account reset lockout counter interval	Change	U.ADMIN	The evaluator verified when signed in as U.ADMIN that the administrator could change the Account reset lockout counter interval for Local Device Sign In.
Session inactivity timeout	Change	U.ADMIN	The evaluator verified when signed in as U.ADMIN that the administrator could change the Session inactivity timeout, both for EWS and Control Panel.

Test 3

The evaluator performed several tests to verify that no user other than users of the given roles defined in the SFR can perform operations to TSF data. This is presented in the list below:

- **Interface: Control Panel -** The evaluator authenticated in the Control Panel as regular user (U.NORMAL) and verified which functionality the user had access to. U.NORMAL cannot perform operations to TSF data specified in the SFR.
- **Interface: EWS -** The evaluator accessed the EWS interface from an administrative computer (no others have access to the interface because of IPsec rules). He authenticated as regular user (U.NORMAL) and verified which functionality the user had access to. U.NORMAL cannot perform operations to TSF data specified in the SFR.
- **Interface: REST -** Since only administrative users have accesses to this interface because of IPsec rules, the evaluator tried to access the TOE from the administrative computer using REST with wrong credentials. The attempt failed, as expected.

2.1.5.5 Specification of management functions (FMT_SMF.1)

TSS Assurance Activities

Assurance Activity AA-FMT_SMF.1-ASE-50

The evaluator shall check the TSS to ensure that the management functions are consistent with the assignment in the SFR.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FMT_SMF.1 (Management functions)" describes FIA_SMF.1. The TSS description references Table 33 "Specification of management functions" provided in the definition of FMT_SMF.1 ([ST] section 6.1.5.5 "Specification of Management Functions (FMT_SMF.1)") for the mapping of the management functions and their respective management SFR. Due to the explicit reference to Table 33 in the TSS, the evaluator determined that consistency is established.

Guidance Assurance Activities

Assurance Activity AA-FMT_SMF.1-AGD-01

The evaluator shall check the guidance documents to ensure that management functions are consistent with the assignment in the SFR, and that their operation is described.

Summary

[ST] section 6.1.5.5 "Specification of Management Functions (FMT_SMF.1)" provides Table 33 "Specification of management functions" of [ST] outlining the management functions provided by the TOE. Guidance for these management are described throughout [CCECG]. The evaluator constructed the following table mapping the management functions from Table 33 of [ST] to corresponding description provided in the guidance.

Table 13: Management functions and Guidance

Management Function	Provided Guidance	Consistent?
Management of Device Administrator password	[CCECG] chapter 5 "Configure the HCD" section "Local administrator password"	Yes
Management of account lockout policy	[CCECG] chapter 5 "Configure the HCD" section "Account policy"	Yes
Management of minimum length password settings	[CCECG] chapter 5 "Configure the HCD" section "Account policy"	Yes
Management of Internal and External authentication mechanisms	[CCECG] chapter 5 "Configure the HCD" section "Access control"	Yes
Management of "Allow users to choose alternate sign-in methods at the product control panel" function	[CCECG] chapter 5 "Configure the HCD" section "Access control"	Yes
Management of session inactivity timeouts	[CCECG] chapter 5 "Configure the HCD" section "Control panel inactivity timeout"; section "EWS session timeout"	Yes

Management Function	Provided Guidance	Consistent?
Management of permission set associations	[CCECG] chapter 5 "Configure the HCD" section "Configure permission sets"	Yes
Management of permission set permissions	[CCECG] chapter 5 "Configure the HCD" section "Configure permission sets"	Yes
Management of IPsec pre-shared keys	[CCECG] chapter 5 "Configure the HCD" section "IPsec"; section "Configure IPsec/Firewall templates" subsection "Create an IKEv1 IPsec/Firewall template"	Yes
Management of CA and identity certificates for IPsec authentication	[CCECG] chapter 5 "Configure the HCD"; section "Certificates"; section "IPsec"	Yes
Management of enhanced security event logging	[CCECG] chapter 5 "Configure the HCD" section "Enhanced security event logging"	Yes
Management of NTS configuration data	[CCECG] chapter 5 "Configure the HCD" section "Date and time"	Yes
Management of image overwrite option in "Managing temporary Job Files"	[CCECG] chapter 5 "Configure the HCD" section "Managing temporary job files"	Yes

Test Assurance Activities

No assurance activities defined.

2.1.5.6 Security roles (FMT_SMR.1)

TSS Assurance Activities

Assurance Activity AA-FMT_SMR.1-ASE-01

The evaluator shall check to ensure that the TSS contains a description of security related roles that the TOE maintains, which is consistent with the definition of the SFR.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FMT_SMR.1 (Security roles)" describes FIA_SMR.1. Its states that the TOE supports the two roles U.ADMIN and U.NORMAL which the evaluator found to be consistent with the definition of FMT_SMR.1 provided in [ST] section 6.1.5.6 "Security roles (FMT_SMR.1)".

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

Assurance Activity AA-FMT_SMR.1-ATE-01

As for tests of this SFR, it is performed in the tests of FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1.

Summary

Please see tests for FMT_MOF.1, FMT_MSA.1, and FMT_MTD.1.

2.1.6 Protection of the TSF (FPT)

2.1.6.1 Extended: Protection of key and key material (FPT_KYP_EXT.1)

TSS Assurance Activities

No assurance activities defined.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

No assurance activities defined.

Key Management Assurance Activities

Assurance Activity AA-FPT_KYP_EXT.1-AKM-01

> *The evaluator shall examine the Key Management Description (KMD) for a description of the methods used to protect keys stored in nonvolatile memory.*
>
> *The evaluator shall verify the KMD to ensure it describes the storage location of all keys and the protection of all keys stored in nonvolatile memory.*

Summary

The evaluator examined the entire [KMD] document and found that there is a dedicated section for each key type. Each of these sections describes the storage location in non-volatile memory of relevant keys and how they are protected.

2.1.6.2 Extended: Protection of TSF data (FPT_SKP_EXT.1)

TSS Assurance Activities

Assurance Activity AA-FPT_SKP_EXT.1-ASE-01

> *The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.*

Summary

The evaluator checked Table 40 of the TSS in which table entry "FPT_SKP_EXT.1 (Key viewing protection)" describes FPT_SKP_EXT.1. It states the following:

- The TOE is a closed system and does not provide an interface to read pre-shared keys, symmetric keys, or private keys. As a closed system, it does not allow administrators to read memory or to access storage directly.

- The EWS provides an interface to enter IPsec pre-shared key values that does not allow the administrator to query the current pre-shared key value. No other external interfaces allow for the entering or reading of pre-shared keys.
- IPsec pre-share keys are stored in a file on the field-replaceable SED. This file is not accessible through any interface.
- The SED drive-lock password is stored in cleartext in SPI flash and EEPROM, but the TOE provides no interface to view this key or to access SPI flash and EEPROM.
- Ephemeral asymmetric and symmetric keys created and used in IPsec sessions are inaccessible by any user since the TOE does not provide any user interface to read memory.
- The TOE's private asymmetric keys found in X.509v3 certificates (used by IPsec) can be imported by the TOE, but the EWS interface does not display the private keys contained in these certificates.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

No assurance activities defined.

2.1.6.3 Reliable time stamps (FPT_STM.1)

TSS Assurance Activities

Assurance Activity AA-FPT_STM.1-ASE-01

The evaluator shall check to ensure that the TSS describes mechanisms that provide reliable time stamps.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FPT_STM.1 (Time stamps)" describes FPT_STM.1. It states that the TOE contains an internal system clock that is synchronized using an NTS.

Guidance Assurance Activities

Assurance Activity AA-FPT_STM.1-AGD-01

The evaluator shall check to ensure that the guidance describes the method of setting the time.

Summary

The evaluator examined [CCECG] chapter 5 "Configure the HCD" section "Date and time" which provides guidance for FPT_STM.1. The evaluator found the following guidance:

- In the evaluated configuration, the TOE must be configured to synchronize its date and time with the NTS server.
- Firstly, the time zone must be configured which is done via the EWS interface on the **Date/Time Settings** menu by selecting the local time zone from the "Time Zone" drop-down menu.

- Automatic synchronization with an NTS server can be configured via the EWS interface on the **Date/Time Settings** menu by checking the **Automatically synchronize with a Network Time Server** option from the **Network Time Server** section. The next step is to configure the NTS settings by entering the IP address or hostname of the NTS server.

The evaluator determined that the guidance adequately describes the method of setting the time.

Test Assurance Activities

Assurance Activity AA-FPT_STM.1-ATE-01

The evaluator shall also perform the following tests:

1. *The evaluator shall check to ensure that the time is correctly set up in accordance with the guidance or external network services (e.g., NTP).*
2. *The evaluator shall check to ensure that the time stamps are appropriately provided.*

Summary

Test 1

The evaluator signed in as U.ADMIN and successfully synced the TOE time with the configured Network Time Service (i.e., Network Time Protocol server).

Test 2

The evaluator verified that the time stamp presented after performing Test 1 was correct.

2.1.6.4 Extended: TSF testing (FPT_TST_EXT.1)

TSS Assurance Activities

Assurance Activity AA-FPT_TST_EXT.1-ASE-01

The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FPT_TST_EXT.1 (TSF testing)" describes FPT_TST_EXT.1. It states the following. It describes the TSF testing functionality called Whitelisting as follows:

- During the load process, Whitelisting validates the integrity of system firmware files using RSA-2048 with SHA2-256. If the integrity check of a system firmware file fails, Whitelisting will reboot the HCD and the Basic Input/Output System (BIOS) will hold on boot with an error message displayed on the Control Panel UI.
- The TOE Whitelists and checks dynamic-link libraries (DLLs) and executables that have been signed with Microsoft Authenticode signatures. This includes kernel files, device drivers, and applications.
- Whitelisting uses the HP FutureSmart Windows Mobile Enhanced Cryptographic Provider (RSAENH) 6.00.1937 implementation for both the RSA 2048-bit and SHA2-256 algorithms.

The evaluator confirmed that the TSS details the self-tests that are run by the TSF on start-up and that the tests are sufficient to demonstrate that the TSF is operating correctly.

Guidance Assurance Activities

Assurance Activity AA-FPT_TST_EXT.1-AGD-01

The evaluator shall also ensure that the operational guidance describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.

Summary

According to the FPT_TST_EXT.1 (TSF testing) TSS of [ST] section 7.1.1 "TOE SFR compliance rationale", the TOE performs Whitelisting of firmware files while booting. If any of the files fail the integrity check, the TOE reboots and the BIOS will hold on boot with an error message displayed on the Control Panel UI.

[CCECG] chapter 6 "Operational guidance" section "Whitelisting" provides relevant guidance for FTP_TST_EXT.1. It states the following:

- Whitelisting uses code-signing to make sure that only authentic HP code and third-party solution files are loaded. If validation of a firmware file fails, the HCD will not load the HP code / third-party solution file, will reboot, and will display the preboot menu options on the control panel, thus preventing a potential malware exploit from executing. Digital signatures for HP code and third-party developed solutions residing on the HCD are validated using a SHA-256 hashing algorithm for HP firmware and a SHA1/-256 hash for third-party firmware.

  NOTE: In the evaluated configuration, third-party solutions must not be installed.
- When a failure occurs in the validation of firmware files digital signature or the firmware file certificate, a 33.05.1X Whitelisting error code is generated to report the security event. Whitelisting errors are described in Table 6-2 "EWS event log entries for 33.05.1X Whitelisting errors and solutions" and Table 6-3 "Control panel error codes and messages for 33.05.1X Whitelisting errors and solutions" of [CCECG].
- If any of the Whitelisting errors seen on the control panel screen, the administrator must perform a partial clean as described in subsection "Perform a partial clean" [CCECG].
- If the HCD does not reboot to a ready state, the administrator must reinstall the CC certified TOE firmware from the preboot menu using a USB thumb-drive. For steps to reinstall the CC certified TOE firmware from the preboot menu using a USB thumb-drive, see the Reinstall CC certified TOE firmware from preboot menu section.

Test Assurance Activities

No assurance activities defined.

2.1.6.5 Extended: Trusted update (FPT_TUD_EXT.1)

TSS Assurance Activities

Assurance Activity AA-FPT_TUD_EXT.1-ASE-01

The evaluator shall check to ensure that the TSS contains a description of mechanisms that verify software for update when performing updates, which is consistent with the definition of the SFR.

The evaluator shall check to ensure that the TSS identifies interfaces for administrators to obtain the current version of the TOE as well as interfaces to perform updates.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FPT_TUD_EXT.1 (Trusted update)" describes FPT_TUD_EXT.1. It states the following:

- The TOE's firmware can be updated by an administrator by downloading an update image from the HP Inc. Software Depot kiosk (website) and installing it on the TOE.
- Each update image is digitally signed by HP using the RSA 2048-bit and SHA2-256 algorithms. Each HCD has a factory-installed public key certificate from HP for verifying the update image's digital signature.
- Once the update image is uploaded to the TOE by the administrator through the EWS interface, the TOE verifies the update image's signature prior to installing using the RSA 2048-bit and SHA2-256 algorithms and the factory installed certificate. If the TOE's signature verification fails, the TOE won't allow the update to proceed.
- The current version of both the System firmware and the Jetdirect Inside firmware can be obtained through Control Panel and EWS.

The evaluator verified that in the TSS, the description of mechanisms that verify software for update when performing updates is consistent with the definition of the SFR. The evaluator also verified that the TSS identifies interfaces for administrators to obtain the current version of the TOE as well as interfaces to perform updates.

Guidance Assurance Activities

Assurance Activity AA-FPT_TUD_EXT.1-AGD-01

> *The evaluator shall check to ensure that the administrator guidance contains descriptions of the operation methods to obtain the TOE version as well as the operation methods to start update processing, which are consistent with the description of the TSS.*

Summary

According to the FPT_TUD_EXT.1 (Trusted update) TSS of [ST] section 7.1.1 "TOE SFR compliance rationale", the TOE firmware update image can be obtained electronically from the HP Inc. Software Depot kiosk. The download is digitally signed by HP using RSA 2048-bit and SHA2-256 algorithms which can be verified using the factory-installed HP certificate. Once downloaded, the image can be uploaded to the TOE via the EWS interface, which verifies the digitally signed update image using the RSA 2048-bit and SHA2-256 algorithms and the factory-installed certificate. The TOE will not install the update if the signature verification fails.

Also, the TSS states TOE's firmware versions (i.e., System firmware and Jetdirect Inside firmware) can be obtained via the Control Panel or EWS.

The evaluator examined [CCECG] chapter 5 "Configure the HCD" section "Certified TOE firmware" provides guidance for updating the TOE firmware and verifying the firmware version.

Additionally, section "Update the firmware" provides step-by-step instructions to install the TOE firmware update via the EWS interface which involves selecting the Firmware Upgrade menu item to upload/transfer the update to the TOE. After the update transfer is finished, the device will reboot itself and applies the update during start-up.

The TOE firmware version can be obtained via the EWS or Control panel interface. For each of these interfaces, section "Check version of installed TOE firmware" of [CCECG] describes step-by-step instructions to get the TOE version information.

Test Assurance Activities

Assurance Activity AA-FPT_TUD_EXT.1-ATE-01

The evaluator shall also perform the following tests:

1. *The evaluator shall check to ensure the current version of the TOE can be appropriately obtained by means of the operation methods specified by the administrator guidance.*
2. *The evaluator shall check to ensure that the verification of the data for updates of the TOE succeeds using authorized data for updates by means of the operation methods specified by the administrator guidance.*
3. *The evaluator shall check to ensure that only administrators can implement the application for updates using authorized data for updates.*
4. *The evaluator shall check to ensure that the updates are correctly performed by obtaining the current version of the TOE after the normal updates finish.*
5. *The evaluator shall check to ensure that the verification of the data for updates of the TOE fails using unauthorized data for updates by means of the operation methods specified by the administrator guidance. (The evaluator shall also check those cases where hash verification mechanism and digital signature verification mechanism fail.)*

Summary

Test 1

The evaluator verified the download and firmware verification process during evaluation of AGD_PRE.1-1.

Test 2

The evaluator installed an authorized update and verified that it was successful.

Test 3

The evaluator first verified that unauthenticated user cannot access management functions of the TOE. He then verified that regular users (U.NORMAL) cannot update the firmware via the management interface (EWS). The evaluator also notes that only the administrative computer has access to the EWS interface. All other computers are blocked using IPsec.

Test 4

The administrator guidance describes that you can check firmware (TOE) version using EWS and Control Panel. The evaluator verified that the TOE version can be obtained using each interface described in the administrator guidance.

Test 5

The evaluator first tried to install a firmware bundle with a bad signature, the installation failed as expected. The evaluator then tried to install a firmware bundle that was not signed, the installation failed as expected.

2.1.7 TOE access (FTA)

2.1.7.1 TSF-initiated termination (FTA_SSL.3)

TSS Assurance Activities

Assurance Activity AA-FTA_SSL.3-ASE-01

The evaluator shall check to ensure that the TSS describes the types of user sessions to be terminated (e.g., user sessions via operation panel or Web interfaces) after a specified period of user inactivity.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FTA_SSL.3 (Interactive session termination)" describes FTA_SSL.3. It states that all Control Panel and EWS sessions support session termination as well as administrator-configurable timeout periods. The TOE's REST interfaces do not support the concept of sessions.

Guidance Assurance Activities

Assurance Activity AA-FTA_SSL.3-AGD-01

The evaluator shall check to ensure that the guidance describes the default time interval and, if it is settable, the method of setting the time intervals until the termination of the session.

Summary

The evaluator examined [CCECG] chapter 5 "Configure the HCD" in which section "Control panel inactivity timeout" and section "EWS session timeout" provide guidance for FTA_SSL.3.

Per section "Control panel inactivity timeout", the administrator can configure the inactivity timeout for the Control Panel using the Inactivity Timeout configuration option on the EWS. This is configured by specifying 10-60 in the **Inactivity Timeout** in the **Display Settings** of the **General** tab of the EWS. 60 seconds is the default value.

Per section "EWS session timeout", the administrator can configure the inactivity timeout using the EWS by selecting the **General Security** menu item from the **Security** tab and specify a value of 3-10 minutes in the **EWS Session Timeout** field in the **Embedded Web Server Options**. By default, the EWS session timeout is set to 30 minutes.

Test Assurance Activities

Assurance Activity AA-FTA_SSL.3-ATE-01

The evaluator shall also perform the following tests:

1. *If it is settable, the evaluator shall check to ensure that the time until the termination of the session can be set up by the method of setting specified in the administrator guidance.*
2. *The evaluator shall check to ensure that the session terminates after the specified time interval.*
3. *The evaluator shall perform the tests 1 and 2 described above for all the user sessions identified in the TSS.*

Summary

The TSS describes two user sessions that are applicable, Control Panel and EWS. Test 1, 2 and 3 were executed together.

- **Interface: Control Panel -** The evaluator configured the session time for Control Panel sessions to 10 seconds. He then signed in on the Control Panel as U.NORMAL and verified that the user was signed out after 10 seconds inactivity. He then signed in as U.ADMIN and verified that the user was signed out after 10 seconds inactivity.
- **Interface: EWS -** The evaluator configured the session time for EWS sessions to 3 minutes. He then signed out and signed in on the EWS and verified that the user was signed out after 3 minutes inactivity.

2.1.8 Trusted path/channels (FTP)

2.1.8.1 Inter-TSF trusted channel (FTP_ITC.1)

TSS Assurance Activities

Assurance Activity AA-FTP_ITC.1-ASE-01

The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST. The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FTP_ITC.1 (Trusted channel)" describes FTP_ITC.1. It states that the TOE uses IPsec to protect communications between itself and the following authorized IT entities.

- authentication server
- DNS server
- FTP server
- NTS server
- SharePoint server
- SMB server
- SMTP server
- syslog server (audit server)
- WINS server

All trusted communication channels to authorized IT entities use IPsec. The TSS refers to the TSS description of FCS_IPSEC_EXT.1 which the evaluator already assessed in the respective assurance activities for FCS_IPSEC_EXT.1.

The evaluator also examined the operational guidance [CCECG] and confirmed that section "IPsec" provides sufficient instructions for establishing IPsec connection with each authorized IT entity and that it also contains recovery instructions should a connection be unintentionally broken.

Guidance Assurance Activities

No assurance activities defined.

Test Assurance Activities

Assurance Activity AA-FTP_ITC.1-ATE-01

The evaluator shall also perform the following tests:

1. *The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.*
2. *For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE.*
3. *The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data are not sent in plaintext.*

4. *The evaluator shall ensure, for each protocol associated with each authorized IT entity tested during test 1, the connection is physically interrupted. The evaluator shall ensure that when physical connectivity is restored, communications are appropriately protected.*

Further assurance activities are associated with the specific protocols.

Summary

The evaluator notes that IPsec is the only protocol selected in [ST] for the SFR FTP_ITC.1.

Test 1, 2 and 3

The evaluator set up Wireshark on the Trusted IT Product and recorded all network traffic. He then performed activities on the TOE so that it would make a connection to the service, e.g. Syslog. This was done for all services listed in FTP_ITC.1.3. Afterwards the evaluator analyzed the traffic log and verified that all relevant traffic was sent encrypted using IPsec.

Test 4

The evaluator set up Wireshark on the Trusted IT Product and recorded all network traffic. He then performed activities on the TOE so that it would make a connection to the service, e.g. Syslog. He then unplugged the network cable from the TOE, waited 5 seconds, then plugged it back. After that he performed some activities on the TOE so that it would make a connection to the same service. This was done for all services listed in FTP_ITC.1.3. Afterwards the evaluator analyzed the traffic log and verified that all relevant traffic was sent encrypted using IPsec and that the physical interruption did not affect the protection of the network traffic.

2.1.8.2 Trusted path (for Administrators) (FTP_TRP.1(a))

TSS Assurance Activities

Assurance Activity AA-FTP_TRP.1-A-ASE-01

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.

Summary

The evaluator checked Table 40 of the TSS in which table entry "FTP_TRP.1(a) (Administrator trusted path) describes FTP_TRP.1(a). It lists the administrative interfaces which connect over IPsec as follows:

- EWS (via a web browser)
- REST

All these remote administrative interfaces use IPsec. The TSS refers to the TSS description of FCS_IPSEC_EXT.1 which the evaluator already assessed in the respective assurance activities for FCS_IPSEC_EXT.1. The TSS description is found to be consistent with the definition of FTP_TRP.1(a) ([ST] section 6.1.8.2) which specifies that the TOE uses IPsec for trusted communication with remote administrator.

Guidance Assurance Activities

Assurance Activity AA-FTP_TRP.1-A-AGD-01

The evaluator shall confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.

Summary

According to the FTP_TRP.1(a) (Administrator trusted path) TSS of [ST] section 7.1.1 "TOE SFR compliance rationale", the TOE implements IPsec to provide a trusted path between itself and remote administrators. The following interfaces are the remote administrative interfaces of the TOE in the evaluated configuration:

- EWS (via a web browser)
- REST

The evaluator noted that the majority of evaluated configuration tasks are performed from the EWS interface, thus the evaluator determined that EWS is the main administrative interface of the TOE.

Guidance to access the EWS interface is provided in chapter 5 "Configure the HCD" starting with section "How to find the HCD's IP address or hostname". EWS is accessed via a web browser with the TOE's address or hostname as described in section "How to access the EWS".

Guidance to access the REST interface is provided in chapter 6 "Operational guidance" section "REST Web Services authentication" includes which credentials are used to authenticate against the TOE and the mechanisms used by the TOE to authenticate users.

Since all the remote administrative interfaces listed above are connected via IPsec thus the evaluator looked for guidance on IPsec. The evaluator found in [CCECG] chapter 5, "Configure the HCD", section "IPsec" as guidance dedicated to IPsec. This section is very detailed providing proper instructions to configure IPsec including creating an address template and service template as well as IPsec/Firewall template (including specification of cryptographic-related settings defined in [ST]) and IPsec/Firewall rules.

The evaluator determined that appropriate guidance is provided for establishing each trusted path defined in FTP_TRP.1(a) of [ST].

Test Assurance Activities

Assurance Activity AA-FTP_TRP.1-A-ATE-01

The evaluator shall also perform the following tests:

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.*
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 a remote administrative sessions without invoking the trusted path.*
3. *The evaluator shall ensure, for each method of remote administration, the channel data are not sent in plaintext.*

Further assurance activities are associated with the specific protocols.

Summary

The evaluator notes that IPsec is the only protocol selected in [ST] for the SFR FTP_TRP.1(a).

The evaluator set up Wireshark on Administrative Computer and recorded all network traffic. He connected to TOE using all administrative interfaces. Afterwards the evaluator analyzed the traffic log and verified that all relevant traffic was sent encrypted using IPsec.

During testing and guidance review, the evaluator found no available interface that can be used by a remote user to establish a remote administrative sessions without invoking the trusted path.

2.2 Security Assurance Requirements

2.2.1 Guidance documents (AGD)

2.2.1.1 Operational user guidance (AGD_OPE.1)

Assurance Activity AA-AGD_OPE.1-OPE-01

The contents of operational guidance are confirmed by the assurance activities in Section 4 [of the PP], and applicable assurance activities in Appendix B, Appendix C, and Appendix D [of the PP], and the TOE evaluation in accordance with the CEM.

The evaluator shall check to ensure that the following guidance is provided:

Procedures for administrators to confirm that the TOE returns to its evaluation configuration after the transition from the maintenance mode to the normal Operational Environment.

Summary

Section "Operational modes of the HCD" in Chapter 6 of [CCECG] describes the modes of operation of the TOE. There are 5 operational modes:

- Ready
- Sleep mode
- Powered off
- Boot up
- Error condition

In the Ready mode, the HCD is powered on and fully operational.

The HCD enters Sleep mode when a predefined period of user inactivity is reached or per sleep schedule. The user can also press the sleep button on the control panel to put the HCD in Sleep mode. While in Sleep mode, the HCD is not operational but IPsec is still working to restrict access to the HCD's functions over the network and to secure all network data exchanges with client computers. Secure event logging also continues in the Sleep mode. The HCD must exit the Sleep mode before a user can access any functions from the control panel. The HCD exits the Sleep mode when certain events occur (e.g. a job submission) or per a wake schedule.

When powered off, the HCD does not accept user input through any of its interfaces. Any user with physical access to the HCD can power it on.

During boot-up, the user can interact with the control panel to enter the preboot menu. To access any diagnostic functions in the preboot menu, the user must sign in with the preboot menu administrator password. Besides the diagnostic functions available in the preboot menu, there are no other functions the user can access through the control panel prior to system initialization completing.

Depending on the error condition, the HCD may or may not accept user input through its interfaces. For most error conditions, the HCD displays a message and an animation on the control panel that describes the error and corrective action to take. The help screens on the control panel can also be used to diagnose different errors related to normal device operations. As found in AGD_OPE.1-4, the provided guidance provides instructions for actions to take in various error conditions.

The evaluator concludes that [CCECG] clearly identifies all modes of operation and the implications of each mode on secure operation.

2.2.1.2 Preparative procedures (AGD_PRE.1)

Assurance Activity AA-AGD_PRE.1-PRE-01

The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.

Summary

[CCECG] which provides both operational and preparative guidance is the main and only user guidance required for the evaluated configuration of the TOE. Unless stated otherwise, [CCECG] supersedes all other related information in other product documentations. Also, [CCECG] in Table 1-1 "Supported HCD models and evaluated System firmware versions" covers all TOE platforms claimed in [ST] as explicitly listed chapter 1 "Introduction". The supported scanner models are listed in the table below:

Table 14: Supported HCD models and evaluated System firmware versions

Model name	Product number	System firmware version
HP Digital Sender Flow 8500 fn2 Document Capture Workstation	L2762A	2411221_066358
HP ScanJet Enterprise Flow N9120 fn2 Document Scanner	L2763A	2411221_066386

All scanner models use the same JSI24110061 Jetdirect Inside firmware version.

The evaluator concluded that provided guidance, i.e., [CCECG] covers all the TOE platforms claimed in [ST].

2.2.2 Tests (ATE)

2.2.2.1 Independent testing - conformance (ATE_IND.1)

Assurance Activity AA-ATE_IND.1-ATE-01

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators must document in the test plan that each applicable testing requirement in the ST is covered.

The Test Plan identifies the product models to be tested, and for those product models not included in the test plan but included in the ST, the test plan provides a justification for not testing the models. This justification must address the differences between the tested models and the untested models, 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 affect; rationale must be provided. In case the ST describes multiple models (product names) in particular, the evaluator shall consider the differences in language specification as well as the influences, in which functions except security functions such as a printing function, may affect security functions when creating this justification. If all product models claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each product model 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 model 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.

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include the goal of the particular procedure, the test steps used to achieve the goal, and the 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.

Summary

The evaluator created a test plan containing the following information:

- Test cases that fulfill all Test Assurance Activities specified in [HCDPPv1.0], [HCDPP-ERRATA] and Technical Decisions listed in [ST] 2.1.1 "Protection Profile for Hardcopy Devices; IPA, NIAP, and the MFP Technical Community ([HCDPP])".
- Test results from each test case.
- The exact TOE models that were used during testing.
- Detailed description of the test environment and special setups of the TOE for certain tests. The test environment description also includes information about the tools used during testing.
- The test plan also includes test objectives, test procedures, expected outcome of the test and test results.

2.2.3 Life-cycle support (ALC)

2.2.3.1 Labelling of the TOE (ALC_CMC.1)

Assurance Activity AA-ALC_CMC.1-ALC-01

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 ensure that this identifier is sufficient for an acquisition entity to use in procuring the TOE (including the appropriate administrative guidance) as specified in the ST. Further, 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 web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

Summary

The [ST] specifies in section 1.4, "TOE Overview", that the TOE is a hardcopy device (HCD), including internal firmware and the guidance documentation. Table 1, "TOE hardware and firmware reference", in the [ST] provides specific model numbers for the hardware, and version numbers for the firmware. Table 2 "TOE English-guidance documentation reference" contains the TOE's English-guidance documentation reference, i.e. the [CCECG] and the user guides.

The [CCECG] chapter 2 contains detailed step-by-step instruction for downloading the firmware and guidance portion of the TOE from developer's web site as a .zip file. Tables 2-1 and 2-2 in the "Acquire the TOE firmware and guidance documentation files" section of the same chapter are separated by hardware model, number and detail the content of each of these files. At the time of this report, these files were not available on the web site, however, the evaluator is confident that the correct file will be easily identifiable based on the model number of the hardware.

Examination of the developer's website demonstrated that hardware products are always referred to by name and model number, for example "HP Digital Sender Flow 8500 fn2 Document Capture Workstation". This is the nomenclature used to identify the correct hardware and firmware of the TOE in the [ST], and is sufficient for an acquisition entity to use in procuring the TOE.

Table 1-1 and Table 5-1 of the [CCECG] also contain a list of TOE models and firmware versions. These models and their corresponding firmware versions are identical to those in the [ST].

The evaluator verified during testing that the TOE hardware is labeled with model name and product number. These labels are consistent with the models given in the [ST]. As described in ATE_IND.1-1, the TOE firmware versions are verified during independent testing by following the instructions in the [CCECG].

The evaluator due the remote test only procedure, checked the hardware portions of the TOE used for testing at the developer's site in Boise, ID, USA, by means of photographic evidence [TOEPICS]. The evaluator observed that the product number of the photographic evidence matches with the product number in both the [ST] and [CCECG].

2.2.3.2 TOE CM coverage (ALC_CMS.1)

Assurance Activity AA-ALC_CMS.1-ALC-01

The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

Summary

Table 1, "TOE hardware and firmware reference", in the [ST] provides a complete list of TOE models and firmware versions. Table 1-1 and Table 5-1 of the [CCECG] also contain a list of TOE models and firmware versions. The models and their corresponding firmware versions in these tables are identical.

2.2.4 Vulnerability assessment (AVA)

2.2.4.1 Vulnerability survey (AVA_VAN.1)

Assurance Activity AA-AVA_VAN.1-AVA-01

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 printing devices and the implemented communication protocols 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, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid nitrogen, for instance, then a test would not be suitable and an appropriate justification would be formulated.

Summary

The evaluator used the following vulnerability databases for the public vulnerability search:

- Common Vulnerabilities and Exposures (CVE)
  https://cve.mitre.org/cve/search_cve_list.html
- Exploit Database (EDB)
  https://www.exploit-db.com/
- Packet Storm (PS)

https://packetstormsecurity.com

- Hewlette-Packard Support Center
  https://support.hp.com/us-en

The search was also performed using Google.

The last public vulnerability search was performed on 2023-07-21.

Based on an analysis of TOE components and interfaces, the evaluator devised the following list of search terms to use in the aforementioned vulnerability searches:

- IPsec
- IKEv1
- Digital Sender/ScanJet Enterprise
- Capture Workstation/Document Scanner
- Windows Embedded CE 6.0 R3
- Arm Cortex-A8
- OpenSSL FIPS Object Module 2.0.4
- QuickSec 5.1
- RSAENH
- Rebex
- Seagate Self-Encrypting Drive
- JetDirect

The evaluator found no vulnerabilities applicable to the TOE that could be exploited by a Basic Attack Potential or that required any additional testing apart from the evaluator's normal independent testing.

In addition to the vulnerability searches, the evaluator also performed a port scan on all TCP and UDP ports using both IPv4 and IPv6 addresses to verify no unexpected ports were open.

A Appendixes

A.1 References

CAVP_TEST **CAVP testing**
Date 2023-08-03
File name ate/TestVectorsAndResults.zip

CC **Common Criteria for Information Technology Security Evaluation**
Version 3.1R5
Date April 2017
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

CCDB-2017-05-17 **CC and CEM addenda - Exact Conformance, Selection-Based SFRs, Optional SFRs**
Version 0.5
Date 2017-05-17
Location https://www.commoncriteriaportal.org/files/ccfiles/CCDB-2017-05-17-CCaddenda-Exact_Conformance.pdf

CCECG **Common Criteria Evaluated Configuration Guide for HP Document Scanners HP Digital Sender Flow 8500 fn2 Document Capture Workstation HP ScanJet Enterprise Flow N9120 fn2 Document Scanner**
Author(s) HP Inc.
Version Edition 1
Date 8/2023
File name agd/HP_YA3_HCDPP_CCECG_Ed_1.pdf

CCEVS-TD0157 **FCS_IPSEC_EXT.1.1 - Testing SPDs**
Date 2017-06-15
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0157

CCEVS-TD0176 **FDP_DSK_EXT.1.2 - SED Testing**
Date 2017-04-11
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0176

CCEVS-TD0219 **NIAP Endorsement of Errata for HCD PP v1.0**
Date 2017-07-07
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0219

CCEVS-TD0253 **Assurance Activities for Key Transport**
Date 2017-11-08
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0253

CCEVS-TD0261 **Destruction of CSPs in flash**
Date 2017-11-14
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0261

CCEVS-TD0393 **Require FTP_TRP.1(b) only for printing**
Date 2019-02-26
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0393

CCEVS-TD0474 **Removal of Mandatory Cipher Suite in FCS_TLS_EXT.1**
Date 2019-12-04
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0474

CCEVS-TD0494 **Removal of Mandatory SSH Ciphersuite for HCD**
Date 2020-02-20
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0494

CCEVS-TD0562 **Test activity for Public Key Algorithms**
Date 2021-01-27
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0562

CCEVS-TD0642 **FCS_CKM.1(a) Requirement; P-384 keysize moved to selection**
Date 2022-06-17
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0642

CEM **Common Methodology for Information Technology Security Evaluation**
Version 3.1R5
Date April 2017
Location http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf

EAR **Entropy Assessment Report for HP Hardcopy Devices with 4.12 Firmware and Windows Embedded CE 6.0 R3 HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner**
Author(s) HP Inc.
Version 1.0
Date 2023-01-20
File name aen/YA3-HCDPP_HCDs_EAR.v1.0.pdf

FIPS186-4 **Digital Signature Standard (DSS)**
Date 2013-07-19
Location https://csrc.nist.gov/pubs/fips/186-4/final

HCDPP-ERRATA **Protection Profile for Hardcopy Devices**
Version 1.0
Date 2017-07-01
Location https://www.niap-ccevs.org/MMO/PP/pp_hcd_v1.0-err.pdf
File name ase/PP/pp_hcd_v1.0-err.pdf

HCDPPv1.0	**HardCopy Device Protection Profile** Date received 2015-09-10 Location https://www.niap-ccevs.org/MMO/PP/pp_hcd_v1.0.pdf File name ase/PP/pp_hcd_v1.0.pdf
HP_CAVS	**Cryptographic Modules and CAVS Testing Instructions** Date received 2023-07-17 File name ate/HP_CAVS_Testing.pdf
KMD	**Key Management Description for HP Hardcopy Devices with 4.12 Firmware and Windows Embedded CE 6.0 R3 HP Digital Sender Flow 8500 fn2 Document Capture Workstation HP ScanJet Enterprise Flow N9120 fn2 Document Scanner** Version 1.0 Date 2023-01-20 File name akm/YA3-HCDPP_KMD_v1.0
ManualTestResults	**atsec manual test results** Date 2023-07-26 File name ate/ManualTests.zip
OCSI-NIS01	**Scheme Information Notice No. 1/23 - Changes to LGP1** Version 1.1 Date 2023-08-21
OCSI-NIS02	**Scheme Information Notice No. 2/23 - Changes to LGP2** Version 1.1 Date 2023-08-21
OCSI-NIS03	**Scheme Information Notice No. 3/23 - Changes to LGP3** Version 1.1 Date 2023-08-21
OCSI-NIS04	**Scheme Information Notice No. 4/23 - Assurance Continuity** Version 1.1 Date 2023-08-21
OCSI-NIS05	**Scheme Information Notice No. 5/13 - Conditions for performing tests remotely in Common Criteria evaluations** Version 1.1 Date 2023-08-21
RFC3526	**More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)** Author(s) T. Kivinen, M. Kojo Date 2003-05-01 Location http://www.ietf.org/rfc/rfc3526.txt
SP800-56A-Rev3	**Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography** Date 2018-04-16 Location https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final

ST	**HP Digital Sender Flow 8500 fn2 Document Capture Workstation, HP ScanJet Enterprise Flow N9120 fn2 Document Scanner Security Target**	
	Version	1.0
	Date	2023-08-14
	File name	ase/HP_YA3-HCDPP_ST_v1.0/HP_YA3-HCDPP_ST_v1.0.pdf
TOEPICS	**TOEPICS**	
	Date received	2023-06-16
	File name	alc/DevicePictures.zip
VTL	**Virtual Test Lab Environment for Common Criteria Certification Testing**	
	Version	2.8
	Date received	2023-06-22
	File name	ate/CCC_Virtual_Test_Lab_Environment_v2.8.pdf

A.2 Glossary

Augmentation
The addition of one or more requirement(s) to a package.

Authentication data
Information used to verify the claimed identity of a user.

Authorised user
A user who may, in accordance with the SFRs, perform an operation.

Class
A grouping of CC families that share a common focus.

Component
The smallest selectable set of elements on which requirements may be based.

Connectivity
The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Dependency
A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.

Deterministic RNG (DRNG)
An RNG that produces random numbers by applying a deterministic algorithm to a randomly selected seed and, possibly, on additional external inputs.

Element
An indivisible statement of security need.

Entropy
The entropy of a random variable X is a mathematical measure of the amount of information gained by an observation of X.

Evaluation
Assessment of a PP, an ST or a TOE, against defined criteria.

Evaluation Assurance Level (EAL)
An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.

Evaluation authority
A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.

Evaluation scheme
The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

Exact conformance
a subset of Strict Conformance as defined by the CC, is defined as the ST containing all of the requirements in the Security Requirements section of the PP, and potentially requirements from Appendices of the PP. While iteration is allowed, no additional requirements (from the CC parts 2 or 3) are allowed to be included in the ST. Further, no requirements in the Security Requirements section of the PP are allowed to be omitted.

Extension
The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.

External entity
Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

Family
A grouping of components that share a similar goal but may differ in emphasis or rigour.

Formal
Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Guidance documentation
Documentation that describes the delivery, preparation, operation, management and/or use of the TOE.

Identity
A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

Informal
Expressed in natural language.

Object
A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Operation (on a component of the CC)
Modifying or repeating that component. Allowed operations on components are assignment, iteration, refinement and selection.

Operation (on an object)
A specific type of action performed by a subject on an object.

Operational environment
The environment in which the TOE is operated.

Organisational Security Policy (OSP)
A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment.

Package
A named set of either functional or assurance requirements (e.g. EAL 3).

PP evaluation
Assessment of a PP against defined criteria.

Protection Profile (PP)
An implementation-independent statement of security needs for a TOE type.

Random number generator (RNG)
A group of components or an algorithm that outputs sequences of discrete values (usually represented as bit strings).

Refinement
The addition of details to a component.

Role
A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret
Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

Secure state
A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.

Security attribute
A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.

Security Function Policy (SFP)
A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.

Security objective
A statement of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions.

Security Target (ST)
An implementation-dependent statement of security needs for a specific identified TOE.

Seed
Value used to initialize the internal state of an RNG.

Selection
The specification of one or more items from a list in a component.

Semiformal
Expressed in a restricted syntax language with defined semantics.

ST evaluation
Assessment of an ST against defined criteria.

Subject
An active entity in the TOE that performs operations on objects.

Target of Evaluation (TOE)
A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE evaluation
Assessment of a TOE against defined criteria.

TOE resource
Anything useable or consumable in the TOE.

TOE Security Functionality (TSF)
A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.

Transfers outside of the TOE
TSF mediated communication of data to entities not under control of the TSF.

True RNG (TRNG)
A device or mechanism for which the output values depend on some unpredictable source (noise source, entropy source) that produces entropy.

Trusted channel
A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.

Trusted path
A means by which a user and a TSF can communicate with necessary confidence.

TSF data
Data created by and for the TOE, that might affect the operation of the TOE.

TSF Interface (TSFI)
A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.

User
See external entity

User data
Data created by and for the user, that does not affect the operation of the TSF.