Assurance Activity Report for
INTEGRITY Enterprise OS - Archon Edition

INTEGRITY Enterprise OS – Archon Edition Security Target

Protection Profile for General Purpose Operating Systems, Version 4.2.1 [GPOSPP]

Evaluated by:

intertek acumen security

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Archon Secure LLC

The Author of the Security Target:
Acumen Security, LLC

The TOE Evaluation was Sponsored by:
Archon Secure LLC

Evaluation Personnel:
Anthony Busciglio
Lucas Shaefer

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	CHANGES
1.0	2/20/2022	Initial Release
1.1	4/11/2022	Responses to ECRs

Table of Contents

1 TOE Overview

The TOE is the INTEGRITY Enterprise OS – Archon Edition, which provides a secure computing environment for mobile platforms. The TOE provides end users with the ability to install their own custom user software in a high security sandbox, while maintaining a secure operating system enclave logically isolated from the end user's application.

2 Assurance Activities Identification

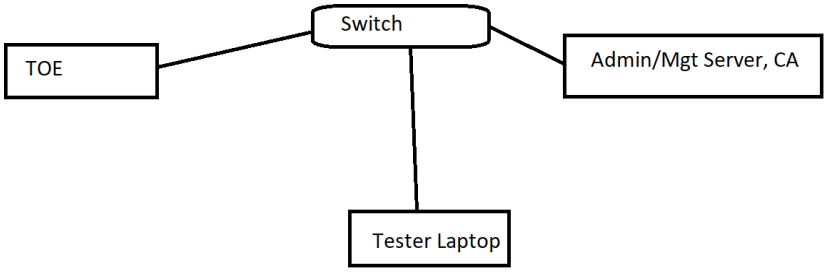
The Assurance Activities contained within this document include all those defined within the GPOS PP v4.2.1.

3 Test Equivalency Justification

The TOE consists of a single OS tested on a single hardware platform, so an equivalency justification is not necessary.

4 Test Bed Descriptions

4.1 Test Bed Diagram



4.2 Detailed Test Information

Name	OS	Version	Function & Location	Protocols	Time	Tools (version)
Archon ZV 5400	INTEGRITY Enterprise OS – Archon Edition	1.0	TOE	TLS ICMP	Manually set	• Anyconnect VPN 4.7 • Aruba VPN 3.4
Administration/ Management Server	Ubuntu 20	20	Third-party VPN Testing	ICMP ISAKMP ESP	Manually set	• INTEGRTY Administration Server (Archon Edition 1.0) • INTEGRITY Management Server (Archon Edition 1.0) • Anyconnect VPN (4.7) • Aruba VPN (3.4) • Wireshark (3.0)
Administration/ Management Server	Ubuntu 20	20	Third-party VPN Testing	ICMP	Manually set	• INTEGRTY Administration Server (Archon Edition 1.0) • INTEGRITY Management Server (Archon Edition 1.0) • Anyconnect VPN (4.7) • Aruba VPN (3.4) • Wireshark (3.0)
Network Switch	IOS XE	15.2	Lab Switch	N/A	Manually set	N/A
Administration/ Management Server	Ubuntu 20	Archon Edition 1.0	Remote administration TLS/X509 Testing Certificate Authority	TLS	Manually set	• INTEGRTY Administration Server (Archon Edition 1.0) • INTEGRITY Management Server (Archon Edition 1.0) • OpenSSL (1.1.1) • Acumen_TLSC (8-23-21) • Wireshark (3.0)
Tester Laptop	Windows 10	10	Test Interface	TLS	Manually set	N/A
Packet captures were taken from the Administration/Management Server.						

4.3 Test Time and Location

Testing was carried at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850 by the evaluator. Testing occurred from February 2021 through February 2022.

Testing was performed within Acumen's Common Criteria lab in a controlled, isolated environment and completed by the Acumen Security Evaluation Team following the CCTL's NVLAP-accredited test procedure.

5 Detailed Test Cases (TSS and Guidance Activities)

5.1 Assurance Activities (Auditing)

5.1.1 FAU_GEN.1.1 Guidance 1

The evaluator will check the administrative guide and ensure that it lists all of the auditable events. The evaluator will check to make sure that every audit event type selected in the ST is included.	
Evaluator Findings	The evaluator examined the guidance document to determine if it lists all auditable events. The section titled "Audit Events" of the AGD was used to determine the verdict of this assurance activity. The evaluator compared the auditable events listed in the ST to the events included in the AGD. Each of the events required by the PP are included in the AGD. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2 FAU_GEN.1.2 Guidance 1

The evaluator will check the administrative guide and ensure that it provides a format for audit records. Each audit record format type must be covered, along with a brief description of each field. The evaluator will ensure that the fields contains the information required.	
Evaluator Findings	The evaluator checked the administrative guide and ensured that it provides a format for audit records. The section titled "Audit Events" of the AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the format of audit events is defined in the AGD, as follows, Timestamp | VAS | User | Event | Event Name | Event Data The evaluator next found that each field in described, as follows, • Timestamp is the time (in seconds) since power was applied to the system, if the TSC frequency was logged. If the TSC frequency was not logged, this is the timestamp counter value. • VAS is the process that logged the event. Some events are logged by a virtual AddressSpace on behalf of another virtual AddressSpace. When this occurs, the User will be changed. • User is the Username or User ID that logged the event. Most of the time this will be the System user, if the event happens automatically without user actions. Sometimes it will be the name of the virtual AddressSpace that the event is being logged on behalf of. The User ID will display if the virtual AddressSpace does not log the name of the user before the event was added. • Event is the number used to signify the Event Name. • Event Name is a short description of the event. • Event Data is a number or text describing what happened. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2 Assurance Activities (Cryptography)

5.2.1 FCS_CKM.1 TSS 1

The evaluator will ensure that the TSS identifies the key sizes supported by the OS. If the ST specifies more than one scheme, the evaluator will examine the TSS to verify that it identifies the usage for each scheme.	
Evaluator Findings	The evaluator examined the TSS to determine if it identifies the key sizes supported by the TOE. The TSS entry for FCS_CKM.1 in the section titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The evaluator found that the TSS states "The TOE implements ECC key generation as specified in FIPS 186-4. ECC curves P-256, P-384, and P-521 are supported." The evaluator examined the TSS and identified the following usage: • The TOE performs Elliptic curve-based key establishment for each trusted channel that uses TLS Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.2 FCS_CKM.1 Guidance 1

The evaluator will verify that the AGD guidance instructs the administrator how to configure the OS to use the selected key generation scheme(s) and key size(s) for all uses defined in this PP.	
Evaluator Findings	The evaluator verified that the AGD guidance instructs the administrator how to configure the OS to use the selected key generation schemes and key sizes. The section titled "Configuring the Cryptographic Engine" of the AGD was used to determine the verdict of this Activity. Upon investigation, the evaluator found that the AGD states, *The TOEs cryptographic engine is pre-configured and cannot be configured by a user or administrator. The only cryptographic engine that was evaluated is the default INTEGRITY Cryptographic Library. No other cryptographic engines were used. It is not possible to configure the TOE to use any other cryptographic engine.* Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.3 FCS_CKM.1 Test 1 (CAVP) [TD0501]

The evaluator will verify the implementation of Key Generation by the OS using the Key Generation test.	
CAVP Algorithm Certificate	C1871
Verdict	Pass

5.2.4 FCS_CKM.2 TSS 1

The evaluator will ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator will examine the TSS to verify that it identifies the usage for each scheme.	
Evaluator Findings	The evaluator examined the TSS to determine if the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. The TSS entries for FCS_CKM.1 and FCS_CKM.2 in the section 6 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity.

	The evaluator compared the key establishment schemes listed in FCS_CKM.2 to the key generation schemes listed in FCS_CKM.1. Upon investigation, the evaluator found that FCS_CKM.2 do not introduce any key generation scheme not included in FCS_CKM.1. The evaluator examined the TSS and verified the usage for the following schemes: • Each TLS channels (administration server) Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.5 FCS_CKM.2 Guidance 1

The evaluator will verify that the AGD guidance instructs the administrator how to configure the OS to use the selected key establishment scheme(s).	
Evaluator Findings	The evaluator verified that the AGD guidance instructs the administrator how to configure the OS to use the selected key establishment schemes. The section titled "Configuring the Cryptographic Engine" of the AGD was used to determine the verdict of this Activity. Upon investigation, the evaluator found that the AGD states, *The TOEs cryptographic engine is pre-configured and cannot be configured by a user or administrator. The only cryptographic engine that was evaluated is the default INTEGRITY Cryptographic Library. No other cryptographic engines were used. It is not possible to configure the TOE to use any other cryptographic engine* Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.6 FCS_CKM.2 Test 1 (CAVP) [TD0501]

The evaluator will verify the implementation of the key establishment schemes supported by the OS using the applicable tests below.	
CAVP Algorithm Certificate	C1871
Verdict	Pass

5.2.7 FCS_CKM_EXT.4 TSS 1

The evaluator examines the TSS 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.	
Evaluator Findings	The evaluator examined the TSS to ensure that it describes how keys are managed in volatile memory, along with details of how each identified key is introduced into volatile memory. The TSS entry for FCS_CKM_EXT.4 in the section titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. For volatile memory, the following keys are managed, as specified in Section 6.1: • The client private key loaded from the MFI entry • The symmetric AES session key • Any asymmetric keys listed by FCS_CKM.2 The TSS entry for FCS_CKM_EXT.4 also includes details of how each key is introduced into volatile memory. All keys or key materials are destroyed upon removal of power to the memory (i.e. upon system shutdown or reboot). Based on these findings, this activity is considered satisfied.

Verdict	Pass

5.2.8 FCS_CKM_EXT.4 TSS 2

The evaluator will check to ensure the TSS lists each type of key that is stored in in non-volatile memory, and identifies how the TOE interacts with the underlying platform to manage keys (e.g., store, retrieve, destroy). The description includes details on the method of how the TOE interacts with the platform, including an identification and description of the interfaces it uses to manage keys (e.g., file system APIs, platform key store APIs).	
Evaluator Findings	The evaluator examined the TSS to ensure that it lists each type of key that is stored in non-volatile memory and whether it identifies how the TOE interacts with the underlying platform to manage the keys. The TSS entry for FCS_CKM_EXT.4 in the Section titled "TOE Summary Specification" was used to determine the verdict of this assurance activity. The evaluator found that the following keys are stored in non-volatile memory: • The client private keys for TLS are stored in on-disk MFI entries. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.9 FCS_CKM_EXT.4 TSS 3

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 will verify that the pattern does not contain any CSPs.	
Evaluator Findings	The evaluator found that the ST does not make use of the open assignment. Based on these findings, this activity is considered satisfied, trivially.
Verdict	Pass

5.2.10 FCS_CKM_EXT.4 TSS 4

The evaluator will check that the TSS identifies any configurations or circumstances that may not strictly conform to the key destruction requirement.	
Evaluator Findings	The TSS does not identify any configurations or circumstances that may not strictly conform to the key destruction requirement. Based on these findings, this activity is considered satisfied, trivially.
Verdict	Pass

5.2.11 FCS_CKM_EXT.4 TSS 5 [TD0365]

If the selection "destruction of all key encrypting keys protecting target key according to FCS_CKM_EXT.4.1, where none of the KEKs protecting the target key are derived" is included the evaluator shall examine the TOE's keychain in the TSS and identify each instance when a key is destroyed by this method. In each instance the evaluator shall verify all keys capable of decrypting the target key are destroyed in accordance with a specified key destruction method in FCS_CKM_EXT.4.1 The evaluator shall verify that all of the keys capable of decrypting the target key are not able to be derived to reestablish the keychain after their destruction.	
Evaluator Findings	The evaluator examine the TOE's keychain in the TSS and identified each instance when a key is destroyed by this method. The FCS_CKM.4 entry in the section titled "TOE Summary Specification" of the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TSS states,

	Each entry is encrypted with a DEK using AES-XTS. Each entry's DEK is stored in the encrypted MFI. A client private key is destroyed upon the destruction of its MFI entry DEK as described previously (making the MFI entry containing the client private key impossible to decrypt). Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.12 FCS_CKM_EXT.4 Guidance 1

There are a variety of concerns that may prevent or delay key destruction in some cases. The evaluator will 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.	
Evaluator Findings	The evaluator examined the guidance document to determine if guidance on situations where key destruction may be delayed at the physical layer and how such situations can be avoided or mitigated if possible. The section titled "Cryptographic Key Destruction and Zeroization" of the AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the AGD describes the following condition, "[t]o ensure that keys are sufficiently decayed to be beyond recovery via even physical recovery attacks, the administrator is advised to wait five (5) minutes after power off before the memory is considered "zeroized"." There are no other conditions which could cause key zeroization to fail. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.13 FCS_CKM_EXT.4 Guidance 2

The evaluator will 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.	
Evaluator Findings	The evaluator checked 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. The section titled "Cryptographic Key Destruction and Zeroization" of the AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the AGD describes the following condition, "[t]o ensure that keys are sufficiently decayed to be beyond recovery via even physical recovery attacks, the administrator is advised to wait five (5) minutes after power off before the memory is considered "zeroized"." There are no other conditions which could cause key zeroization to be delayed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.14 FCS_COP.1(1) – Encryption/Decryption Guidance 1

The evaluator will verify that the AGD documents contains instructions required to configure the OS to use the required modes and key sizes. The evaluator will execute all instructions as specified to configure the OS to the appropriate state. The evaluator will perform all of the following tests for each algorithm implemented by the OS and used to satisfy the requirements of this PP	
Evaluator Findings	The evaluator verified that the AGD guidance instructs the administrator how to configure the OS to use the required modes and key sizes. The section titled "Configuring the Cryptographic

	Engine" of the AGD was used to determine the verdict of this Activity. Upon investigation, the evaluator found that the AGD states, *The TOEs cryptographic engine is pre-configured and cannot be configured by a user or administrator. The only cryptographic engine that was evaluated is the default INTEGRITY Cryptographic Library. No other cryptographic engines were used. It is not possible to configure the TOE to use any other cryptographic engine.* Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.15 FCS_COP.1(1) Test 1 (CAVP)

The evaluator shall verify the implementation of symmetric encryption supported by the TOE.	
CAVP Algorithm Certificate	C1871
Verdict	Pass

5.2.16 FCS_COP.1(2) - Hashing TSS 1

The evaluator will check that the association of the hash function with other application cryptographic functions (for example, the digital signature verification function) is documented in the TSS.	
Evaluator Findings	The evaluator examined the TSS to determine that the association of the hash function with other TSF cryptographic features is documented in the TSS. The TSS entry for FCS_COP.1(2) in the section titled 'TOE Summary Specification' of the ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS describes each of the associated TSF cryptographic functions for which hashing is associated with, as follows: The TSS states: "The TOE uses SHA-256, SHA-384, and SHA-512 for certificate signature checking during TLS. The TOE uses SHA-256 and SHA-384 for message authentication during TLS. The TOE uses SHA-512 to derive the MasterKey from the TPMSalt and the system boot password. The TOE uses SHA-384 in password hashing, and in validation of the update packages." Based on this finding, this assurance activity is considered satisfied.
Verdict	Pass

5.2.17 FCS_COP.1(2) Test 1 (CAVP)

Short Messages Test (Bit oriented Mode) - The evaluator will generate 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 evaluator will 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.	
CAVP Algorithm Certificate	C1871
Verdict	Pass

5.2.18 FCS_COP.1(3) – Signing Test 1 (CAVP)

The evaluator shall verify the implementation of the digital signature algorithms supported by the TOE.	
CAVP Algorithm Certificate	C1871
Verdict	Pass

5.2.19 FCS_COP.1(4) – Keyed-Hash Test 1 (CAVP)

For each of the supported parameter sets, the evaluator will compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator will have the OS generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared against the result of generating HMAC tags with the same key and IV using a known-good implementation.	
CAVP Algorithm Certificate	C1871
Verdict	Pass

5.2.20 FCS_RBG_EXT.1.1 Test 1 (CAVP)

The evaluator will perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator will perform 15 trials for each configuration. The evaluator will also confirm that the operational guidance contains appropriate instructions for configuring the RNG functionality. If the RNG 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 will generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90A). If the RNG 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 will 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.	
CAVP Algorithm Certificate	C1871
Verdict	Pass

5.2.21 FCS_STO_EXT.1.1 TSS 1

The evaluator will check the TSS to ensure that it lists all persistent sensitive data for which the OS provides a storage capability. For each of these items, the evaluator will confirm that the TSS lists for what purpose it can be used, and how it is stored. The evaluator will confirm that cryptographic operations used to protect the data occur as specified in FCS_COP.1(1).

Evaluator Findings	The evaluator examined the TSS to ensure that it lists all persistent sensitive data for which the OS provides a storage capability. The TSS entries for FCS_STO_EXT.1 in the section titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The TSS lists the sensitive data as: • User application private keys • User login information • The administration/update/audit client private key. The TSS describes that all sensitive data "are automatically encrypted with AES-XTS with 256-bit keys. No user intervention is required to protect them." This is consistent with the definition of FCS_COP.1 of the ST. Based on this finding, this assurance activity is considered satisfied.
Verdict	Pass

5.2.22 FCS_STO_EXT.1.1 Guidance 1

The evaluator will also consult the developer documentation to verify that an interface exists for applications to securely store credentials.	
Evaluator Findings	The evaluator examined the guidance document to verify that an interface exists for applications to securely store credentials. The section titled "Sensitive Data Protection" of the AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that encrypted storage happens automatically, and no user intervention is required. Normal user interfaces are used to facilitate secure storage. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.23 FCS_TLSC_EXT.1.1 TSS 1

The evaluator will check the description of the implementation of this protocol in the TSS to ensure that the cipher suites supported are specified. The evaluator will check the TSS to ensure that the cipher suites specified include those listed for this component.	
Evaluator Findings	The evaluator examined the TSS to ensure that the ciphersuites supported are specified. The TSS entry for FCS_TLSC_EXT.1 in the section titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The evaluator first examined the TSS of ST to identify the ciphersuites supported by the TOE for TLS client connections. The following ciphersuites are identified as supported within the TSS: • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 Next, the evaluator examined the definition of FCS_TLSC_EXT.1 in ST. The evaluator found that the ciphersuites for TLS client connection specified in the definition of the SFR are consistent with the description within the TSS of ST. Based on this finding, this assurance activity is considered satisfied.
Verdict	Pass

5.2.24 FCS_TLSC_EXT.1.1 Guidance 1

The evaluator will also check the operational guidance to ensure that it contains instructions on configuring the OS so that TLS conforms to the description in the TSS.

Evaluator Findings	The evaluator verified that the AGD guidance instructs the administrator how to configure the OS so that TLS conforms to the description in the TSS. The section titled "Configuring the Cryptographic Engine" of the AGD was used to determine the verdict of this Activity. Upon investigation, the evaluator found that the AGD states, *The TOEs cryptographic engine is pre-configured and cannot be configured by a user or administrator. The only cryptographic engine that was evaluated is the default INTEGRITY Cryptographic Library. No other cryptographic engines were used. It is not possible to configure the TOE to use any other cryptographic engine.* Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.25 FCS_TLSC_EXT.1.2 TSS 1

The evaluator will ensure that the TSS describes the client's method of establishing all reference identifiers from the application-configured reference identifier, including which types of reference identifiers are supported (e.g. Common Name, DNS Name, URI Name, Service Name, or other application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported. The evaluator will ensure that this description identifies whether and the manner in which certificate pinning is supported or used by the OS.	
Evaluator Findings	The evaluator checked the TSS to determine if it describes the client's method of establishing reference identifiers. The TSS entry for FCS_TLSC_EXT.1 in the section titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The evaluator found that the TOE allows administrators to configure the TLS client's expected reference identifier by setting the FQDN of the destination server. For example, "audit.example.com". The TOE supports only DNS name / SAN-DNS, CommonName, and FQDN. IP addresses are not supported. Additionally, the TSS states that: • The TOE does not support certificate pinning. • Wildcards may only be used in the leftmost label of a domain name Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.26 FCS_TLSC_EXT.1.2 Guidance 1

The evaluator will verify that the AGD guidance includes instructions for setting the reference identifier to be used for the purposes of certificate validation in TLS.	
Evaluator Findings	The evaluator verified that the AGD guidance includes instructions for setting the reference identifier to be used for the purposes of certificate validation in TLS. The section titled, "Transport Layer Security (TLS)" of the AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found that the AGD states, "[t]he TOE administrator configures the reference identifier for certificate validation by assigning the DN of the destination server(s), which is compared to the DN in the certificate received. This configuration, and choosing which local certificate to use, are performed in the configuration file update downloaded by the TOE from the Administration Server." Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.27 FCS_TLSC_EXT.2.1 TSS 1

The evaluator will verify that the TSS describes support for the Supported Groups Extension and whether the required behavior is performed by default or may be configured.	
Evaluator Findings	The evaluator verified that the TSS describes support for the Supported Groups Extension and whether the required behavior is performed by default or may be configured. The section of the ST titled "TOE Summary Specification" was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TSS states, "[t]he TOE supports the secp384r1 group extension. This is by default no configuration is available." Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.28 FCS_TLSC_EXT.2.1 Guidance 1

If the TSS indicates that support for the Supported Groups Extension must be configured to meet the requirement, the evaluator will verify that AGD guidance includes configuration instructions for the Supported Groups Extension.	
Evaluator Findings	The evaluator examined the guidance document to verify that AGD guidance includes configuration of the supported Elliptic Curves Extension. The section titled "Transport Layer Security (TLS)" of the AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the AGD states, that the TOE "only supports the Supported Groups Extension containing the group secp384r1. This behavior is performed by default. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.29 FCS_TLSC_EXT.4 TSS 1

The evaluator will ensure that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication.	
Evaluator Findings	The evaluator verified that the TSS describes support for mutual authentication. The section of the ST titled "TOE Summary Specification" was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TSS states that the TOE "presents its client certificate associated with the connection to the remote server." Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.2.30 FCS_TLSC_EXT.4 Guidance 1

The evaluator will verify that the AGD guidance required per FIA_X509_EXT.2.1 includes instructions for configuring the client-side certificates for TLS mutual authentication.	
Evaluator Findings	The evaluator examined the guidance document to verify that AGD guidance includes This configuration, and choosing which local certificate to use, are performed in the configuration file update downloaded by the TOE from the Administration Server. The section titled "Transport Layer Security (TLS)" of the AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the AGD states that "[t]his configuration, and choosing which local certificate to use, are performed in the configuration file update downloaded by the TOE from the Administration Server." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3 Assurance Activities (User Data Protection)

5.3.1 FDP_ACF_EXT.1.1 TSS 1

The evaluator will confirm that the TSS comprehensively describes the access control policy enforced by the OS. The description must include the rules by which accesses to particular files and directories are determined for particular users. The evaluator will inspect the TSS to ensure that it describes the access control rules in such detail that given any possible scenario between a user and a file governed by the OS the access control decision is unambiguous.	

Evaluator Findings	The evaluator examined the TSS to ensure that it describes the access control policy enforced by the OS and whether the description includes the rules by which accesses to files and directories are determined for particular users. The TSS entry for FDP_ACF_EXT.1 in the section titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The TSS states the following
	• Root:
	  ○ The TOE contains a root directory owned only by the root user.
	  ○ The root directory also contains a special "sys" directory containing system files and is owned by the "root" user
	  ○ The "root" user may list, create, delete, read, and write any file regardless of ownership
	• Users:
	  ○ The TOE contains "home" directories for each user and users are limited to their own directory for viewing, modifying, creating or deleting anything within the "home" directories.
	Based on these findings, this activity is considered satisfied.

Verdict	Pass

5.3.2 FDP_IFC_EXT.1.1 TSS 1

The evaluator will verify that the TSS section of the ST describes the routing of IP traffic when a VPN client is enabled. The evaluator will ensure that the description indicates which traffic does not go through the VPN and which traffic does, and that a configuration exists for each in which only the traffic identified by the ST author as necessary for establishing the VPN connection (IKE traffic and perhaps HTTPS or DNS traffic) is not encapsulated by the VPN protocol (IPsec).	
Evaluator Findings	The evaluator examined the TSS to ensure that it describes the routing of IP traffic when a VPN client is enabled. The TSS entry for FDP_IFC_EXT.1 in the section titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The TSS states that "[w]hen the VPN client is enabled, the client will configure the rules under which traffic is handled (i.e., to or from certain addresses, or of a certain traffic type, or all traffic, etc.)." Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.4 Assurance Activities (Identification and Authentication)

5.4.1 FIA_UAU.5.2 TSS 1

The evaluator will ensure that the TSS describes each mechanism provided to support user authentication and the rules describing how the authentication mechanism(s) provide authentication.	
Evaluator Findings	The evaluator examined the TSS to ensure that it describes each mechanism provided to support user authentication and the rules describing how the authentication mechanism(s) provide

	authentication. The TSS entry for FIA_UAU.5 in the section titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The TSS states that, On system boot, the bootloader prompts the user for this password. Without the correct boot password booting of the TOE cannot proceed…After fully booting the TOE, the user may login to the system shell with their username and password. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.4.2 FIA_UAU.5.2 Guidance 1

The evaluator will verify that configuration guidance for each authentication mechanism is addressed in the AGD guidance.	
Evaluator Findings	The evaluator verified that configuration guidance for each authentication mechanism is addressed in the AGD guidance. The sections titled "The Special Operations Tab" and "User Passwords" were used to determine the verdict of this activity. Upon investigation, the evaluator found that the AGD describes the configuration of password-based authentication for the TOE. This is consistent with the authentication mechanisms described in the ST. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.4.3 FIA_X509_EXT.1.1 TSS 1 [TD0525]

The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place. The evaluator ensures the TSS also provides a description of the certificate path validation algorithm.	
Evaluator Findings	The evaluator examined the TSS to determine where certificate validation occurs and that the TSS also provides a description of the certificate path validation algorithm. The TSS entry for FIA_X509_EXT.1 in the section titled "TOE Summary Specification" states, "TLS X.509 certificates are validated according to the algorithm specified in RFC 5280 Section 6 et seq. The certificates of the Trust Anchor Database are chosen by the administrator during provisioning or automatic update of the TOE. Verification (including revocation checking) of a certificate occurs when the certificate is first loaded into the TOE, when the certificate is loaded for first-use, and when a peer certificate is presented during an authentication step. Certificate revocation checking of a server certificate (including it's complete CA chain) is done via either the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, or the checking of Certificate Revocation Lists (CRL) as specified in RFC 5759. This occurs immediately after receipt of the server certificate and before key exchange." Additionally, the TSS states, "the implementation is configured to reject any peer certificates that meet any of the following conditions: • Any CA certificate in the certificate path is missing the basicConstraints extension or does not have the CA flag set to TRUE in this extension. • A server certificate does not have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field. • A certificate used to sign an OCSP response does not have the OCSP Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field. • A certificate used to sign a CRL does not have the CRL-signing bit set." Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.5 Assurance Activities (Security Management)

5.5.1 FMT_MOF_EXT.1 TSS 1

The evaluator will verify that the TSS describes those management functions that are restricted to Administrators, including how the user is prevented from performing those functions, or not able to use any interfaces that allow access to that function.	
Evaluator Findings	The evaluator examined the TSS to ensure that it describes that the management functions that are restricted to Administrators, including how the user is prevented from performing those functions, or not able to use any interfaces that allow access to that function. The TSS entry for FMT_MOF_EXT.1 & FMT_SMF_EXT.1 in the section titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The TSS states that, The TOE restricts all "Administrator" management activities listed below • Set the session inactivity timeout (in minutes). Setting the timeout value to zero disables the session inactivity timeout. • Set the address of the administration server from which to receive software updates and management settings from. • Enable/disable automatic software updates. • Create a new user account and set its initial password. • Delete a user account. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.5.2 FMT_SMF_EXT.1.1 Guidance 1

The evaluator will verify that every management function captured in the ST is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.	
Evaluator Findings	The evaluator verified that the guidance documentation provides information required to perform the management duties associated with the management function. The sections titled, "The Configuration Tab," "Updating the Client," "Configuring Automatic Updates," and "User Passwords." Upon investigation, the evaluator found that the AGD describes each of the management functionality claimed in the ST. Based on these findings, the activities are considered satisfied.
Verdict	Pass

5.6 Assurance Activities *(Protection of the TSF)*

5.6.1 FPT_ACF_EXT.1.1 TSS 1

The evaluator will confirm that the TSS specifies the locations of kernel drivers/modules, security audit logs, shared libraries, system executables, and system configuration files. Every file does not need to be individually identified, but the system's conventions for storing and protecting such files must be specified.	
Evaluator Findings	The evaluator examined the TSS to ensure that it identifies the locations of kernel drivers/modules, security audit logs, shared libraries, system executables, and system configuration files. Every file does not need to be individually identified, but the system's conventions for storing and protecting such files must be specified. The TSS entry for FPT_ACF_EXT.1 in the section 6.1.7 states that:

	All Kernel modules, all audit logs, all applications and system configuration files are stored in various directories that are not accessible to non-administrative users. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.2 FPT_SBOP_EXT.1.1 TSS 1

For stack-based OSes, the evaluator will determine that the TSS contains a description of stack-based buffer overflow protections used by the OS. These are referred to by a variety of terms, such as stack cookie, stack guard, and stack canaries. The TSS must include a rationale for any binaries that are not protected in this manner.	
Evaluator Findings	The evaluator examined the TSS to ensure that it contains a description of stack-based buffer overflow protections used by the OS. These are referred to by a variety of terms, such as stack cookie, stack guard, and stack canaries. The TSS entry for FPT_SBOP_EXT.1 in the section titled "TOE Summary Specification" states: "INTEGRITY Applications on the TOE use "stack guards" for stack-based buffer overflow protection. On system boot, a random 64-bit guard value is generated using the RDRAND platform-based noise source. On function entrance, the callee pushes the guard value onto the stack. Right before exit from the function, the callee pops the guard value from the stack and compares it to its initial value. If it has changed, a buffer overflow is detected, and the application self-terminates." There are no binaries that are not subject to the protection. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.3 FPT_TST_EXT.1.1 TSS 1

The evaluator will verify that the TSS section of the ST includes a comprehensive description of the boot procedures, including a description of the entire bootchain, for the TSF. The evaluator will ensure that the OS cryptographically verifies each piece of software it loads in the bootchain to include bootloaders and the kernel. Software loaded for execution directly by the platform (e.g. first-stage bootloaders) is out of scope. For each additional category of executable code verified before execution, the evaluator will verify that the description in the TSS describes how that software is cryptographically verified.	
Evaluator Findings	The evaluator examined the TSS to ensure that it contains description of the boot procedures, including a description of the entire bootchain, for the TSF. The TSS entry for FPT_TST_EXT.1 in the section titled "TOE Summary Specification" states: "After power on, the hardware platform firmware loads the digitally signed SWIC bootloader. The digital signature of the signed bootloader is verified using ECDSA over NIST curve P-384. The SWIC bootloader then attempts to obtain the 256-bit TPMSalt from the hardware system environment's TPM 2.0 module. This will only be successful if the TPM's PCRs (Platform Configuration Registers) have the correct values. The bootloader then prompts the user for the "system boot password." The bootloader generates the 512-bit MasterKey (consisting of the 256-bit MfiKey and 256-bit OpalKey) by combining the TPMSalt and boot password using PBKDF2-HMAC-SHA512. The bootloader then uses the MfiKey to decrypt the on-disk AES-GCM-256 encrypted MFI (Master File Index). The bootloader checks the integrity of the decrypted MFI by validating its GCM value. The entire INTEGRITY Enterprise OS including the kernel is stored as an on-disk AES-XTS encrypted MFI entry. The bootloader decrypts the INTEGRITY Enterprise OS using its 256-bit DEK stored in the MFI. The bootloader checks the integrity of the decrypted INTEGRITY Enterprise OS by computing its SHA-384 hash and comparing this value to the hash stored in the

	MFI. After confirmation of the integrity of the INTEGRITY Enterprise OS, the bootloader loads the INTEGRITY Enterprise OS's INTEGRITY Separation Kernel." Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.4 FPT_TST_EXT.1.1 TSS 2

The evaluator will verify that the TSS contains a description of the protection afforded to the mechanism performing the cryptographic verification.	
Evaluator Findings	The evaluator examined the TSS to ensure that it contains description of the boot procedures, including a description of the entire bootchain, for the TSF. The evaluator will ensure that the OS cryptographically verifies each piece of software it loads in the bootchain to include bootloaders and the kernel. Software loaded for execution directly by the platform (e.g. first-stage bootloaders) is out of scope. For each additional category of executable code verified before execution, the evaluator will verify that the description in the TSS describes how that software is cryptographically verified. The TSS entry for FPT_TST_EXT.1 in the section titled "TOE Summary Specification" states: "The bootloader checks the integrity of the decrypted MFI by validating its GCM value. The entire INTEGRITY Enterprise OS including kernel is stored as an on-disk AES-XTS encrypted MFI entry. The bootloader decrypts the INTEGRITY Enterprise OS using its 256-bit DEK stored in the MFI. The bootloader checks the integrity of the decrypted INTEGRITY Enterprise OS by computing its SHA-384 hash and comparing this value to the hash stored in the MFI. After confirmation of the integrity of the SWIC OS, the bootloader loads the INTEGRITY Enterprise OS' INTEGRITY Separation Kernel." Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.5 FPT_TUD_EXT.1.2 TSS 1

All supported origins for the update must be indicated in the TSS.	
Evaluator Findings	The evaluator examined the TSS to determine the supported origins for updates. The FPT_TUD_EXT.1 entry in TSS under the section titled "TOE Summary Specification" states that, "[a]fter establishing the trusted channel to an authorized administration server, the TOE requests a system update from the server over this channel". Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.6.6 FPT_TUD_EXT.2.2 TSS 1

All origins supported by the OS must be indicated in the TSS. However, this only includes those mechanisms for which the OS is providing a trusted installation and update functionality. It does not include user or administrator-driven download and installation of arbitrary files.	
Evaluator Findings	The evaluator examined the TSS to determine the supported origins for updates. The FPT_TUD_EXT.1 entry in TSS under the section titled "TOE Summary Specification" states that, "[a]fter establishing the trusted channel to an authorized administration server, the TOE requests a system update from the server over this channel". Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.7 Assurance Activities *(Trusted Path/Channels)*

5.7.1 FTP_TRP.1 TSS 1

The evaluator will examine the TSS to determine that the methods of remote OS administration are indicated, along with how those communications are protected. The evaluator will also confirm that all protocols listed in the TSS in support of OS administration are consistent with those specified in the requirement, and are included in the requirements in the ST.	
Evaluator Findings	The evaluator examined the TSS to determine that the methods of remote OS administration are indicated, along with how those communications are protected and also confirm that all protocols listed in the TSS in support of OS administration are consistent with those specified in the requirement, and are included in the requirements in the ST. The FTP_TRP.1 entry in TSS under the section titled "TOE Summary Specification" states that "[a]n authorized administrator may perform remote administrative actions of the TOE via the automatic update trusted path." It also states that the TOE uses TOE-initiated TLS in support of remote administration. This is consistent with the definition of the requirement in the ST. Based on these findings, this activity is considered satisfied.
Verdict	Pass

5.7.2 FTP_TRP.1 Guidance 1

The evaluator will confirm that the operational guidance contains instructions for establishing the remote administrative sessions for each supported method.	
Evaluator Findings	The evaluator examined the guidance document to includes instructions for establishing remote administrative sessions. The section titled, "Remote Management Operations" of AGD was used to determine the verdict of this activity. Upon investigation, the evaluator found that the AGD describes the configuration and options necessary to facilitate remote administration via the Admin/Management Server. Based on these findings, this activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1 Assurance Activities *(Testing)*

6.1.1 FAU_GEN.1.1 Test#1

Item	Data
Test Assurance Activity	The evaluator will test the OS's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the ST. This should include all instance types of an event specified. When verifying the test results, the evaluator will ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record have the proper entries.
Test Steps	• Obtain an audit record that fulfills all auditable events and additional audit record contents for all individual SFR requirements
Expected Test Results	• A table will be generated containing screenshots of all auditable events generated by the TOE
Pass/Fail with Explanation	Pass. The TOE generates the appropriate audit logs that match the format specified in the administrative guide and the fields in each audit record provide the required information. This meets the testing requirements.

6.1.2 FAU_GEN.1.2 Test#1

Item	Data
Test Assurance Activity	The evaluator shall test the OS's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the ST. The evaluator will ensure the audit records generated during testing match the format specified in the administrative guide, and that the fields in each audit record provide the required information.
Pass/Fail with Explanation	Pass. This test is satisfied in conjunction with FAU_GEN.1.1 Test #1. The TOE generates the appropriate audit logs that match the format specified in the administrative guide and the fields in each audit record provide the required information.

6.1.3 FCS_CKM_EXT.4 Test #1 [TD0365]

Item	Data
Test Assurance Activity	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 will: 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.

Pass/Fail with Explanation	Pass. The ST selects destruction executed by a removal of power to memory. This activity is met trivially.

6.1.4 FCS_CKM_EXT.4 Test #2 [TD0365]

Item	Data
Test Assurance Activity	Test 2: Applied to each key help in non-volatile memory and subject to destruction by the TOE. The evaluator will 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 Steps	• Identify the purpose of the key and what access should fail when it is deleted
	  ○ Key is used for TLS connections
	• Establish TLS connection to demonstrate the key usage
	• Clear the key
	  ○ This is done by factory resetting the TOE
	• Attempt functionality that requires the key
	  ○ A TLS connection is not possible

Expected Output	• The product can make a TLS connection • The key is zeroized • The product cannot make a TLS connection
Pass/Fail with Explanation	Pass. The evaluator is able to clear persistent keys on the TOE. After clearing, the associated services are not available. This meets the testing requirements.

6.1.5 FCS_CKM_EXT.4 Test #3 [TD0365]

Item	Data
Test Assurance Activity	**Tests 3 and 4** do not apply for the selection **instructing the underlying platform to destroy the representation of the key**, as the TOE has no visibility into the inner workings and completely relies on the underlying platform. Test 3: The following tests are used to determine the TOE is able to request the platform to overwrite the key with a TOE supplied pattern. Applied to each key held in non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator will use a tool that provides a logical view of the media (e.g., MBR file system): 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 logical view that 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 Steps	• Record the value of the key ○ This requires that private key being decrypted • Perform a TLS connection • Zeroize the key on the TOE

	• Verify the key value is now filled with zeros
Expected Test Results	• After the zeroization operation is performed the key is overwritten with zeros
Pass/Fail with Explanation	Pass. After the zeroization operation, the key value is overwritten by zeros. This meets the testing requirements.

6.1.6 FCS_CKM_EXT.4 Test #4 [TD0365]

Item	Data
Test Assurance Activity	**Tests 3 and 4** do not apply for the selection **instructing the underlying platform to destroy the representation of the key**, as the TOE has no visibility into the inner workings and completely relies on the underlying platform. Test 4: Applied to each key held as non-volatile memory and subject to destruction by overwrite by the TOE. The evaluator will use a tool that provides a logical view of the media: 1. Record the logical 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. Read the logical 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.
Test Steps	• Record the logical location of the key • Perform a TLS connection using the key • Perform a factory reset • Overwrite the value of the key with a new key • Verify the new value
Expected Test Results	• After the zeroization operation is performed the key is overwritten with zeros • The value is replaced with the new key value • The old key does not exist any longer
Pass/Fail with Explanation	Pass. When a key is overwritten with a new key value, the previous key ceases to exist. This meets the testing requirements.

6.1.7 FCS_TLSC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	**Test 1:** The evaluator will establish a TLS connection using each of the cipher suites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an EAP session. It is sufficient to observe the successful negotiation of a cipher suite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the cipher suite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Steps	For each cipher suite selected: • Start a TLS server that is offering only that cipher suite • Attempt to connect to the TLS server from the TOE • Verify that the connection succeeds

Expected Test Results	• The TOE can connect to the TLS server with each of the cipher suites selected in the ST.
Pass/Fail with Explanation	Pass. The TOE is able to connect with both claimed ciphersuites (TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384). This meets the testing requirements.

6.1.8 FCS_TLSC_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	**Test 2:** The evaluator will attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
Test Steps	• Start a TLS server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field • Attempt to connect to the TLS server from the TOE • Verify that a connection is established • Start a TLS server with a server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field • Attempt to connect to the TLS server from the TOE • Verify that the connection is not established
Expected Test Results	• The TOE should connect to a TLS server that is using a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field. • The TOE should not connect to a server that is using a server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field.
Pass/Fail with Explanation	Pass. The TOE properly allowed a connection to a TLS server using a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and denied a connection to a TLS server with a server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field. This meets the testing requirements.

6.1.9 FCS_TLSC_EXT.1.1 Test #3

Item	Data
Test Assurance Activity	**Test 3:** The evaluator will send a server certificate in the TLS connection that does not match the server-selected cipher suite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite or send a RSA certificate while using one of the ECDSA cipher suites.) The evaluator will verify that the OS disconnects after receiving the server's Certificate handshake message.
Test Steps	• Start the acumen-tlsc tool to starts a TLS server that will use cipher suite that does not match the server certificate type • Attempt to connect to the TLS server from the TOE • Verify that the connection fails
Expected Test Results	• The TOE should reject the connection.
Pass/Fail with Explanation	Pass. The TOE rejected the connection when the cipher suite that does not match the server certificate type. This meets the testing requirements.

6.1.10 FCS_TLSC_EXT.1.1 Test #4

Item	Data
Test Assurance Activity	**Test 4:** The evaluator will configure the server to select the TLS_NULL_WITH_NULL_NULL cipher suite and verify that the client denies the connection.
Test Steps	• Start a TLS server with the acumen-tlsc tool that will present the TLS_NULL_WITH_NULL_NULL cipher suite • Attempt to connect to the TLS server from the TOE • Verify that the TOE denies the connection
Expected Test Results	• The TOE should deny the connection with the TLS server.
Pass/Fail with Explanation	Pass. The TOE denies a connection to a TLS server that offered the TLS_NULL_WITH_NULL_NULL cipher suite. This meets the testing requirements.

6.1.11 FCS_TLSC_EXT.1.1 Test #5.1

Item	Data
Test Assurance Activity	**Test 5:** The evaluator will perform the following modifications to the traffic: • Change the TLS version selected by the server in the Server Hello to a non-supported TLS version (for example 1.3 represented by the two bytes 03 04) and verify that the client rejects the connection.
Test Steps	• Attempt a connection to a remote TLS server that uses a non-supported TLS version in the Server Hello • Show the TOE rejects the connection
Expected Test Results	• The TOE rejects a connection with the external TLS server when presented a non-supported TLS version
Pass/Fail with Explanation	Pass. The TOE rejected a connection with the external TLS server when presented a TLS version that is not supported. This meets the testing requirements.

6.1.12 FCS_TLSC_EXT.1.1 Test #5.2

Item	Data
Test Assurance Activity	**Test 5:** The evaluator will perform the following modifications to the traffic: • Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE cipher suite) or that the server denies the client's Finished handshake message.
Test Steps	• Modify at least one byte in the server's nonce in the Server Hello handshake message, and verify that the client rejects the Server Key Exchange handshake message • Show the connection fails
Expected Test Results	• The TOE rejects a connection to a TLS server when the server’s nonce is modified.
Pass/Fail with Explanation	Pass. The TOE rejects a connection to a TLS server when the server’s nonce is modified. This meets the testing requirements.

6.1.13 FCS_TLSC_EXT.1.1 Test #5.3

Item	Data
Test Assurance Activity	**Test 5:** The evaluator will perform the following modifications to the traffic: • **Test 5.3:** Modify the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake

	message. The evaluator will verify that the client rejects the connection after receiving the Server Hello.
Test Steps	• Start the acumen-tlsc tool to create a TLS server that will modify the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message • Attempt to connect to the TLS server from the TOE • Verify that the TOE rejects the connection
Expected Test Results	• The TOE should reject a connection to a TLS server when the server's selected cipher suite in the Server Hello handshake message is a cipher suite not presented in the Client Hello handshake message.
Pass/Fail with Explanation	Pass. The TOE rejected a connection to a TLS server that modified the server's selected cipher suite in the Server Hello handshake message to be a cipher suite not presented in the Client Hello handshake message. This meets the testing requirements.

6.1.14 FCS_TLSC_EXT.1.1 Test #5.4

Item	Data
Test Assurance Activity	**Test 5:** The evaluator will perform the following modifications to the traffic: • **Test 5.4:** If an ECDHE or DHE ciphersuite is selected, modify the signature block in the Server's Key Exchange handshake message, and verify that the client rejects the connection after receiving the Server Key Exchange message.
Test Steps	• Start the acumen-tlsc tool to start a TLS server that will modify the signature block in the Server's Key Exchange handshake message • Attempt to connect to the TLS server from the TOE • Verify that the connection is rejected by the TOE
Expected Test Results	• The TOE should reject a connection to the TLS server that will modify the signature block in the Server's Key Exchange handshake message.
Pass/Fail with Explanation	Pass. The TOE rejected a connection to a TLS server that modified the signature block in the Server's Key Exchange handshake message. This meets the testing requirements.

6.1.15 FCS_TLSC_EXT.1.1 Test #5.5

Item	Data
Test Assurance Activity	**Test 5:** The evaluator will perform the following modifications to the traffic: • **Test 5.5:** Modify a byte in the Server Finished handshake message, and verify that the client sends a fatal alert upon receipt and does not send any application data.
Test Steps	• Start the acumen-tlsc tool to create a TLS server that will modify a byte in the Server Finished handshake message • Attempt to connect to the TLS server from the TOE • Verify that the TOE rejects the connection
Expected Test Results	• The TOE should reject a connection to a TLS server that has modified a byte in the Server Finished handshake message.
Pass/Fail with Explanation	Pass. The TOE rejected a connection to a TLS server that has modified a byte in the Server Finished handshake message. This meets the testing requirement.

6.1.16 FCS_TLSC_EXT.1.1 Test #5.6

Item	Data
Test Assurance Activity	**Test 5:** The evaluator will perform the following modifications to the traffic:

	• **Test 5.6:** Send a garbled message from the Server after the Server has issued the Change Cipher Spec message and verify that the client denies the connection.
Test Steps	• Start the acumen-tlsc tool to create a TLS server that will send a garbled message from the Server after the Server has issued the Change Cipher Spec message • Attempt to connect to the TLS server from the TOE • Verify that the TOE rejects the connection
Expected Test Results	• The TOE should reject a connection to a TLS server that send garbled message after the Server has issued the Change Cipher Spec message.
Pass/Fail with Explanation	Pass. The TOE rejects a connection to a TLS server that sends a garbled message after the Server has issued the Change Cipher Spec message. This meets the testing requirement.

6.1.17 FCS_TLSC_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator will configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: • **Test 1:** The evaluator will present a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier. The evaluator will verify that the connection fails.
Test Steps	• Start a TLS server that has a server certificate that does not contain an identifier in either the Subject Alternative Name (SAN) or Common Name (CN) that matches the reference identifier • Attempt to connect to the TLS server from the TOE • Verify that the connection fails
Expected Test Results	• The connection should fail.
Pass/Fail with Explanation	Pass. The TOE did not connect to a TLS server using a server certificate that has a CN and SAN that do not match the reference identifier. This meets the testing requirements.

6.1.18 FCS_TLSC_EXT.1.2 Test #2

Item	Data
Test Assurance Activity	The evaluator will configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: • **Test 2:** The evaluator will present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator will repeat this test for each supported SAN type.
Test Steps	• Start a TLS server that is using a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier • Attempt to connect to the TLS server from the TOE • Verify that the connection fails
Expected Test Results	• The connection should fail.
Pass/Fail with Explanation	Pass. The TOE did not connect to a TLS server that is using a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but

	does not contain an identifier in the SAN that matches the reference identifier. This meets the testing requirements.

6.1.19 FCS_TLSC_EXT.1.2 Test #3

Item	Data
Test Assurance Activity	The evaluator will configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: • **Test 3:** [conditional] If the TOE does not mandate the presence of the SAN extension, the evaluator will present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator will verify that the connection succeeds. If the TOE mandates the presence of the SAN extension, this test shall be omitted.
Test Steps	• Start a TLS server with a server certificate that has a CN that matches the reference identifier and no SAN • Attempt to connect to the TLS server from the TOE • Verify that the connection succeeds
Expected Test Results	• The connection should succeed.
Pass/Fail with Explanation	Pass. The TOE connected to a TLS server that used a server certificate that had a CN that matches the reference identifier and a missing SAN. This meets the testing requirements.

6.1.20 FCS_TLSC_EXT.1.2 Test #4

Item	Data
Test Assurance Activity	The evaluator will configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: • **Test 4:** The evaluator will present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator will verify that the connection succeeds.
Test Steps	• Start a TLS server that has a server certificate containing a CN that does not match the reference identifier but a SAN that does • Attempt to connect to the TLS server from the TOE • Verify that the connection succeeds
Expected Test Results	• The connection should succeed.
Pass/Fail with Explanation	Pass. The TOE connected to a TLS server that used a server certificate that had a CN that does not match the reference identifier and a SAN that does. This meets the testing requirements.

6.1.21 FCS_TLSC_EXT.1.2 Test #5.1

Item	Data
Test Assurance Activity	The evaluator will configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: • **Test 5:** The evaluator will perform the following wildcard tests with each supported type of reference identifier: ○ **Test 5.1:** The evaluator will present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails.
Test Steps	• Attempt a connection to a remote TLS server using a wildcard not in the left-most label

	• Show the TOE rejects the connection
Expected Test Results	• The TOE rejects a TLS connection with a TLS server with a certificate using a wildcard not in the left-most label
Pass/Fail with Explanation	Pass. The TOE rejected the connection to the TLS server with a certificate containing a wildcard that is not in the left-most label of the presented identifier. This meets the testing requirements.

6.1.22 FCS_TLSC_EXT.1.2 Test #5.2

Item	Data
Test Assurance Activity	The evaluator will configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: • **Test 5:** The evaluator will perform the following wildcard tests with each supported type of reference identifier: ○ **Test 5.2:** The evaluator will present a server certificate containing a wildcard in the left-most label but not preceding the public suffix (e.g. *.example.com). The evaluator will configure the reference identifier with a single left-most label (e.g. foo.example.com) and verify that the connection succeeds. The evaluator will configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails. The evaluator will configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails.
Test Steps	• Attempt a connection to a remote TLS server using a certificate with a wildcard in the left-most label with the reference identifier set to a single left-most label: CN=*.admin.com • Show the connection succeeds • Change the reference identifier to not have any leftmost label and attempt to connect to the same TLS server: CN=admin.com • Show the connection fails • Change the reference identifier to have 2 leftmost labels and attempt to connect to the same TLS server: CN=foo.test.admin.com • Show the connection fails
Expected Test Results	• The TOE is able to connect to a remote TLS server using a certificate with a wildcard in the left-most label with the reference identifier set to a single left-most label • The TOE rejects a connection to a remote TLS server using a certificate that does not have any leftmost label • The TOE rejects a connection to a remote TLS server using a certificate that does has 2 leftmost labels
Pass/Fail with Explanation	Pass. The TOE can connect to a remote TLS server using a certificate with a wildcard in the left-most label with the reference identifier set to a single left-most label. The TOE rejects a connection to a remote TLS server using a certificate that does not have any leftmost label. The TOE rejects a connection to a remote TLS server using a certificate that does has 2 leftmost labels. This meets the testing requirements.

6.1.23 FCS_TLSC_EXT.1.2 Test #5.3

Item	Data
Test Assurance Activity	The evaluator will configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection:

	• **Test 5:** The evaluator will perform the following wildcard tests with each supported type of reference identifier: ○ **Test 5.3:** The evaluator will present a server certificate containing a wildcard in the left-most label immediately preceding the public suffix (e.g. *.com). The evaluator will configure the reference identifier with a single left-most label (e.g. foo.com) and verify that the connection fails. The evaluator will configure the reference identifier with two left-most labels (e.g. bar.foo.com) and verify that the connection fails.
Test Steps	• Attempt a connection to a remote TLS server using a certificate with a wildcard preceding the public suffix and with the reference identifier set to a single left-most label: CN=*.com • Show the connection fails • Change the reference identifier with a single left-most label (e.g. foo.com) and attempt to connect to the same TLS server: CN=admin.com • Show the connection fails • Change the reference identifier to not have 2 leftmost labels and attempt to connect to the same TLS server: CN=foo.bar.com • Show the connection fails
Expected Test Results	• The TOE rejects a connection to a remote TLS using a certificate with a wildcard preceding the public suffix and with the reference identifier set to a single left-most label • The TOE rejects a connection to a remote TLS using a certificate with a single left-most label (e.g. foo.com) • The TOE rejects a connection to a remote TLS using a certificate that does not have 2 leftmost labels
Pass/Fail with Explanation	Pass. The TOE rejects a connection to a remote TLS using a certificate with a wildcard preceding the public suffix and with the reference identifier set to a single left-most label. The TOE rejects a connection to a remote TLS using a certificate with a single left-most label (e.g. foo.com). The TOE rejects a connection to a remote TLS using a certificate that does not have 2 leftmost labels. This meets the testing requirements.

6.1.24 FCS_TLSC_EXT.1.2 Test #6

Item	Data
Test Assurance Activity	The evaluator will configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: • **Test 6:** [conditional] If URI or Service name reference identifiers are supported, the evaluator will configure the DNS name and the service identifier. The evaluator will present a server certificate containing the correct DNS name and service identifier in the URIName or SRVName fields of the SAN and verify that the connection succeeds. The evaluator will repeat this test with the wrong service identifier (but correct DNS name) and verify that the connection fails.
Pass/Fail with Explanation	Pass. The TOE does not support URI or Service name reference identifiers. This activity is met trivially.

6.1.25 FCS_TLSC_EXT.1.2 Test #7

Item	Data
Test Assurance Activity	The evaluator will configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection:

	• **Test 7:** [conditional] If pinned certificates are supported the evaluator will present a certificate that does not match the pinned certificate and verify that the connection fails.
Pass/Fail with Explanation	Pass. The TOE does not support pinned certificates. This activity is met trivially.

6.1.26 FCS_TLSC_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	The evaluator will use TLS as a function to verify that the validation rules in FIA_X509_EXT.1.1 are adhered to and shall perform the following additional test: • Test 1: The evaluator will demonstrate that a peer using a certificate without a valid certification path results in an authenticate failure. Using the administrative guidance, the evaluator will then load the trusted CA certificate(s) needed to validate the peer's certificate, and demonstrate that the connection succeeds. The evaluator then shall delete one of the CA certificates, and show that the connection fails.
Test Steps	• Attempt to connect to a TLS server without a full certificate chain • Verify the connection fail • Load the missing certificates • Attempt to connect to a TLS server with a full certificate chain • Verify the connection succeeds • Remove certificates from the certificate chain • Verify the connection fail
Expected Test Results	• When a full certificate chain is present, the TOE will connect to a TLS server. • When a full chain is not present, the TOE will not connect to a TLS server.
Pass/Fail with Explanation	Pass. When a full certificate chain is present, the TOE will connect to a TLS server. When a full chain is not present, the TOE will not connect to a TLS server. This meets the testing requirements.

6.1.27 FCS_TLSC_EXT.1.3 Test #2

Item	Data
Test Assurance Activity	The evaluator will use TLS as a function to verify that the validation rules in FIA_X509_EXT.1.1 are adhered to and shall perform the following additional test: • Test 2: The evaluator will demonstrate that a peer using a certificate which has been revoked results in an authentication failure.
Pass/Fail with Explanation	Pass. This testcase was performed in conjunction with FIA_X509_EXT.1.1 Test#3. In this test case, proper handling of revoked is covered. This meets the testing requirements.

6.1.28 FCS_TLSC_EXT.1.3 Test #3

Item	Data
Test Assurance Activity	The evaluator will use TLS as a function to verify that the validation rules in FIA_X509_EXT.1.1 are adhered to and shall perform the following additional test: • Test 3: The evaluator will demonstrate that a peer using a certificate which has passed its expiration date results in an authentication failure.
Test Steps	• Generate an expired TLS server certificate • Attempt to connect to the TLS server with the expired certificate • Verify the connection fails via log • Verify the connection fails via wire capture

Expected Test Results	• The TOE rejects a connection to a TLS server with an expired certificate
Pass/Fail with Explanation	Pass. The TOE rejects connections to external TLS servers when the server certificate is expired. This meets the testing requirements.

6.1.29 FCS_TLSC_EXT.1.3 Test #4

Item	Data
Test Assurance Activity	The evaluator will use TLS as a function to verify that the validation rules in FIA_X509_EXT.1.1 are adhered to and shall perform the following additional test: • Test 4: the evaluator will demonstrate that a peer using a certificate which does not have a valid identifier shall result in an authentication failure.
Test Steps	• Attempt a connection to a remote TLS server using an invalid certificate • Verify the connection fails via pcap
Expected Test Results	• The connection to a server with an invalid certificate fails.
Pass/Fail with Explanation	Pass. Client connection failed when presented with a certificate with an invalid identifier. This meets the testing requirement.

6.1.30 FCS_TLSC_EXT.2.1 Test #1

Item	Data
Test Assurance Activity	The evaluator will also perform the following test: • The evaluator will configure a server to perform ECDHE key exchange using each of the TOE's supported curves and shall verify that the TOE successfully connects to the server.
Test Steps	• Create a TLS server certificate with P-384 curve • Connect to the TLS server using P-384 curve • Verify via wire capture that the connection was successful • Verify via log that the connection was successful
Expected Test Results	• The TOE can connect to a TLS server using the supported elliptic curves
Pass/Fail with Explanation	Pass. The TOE is able to connect to a TLS server using the supported elliptic curves. This meets the testing requirements.

6.1.31 FCS_TLSC_EXT.4.1 Test #1

Item	Data
Test Assurance Activity	The evaluator will also perform the following test: • Test 1: The evaluator will establish a connection to a peer server that is not configured for mutual authentication (i.e. does not send Server's Certificate Request (type 13) message). The evaluator observes negotiation of a TLS channel and confirms that the TOE did not send Client's Certificate message (type 11) during handshake.
Test Steps	• Configure a TLS server without mutual authentication • Connect to the TLS server from the TOE • Verify that the TOE does not send a client certificate via wirecapture • Verify the connection was successful via log
Expected Test Results	• The TOE successfully connects to the TLS server • The TOE does not send a client certificate when it is not requested

Pass/Fail with Explanation	Pass. The TOE does not send a client certificate if it is not requested by the TLS server during a TLS connection. This meets the testing requirements.

6.1.32 FCS_TLSC_EXT.4.1 Test #2

Item	Data
Test Assurance Activity	The evaluator will also perform the following test: • Test 2: The evaluator will establish a connection to a peer server with a shared trusted root that is configured for mutual authentication (i.e. it sends Server's Certificate Request (type 13) message). The evaluator observes negotiation of a TLS channel and confirms that the TOE responds with a non-empty Client's Certificate message (type 11) and Certificate Verify (type 15) messages.
Test Steps	• Configure a TLS server with mutual authentication • Connect to the TLS server from the TOE • Verify that the TOE sends a client certificate via wirecapture • Verify the connection was successful via log
Expected Test Results	• The TOE successfully connects to the TLS server • The TOE sends a client certificate when it is requested
Pass/Fail with Explanation	Pass. The TOE sends a client certificate when requested by the TLS server during a TLS session. This meets the testing requirements.

6.1.33 FDP_ACF_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator will create two new standard user accounts on the system and conduct the following tests: • **Test 1:** The evaluator will authenticate to the system as the first user and create a file within that user's home directory. The evaluator will then log off the system and log in as the second user. The evaluator will then attempt to read the file created in the first user's home directory. The evaluator will ensure that the read attempt is denied.
Test Steps	• Create two users. • Log into the first user and create a file in the home directory. • Log into the second user and try to read the file that is in the other directory. • Verify that it is not successful.
Expected Test Results	• user2 should not be able to access files that belong to user1.
Pass/Fail with Explanation	Pass. The TOE properly restricted user2 from reading a file in the home directory for user1. This meets the testing requirements.

6.1.34 FDP_ACF_EXT.1 Test #2

Item	Data
Test Assurance Activity	The evaluator will create two new standard user accounts on the system and conduct the following tests: • **Test 2:** The evaluator will authenticate to the system as the first user and create a file within that user's home directory. The evaluator will then log off the system and log in as the second user. The evaluator will then attempt to modify the file created in the first user's home directory. The evaluator will ensure that the modification is denied.
Test Steps	• Create two users. • Log into the first user and create a file in the home directory.

	• Log into the second user and try to modify the file that is in the other directory. • Verify that it is not successful.
Expected Test Results	• user2 should not be able to modify files that belong to user1.
Pass/Fail Explanation	Pass. The TOE properly restricted user2 from modifying a file in the home directory for user1. This meets the testing requirements.

6.1.35 FDP_ACF_EXT.1 Test #3

Item	Data
Test Assurance Activity	The evaluator will create two new standard user accounts on the system and conduct the following tests: • **Test 3:** The evaluator will authenticate to the system as the first user and create a file within that user's user directory. The evaluator will then log off the system and log in as the second user. The evaluator will then attempt to delete the file created in the first user's home directory. The evaluator will ensure that the deletion is denied.
Test Steps	• Create two users. • Log into the first user and create a file in the home directory. • Log into the second user and try to delete the file that is in the other directory. • Verify that it is not successful.
Expected Test Results	• user2 should not be able to delete files that belong to user1.
Pass/Fail Explanation	Pass. The TOE properly restricted user2 from deleting a file in the home directory for user1. This meets the testing requirements.

6.1.36 FDP_ACF_EXT.1 Test #4

Item	Data
Test Assurance Activity	The evaluator will create two new standard user accounts on the system and conduct the following tests: • **Test 4:** The evaluator will authenticate to the system as the first user. The evaluator will attempt to create a file in the second user's home directory. The evaluator will ensure that the creation of the file is denied.
Test Steps	• Create two users. • Log into the first user and attempt to create a file in the home directory of user2. • Verify that it is not successful.
Expected Test Results	• user1 should not be able to create a file in the home directory of user2.
Pass/Fail Explanation	Pass. The TOE properly restricted user1 from creating a file in the home directory for user2. This meets the testing requirements.

6.1.37 FDP_ACF_EXT.1 Test #5

Item	Data
Test Assurance Activity	The evaluator will create two new standard user accounts on the system and conduct the following tests: • **Test 5:** The evaluator will authenticate to the system as the first user and attempt to modify the file created in the first user's home directory. The evaluator will ensure that the modification of the file is accepted.
Test Steps	• Create two users.

	• Log into the first user and create a file. • Then attempt to modify that file. • Verify that the modification succeeded.
Expected Test Results	• user1 should be allowed to modify a file in its own home directory.
Pass/Fail Explanation	Pass. The TOE properly allowed user1 to modify a file in the home directory for user1. This meets the testing requirements.

6.1.38 FDP_ACF_EXT.1 Test #6

Item	Data
Test Assurance Activity	The evaluator will create two new standard user accounts on the system and conduct the following tests: • **Test 6:** The evaluator will authenticate to the system as the first user and attempt to delete the file created in the first user's directory. The evaluator will ensure that the deletion of the file is accepted.
Test Steps	• Create two users. • Log into the first user and create a file. • Then attempt to modify that file. • Verify that the modification succeeded.
Expected Test Results	• user1 should be allowed to delete a file in its own home directory.
Pass/Fail Explanation	Pass. The TOE properly allowed user1 to delete a file in the home directory for user1. This meets the testing requirements.

6.1.39 FDP_IFC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator will perform the following test: **Test 1:** • **Step 1**: The evaluator will enable a network connection. The evaluator will sniff packets while performing running applications that use the network such as web browsers and email clients. The evaluator will verify that the sniffer captures the traffic generated by these actions, turn off the sniffing tool, and save the session data. • **Step 2:** The evaluator will configure an IPsec VPN client that supports the routing specified in this requirement. The evaluator will turn on the sniffing tool, establish the VPN connection, and perform the same actions with the device as performed in the first step. The evaluator will verify that the sniffing tool captures traffic generated by these actions, turn off the sniffing tool, and save the session data. • **Step 3:** The evaluator will examine the traffic from both step one and step two to verify that all non-excepted Data Plane traffic in Step 2 is encapsulated by IPsec. The evaluator will examine the Security Parameter Index (SPI) value present in the encapsulated packets captured in Step 2 from the TOE to the Gateway and shall verify this value is the same for all actions used to generate traffic through the VPN. Note that it is expected that the SPI value for packets from the Gateway to the TOE is different than the SPI value for packets from the TOE to the Gateway. • **Step 4:** The evaluator will perform a ping on the TOE host on the local network and verify that no packets sent are captured with the sniffer. The evaluator will

	attempt to send packets to the TOE outside the VPN tunnel (i.e. not through the VPN gateway), including from the local network, and verify that the TOE discards them.
Test Steps	• Ping dns service, local network IP, private host from the TOE. Show that connection succeeds in plaintext. • Configure the third-party IPsec VPN. In this case, two VPNs are configured (inner and outer VPNs). • Start a packet capture on a device that can monitor the local network. Establish both VPNs. • Start a packet capture on a device that can monitor the local network. From the TOE, send a ping to a host on the local network. Verify that no plaintext packets are sent by the TOE. • Verify the SPIs are consistent with correct IPsec behavior and the pings are not seen as plaintext. • From the local network, send a ping to the TOE. • Verify that the TOE does not respond to the ping via wire capture.
Expected Test Results	• The TOE supports the use of third-party VPNs • The TOE allows installed third-party VPNs to correctly handle traffic
Pass/Fail with Explanation	Pass. The TOE supports the use of third-party VPNs. The TOE allows installed third-party VPNs to correctly handle traffic. This meets the testing requirements.

6.1.40 FIA_AFL.1.1 Test#1

Item	Data
Test Assurance Activity	The evaluator will set an administrator-configurable threshold for failed attempts, or note the ST-specified assignment. The evaluator will then (per selection) repeatedly attempt to authenticate with an incorrect password, PIN, or certificate until the number of attempts reaches the threshold. Note that the authentication attempts and lockouts must also be logged as specified in FAU_GEN.1.
Test Steps	• Configure the TOE to 5 max login attempts: • Attempt to log into the TOE with a bad username as password 5 times: • Verify that the system shutdown
Expected Test Results	• The TOE should shut down after the max login attempts is reached
Pass/Fail with Explanation	Pass. The TOE shutdown after the max login attempts was reached. This meets the testing requirements.

6.1.41 FIA_AFL.1.2 Test#1

Item	Data
Test Assurance Activity	**Test 1:** The evaluator will attempt to authenticate repeatedly to the system with a known bad password. Once the defined number of failed authentication attempts has been reached the evaluator will ensure that the account that was being used for testing has had the actions detailed in the assignment list above applied to it. The evaluator will ensure that an event has been logged to the security event log detailing that the account has had these actions applied.
Pass/Fail with Explanation	Pass. The certificate-based authentication was not selected in the SFR. The TOE does not support certificate authentication. This activity is met trivially.

6.1.42 FIA_AFL.1.2 Test#2

Item	Data

Test Assurance Activity	**Test 2:** The evaluator will attempt to authenticate repeatedly to the system with a known bad certificate. Once the defined number of failed authentication attempts has been reached the evaluator will ensure that the account that was being used for testing has had the actions detailed in the assignment list above applied to it. The evaluator will ensure that an event has been logged to the security event log detailing that the account has had these actions applied.
Pass/Fail with Explanation	Pass. The certificate-based authentication was not selected in the SFR. The TOE does not support certificate authentication. This activity is met trivially.

6.1.43 FIA_AFL.1.2 Test#3

Item	Data
Test Assurance Activity	**Test 3:** The evaluator will attempt to authenticate repeatedly to the system using both a bad password and a bad certificate. Once the defined number of failed authentication attempts has been reached the evaluator will ensure that the account that was being used for testing has had the actions detailed in the assignment list above applied to it. The evaluator will ensure that an event has been logged to the security event log detailing that the account has had these actions applied.
Pass/Fail with Explanation	Pass. The certificate-based authentication was not selected in the SFR. The TOE does not support certificate authentication. This activity is met trivially.

6.1.44 FIA_UAU.5.1 Username and Password Test#1

Item	Data
Test Assurance Activity	If user name and password authentication is selected, the evaluator will configure the OS with a known user name and password and conduct the following tests: • **Test 1:** The evaluator will attempt to authenticate to the OS using the known user name and password. The evaluator will ensure that the authentication attempt is successful.
Test Steps	• Attempt to log into the TOE with a good username and password.
Expected Test Results	• Access to the TOE should be granted when a good username and password is presented.
Pass/Fail Explanation	Pass. The evaluator was able to successfully log in to the TOE using a good username/password combination. This meets the testing requirements.

6.1.45 FIA_UAU.5.1 Username and Password Test#2

Item	Data
Test Assurance Activity	If user name and password authentication is selected, the evaluator will configure the OS with a known user name and password and conduct the following tests: • **Test 2:** The evaluator will attempt to authenticate to the OS using the known user name but an incorrect password. The evaluator will ensure that the authentication attempt is unsuccessful.
Test Steps	• Use a good username and a bad password to attempt to login. • Verify that the attempt fails
Expected Test Results	• The TOE should prevent a user from logging in when using a good username and a bad password.
Pass/Fail with Explanation	Pass. The TOE did not allow a user to log into the TOE with a good username and a bad password. This meets the testing requirements.

6.1.46 FIA_UAU.5.2 Test#1

Item	Data
Test Assurance Activity	The evaluator will verify that configuration guidance for each authentication mechanism is addressed in the AGD guidance. • **Test 1:** For each authentication mechanism selected, the evaluator will enable that mechanism and verify that it can be used to authenticate the user at the specified authentication factor interfaces.
Pass/Fail with Explanation	Pass. This test is satisfied by FIA_UAU.5.1 Username and Password Test #1, where the evaluator successfully logged into the TOE with a username and password.

6.1.47 FIA_UAU.5.2 Test#2

Item	Data
Test Assurance Activity	The evaluator will verify that configuration guidance for each authentication mechanism is addressed in the AGD guidance. • **Test 2:** For each authentication mechanism rule, the evaluator will ensure that the authentication mechanism(s) behave as documented in the TSS.
Pass/Fail with Explanation	Pass. This test is satisfied by FIA_UAU.5.1 Username and Password Test #1, where the evaluator successfully logged into the TOE with a username and password. This is also satisfied by FIA_UAU.5.1 Username and Password Test #2, where the TOE denied authentication to a user with a bad password.

6.1.48 FIA_X509_EXT.1.1 Test#1 [TD0525]

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 1:** The evaluator shall demonstrate that validating a certificate without a valid certification path results in the function failing, for each of the following reasons, in turn: ○ by establishing a certificate path in which one of the issuing certificates is not a CA certificate, *create a cert that is not a CA, sign admin server cert with this cert* ○ by omitting the basicConstraints field in one of the issuing certificates, ○ by setting the basicConstraints field in an issuing certificate to have CA=False, ○ by omitting the CA signing bit of the key usage field in an issuing certificate, and *remove keyCertSign from conf* ○ by setting the path length field of a valid CA field to a value strictly less than the certificate path. The evaluator shall then establish a valid certificate path consisting of valid CA certificates, and demonstrate that the function succeeds. The evaluator shall then remove trust in one of the CA certificates, and show that the function fails.
Test Steps	• For each of the following scenarios perform the following: ○ A server certificate path in which one of the issuing certificates is not a CA certificate ○ A server certificate omitting the basicConstraints field in one of the issuing certificates

	○ A server certificate which the basicConstraints field in an issuing certificate to have CA=False ○ A server certificate omitting the CA signing bit of the key usage field in an issuing certificate ○ A server certificate which the path length field of a valid CA field to a value strictly less than the certificate path • Attempt a connection to the TLS server from the TOE. • Verify via PCAP that the connection is rejected via wire capture. • Verify that the connection is rejected via log. • Show a connection succeeds when connecting with a TLS server with a valid certificate path.
Expected Test Results	• The TOE appropriately handles TLS connections when presented certificate chains with various deficiencies
Pass/Fail with Explanation	Pass. The TOE correctly handles TLS connection attempts to TLS servers (rejects the connection) when the server presents invalid certificate chains. The TOE successfully connects to a TLS server when presented a valid certificate chain. This meets the testing requirements.

6.1.49 FIA_X509_EXT.1.1 Test#2

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 2:** The evaluator will demonstrate that validating an expired certificate results in the function failing.
Pass/Fail with Explanation	Pass. This test case was performed in conjunction with FCS_TLSC_EXT.1.3 Test #3. The testcase demonstrated that the TOE will not connect with a peer when presented with an expired certificate. This meets the testing requirements.

6.1.50 FIA_X509_EXT.1.1 Test#3 [TD0525]

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 3:** The evaluator will test that the OS can properly handle revoked certificates - conditional on whether CRL, OCSP, OCSP stapling, or OCSP multi-stapling is selected; if multiple methods are selected, then a test shall be performed for each method. The evaluator will test revocation of the node certificate and revocation of the intermediate CA certificate (i.e. the intermediate CA certificate should be revoked by the root CA). If OCSP stapling per RFC 6066 is the only supported revocation method, testing revocation of the intermediate CA certificate is omitted. The evaluator will ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails.

Test Steps	• Attempt a connection to a server using a good leaf certificate • Show the connection succeeds • Attempt a connection to a server using a revoked leaf certificate • Show the connection fails • Attempt a connection to a server using an unrevoked leaf certificate • Show the connection succeeds • Redo the same steps with the intermediate CA CA Path = Acumen01 > issued from INT-CA2-1 > missing INT-CA1 > issued from ROOT-CA • Issue new INT-CA2-1 certificate from INT-CA1 • Issue CRL to http://test.admin.com/int-ca2-1.crl • Re-issue Admin, Mgmnt, HTTP certificates signed by new INT-CA2-1 certificate • Re-configure Admin, Mgmnt, HTTP servers to use new INT-CA2-1 certificate • Test successful connection to server • Revoke INT-CA2-1 certificate from INT-CA1 • Re-issue CRL to http://test.admin.com/int-ca1.crl • Test failed connection to server • Un-revoke INT-CA2-1 certificate from INT-CA1 • Re-issue CRL to http://test.admin.com/int-ca1.crl • Test successful connection to server • Issue new Acumen01 certificate from INT-CA2 • Re-issue CRL to http://test.admin.com/int-ca2.crl • Test successful connection to server • Revoke Acumen01 certificate from INT-CA2 • Re-issue CRL to http://test.admin.com/int-ca2.crl • Test failed connection to server • Un-revoke Acumen01 certificate from INT-CA2 index/database • Test successful connection to server
Expected Test Results	• The TOE can successfully connect to a TLS server using new certificate. • After revoking a server certificate the TOE rejected the connection to the TLS server. • After unrevoking the certificate, the TOE was able to successfully connect to the TLS server. • After revoking an intermediary certificate of the TLS server, the TOE rejected the TLS connnection. • After the unrevoking the certificate, the TOE was able to connect to the TLS server.
Pass/Fail with Explanation	Pass. The TOE can successfully connect to a TLS server using new certificate. After revoking a server certificate the TOE rejected the connection to the TLS server. After unrevoking the certificate, the TOE was able to successfully connect to the TLS server. After revoking an intermediary certificate of the TLS server, the TOE rejected the TLS connnection. After the unrevoking the certificate, the TOE was able to connect to the TLS server.

6.1.51 FIA_X509_EXT.1.1 Test#4 [TD0525]

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those

	rules. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 4:** If any OCSP option is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLSign key usage bit set and verify that validation of the CRL fails.
Test Steps	• Use an OCSP server missing the OCSP signing purpose • Use a CRL signing certificate that's missing the cRLSign key usage • Attempt a connection to a remote server using a CDP in its certificate • Show the TOE rejects the connection after first checking the OCSP and then CRL because they are invalid
Expected Test Results	• CRL and OCSP are rejected when signed with certs missing crlSign and/or OCSPsigning keys
Pass/Fail with Explanation	Pass. CRL and OCSP are rejected when signed with certs missing crlSign and/or OCSPsigning keys. This meets the testing requirements.

6.1.52 FIA_X509_EXT.1.1 Test#5 [TD0525]

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 5:** The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
Test Steps	• Attempt a connection to a remote server running a tool that would allow sending a modified leaf certificate • Show the TOE denies the connection
Expected Test Results	• The TOE fails to connect to server when the presented certificate was modified.
Pass/Fail with Explanation	Pass. The TOE failed to connect to server when the presented certificate was modified. This meets the testing requirements.

6.1.53 FIA_X509_EXT.1.1 Test#6 [TD0525]

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 6:** The evaluator shall modify any byte in the last byte of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Steps	• Attempt a connection to a remote server running a tool that would allow sending a modified leaf certificate • Show the TOE denies the connection

Expected Test Results	• The TOE fails to connect to server when the presented certificate was modified.
Pass/Fail with Explanation	Pass. The TOE failed to connect to server when the presented certificate was modified. This meets the testing requirements.

6.1.54 FIA_X509_EXT.1.1 Test#7 [TD0525]

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 7:** The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The signature of the certificate will not validate.)
Test Steps	• Attempt a connection to a remote server running a tool that would allow sending a modified leaf certificate • Show the TOE denies the connection
Expected Test Results	• The TOE fails to connect to server when the presented certificate was modified.
Pass/Fail with Explanation	Pass. The TOE failed to connect to server when the presented certificate was modified. This meets the testing requirements.

6.1.55 FIA_X509_EXT.1.1 Test#8a [TD0525]

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 8a:** (Conditional on support for EC certificates as indicated in FCS_COP.1(3)). The evaluator shall establish a valid, trusted certificate chain consisting of an EC leaf certificate, an EC Intermediate CA certificate not designated as a trust anchor, and an EC certificate designated as a trusted anchor, where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain.
Pass/Fail with Explanation	Pass. This test was performed in conjunction with FCS_TLSC_EXT.2.1 Test #1 showing that the TOE can connect with an external server presenting a valid EC certificate. This meets the testing requirements.

6.1.56 FIA_X509_EXT.1.1 Test#8b [TD0525]

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 8b:** (Conditional on support for EC certificates as indicated in FCS_COP.1(3)). The evaluator shall replace the intermediate certificate in the

	certificate chain for Test 8a with a modified certificate, where the modified intermediate CA has a public key information field where the EC parameters uses an explicit format version of the Elliptic Curve parameters in the public key information field of the intermediate CA certificate from Test 8a, and the modified Intermediate CA certificate is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid.
Test Steps	• Attempt a connection to a server using an intermediate certificate that uses an explicit format version of the Elliptic Curve parameters in the public key information field • Show the TOE rejects the connection to the intermediate certificate being invalid
Expected Test Results	• TOE rejects the connection to the intermediate certificate that uses an explicit format version of the Elliptic Curve. This meets the testing requirements.
Pass/Fail with Explanation	Pass. TOE rejected the connection to the intermediate certificate that uses an explicit format version of the Elliptic Curve. This meets the testing requirements.

6.1.57 FIA_X509_EXT.1.2 Test#1

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 1:** The evaluator will construct a certificate path, such that the certificate of the CA issuing the OS's certificate does not contain the basicConstraints extension. The validation of the certificate path fails.
Test Steps	• Attempt a connection to a remote server using a CA missing the basicConstraints extension. • Show the TOE rejects the connection
Expected Test Results	• The TOE rejects a connection with a TLS server that presents a certificate missing the basicConstraints extension.
Pass/Fail with Explanation	Pass. The TOE rejects a connection with a TLS server that presents a certificate missing the basicConstraints extension. This meets the testing requirements.

6.1.58 FIA_X509_EXT.1.2 Test#2

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 2:** The evaluator will construct a certificate path, such that the certificate of the CA issuing the OS's certificate has the CA flag in the basicConstraints extension not set. The validation of the certificate path fails.
Test Steps	• Attempt a connection to a remote server using a CA with the basicConstraints extension set to false • Show the TOE rejects the connection
Expected Test Results	• The TOE rejects a connection with a TLS server that presents a certificate with the basicConstraints extension set to false.

Pass/Fail with Explanation	Pass. The TOE rejects a connection with a TLS server that presents a certificate with the basicConstraints extension set to false. This meets the testing requirements.

6.1.59 FIA_X509_EXT.1.2 Test#3

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The evaluator will create a chain of at least four certificates: the node certificate to be tested, two Intermediate CAs, and the self-signed Root CA. • **Test 3:** The evaluator will construct a certificate path, such that the certificate of the CA issuing the OS's certificate has the CA flag in the basicConstraints extension set to TRUE. The validation of the certificate path succeeds.
Pass/Fail with Explanation	Pass. This test case was tested in conjunction with various FCS_TLSC_EXT.1 and FIA_X509_EXT.1 test cases. In those test cases, the successfully connected to TLS servers presenting a certificate with CA flag in basicConstraints extension set to TRUE. This meets the testing requirements.

6.1.60 FIA_X509_EXT.2 Test#1

Item	Data
Test Assurance Activity	The evaluator will acquire or develop an application that uses the OS TLS mechanism with an X.509v3 certificate. The evaluator will then run the application and ensure that the provided certificate is used to authenticate the connection. The evaluator will repeat the activity for any other selections listed.
Pass/Fail with Explanation	Pass. This test case was tested in conjunction with various FCS_TLSC_EXT.1 and FIA_X509_EXT.1 test cases. In those test cases, the successfully connected to TLS servers presenting a certificate in support of certificate based authentication. This meets the testing requirements.

6.1.61 FMT_MOT_EXT.1 Test #1

Item	Data
Test Assurance Activity	**Test 1:** For each function that is indicated as restricted to the administrator, the evaluation shall perform the function as an administrator, as specified in the Operational Guidance, and determine that it has the expected effect as outlined by the Operational Guidance and the SFR. The evaluator will then perform the function (or otherwise attempt to access the function) as a non-administrator and observe that they are unable to invoke that functionality.

Test Steps	• Perform the following functions as both an administrator and a non-administrator and verify that only the administrator can invoke the functionality.
	  ○ Enable/disable [session timeout]
	  ○ Configure [session] inactivity timeout
	  ○ Configure lockout policy for unsuccessful authentication attempts through [timeouts between attempts]
	  ○ Configure name/address of remote management server from which to receive management settings
	  ○ Configure name/address of audit/logging server to which to send audit/logging records
	  ○ Enable/disable automatic software update
	• Create or Modify user accounts

Expected Test Results	• The TOE should restrict administrator function to an administrator
Pass/Fail with Explanation	Pass. The TOE restricts administrator function to an administrator.

6.1.62 FMT_SMF_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator will test the OS's ability to provide the management functions by configuring the operating system and testing each option selected from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.
Test Steps	• Perform the following management functions in accordance to the guidance and ST documentation. ○ Change the password of the currently-authenticated user ○ Configure network interface settings ○ Set system Time-Zone ○ Perform Factory Reset
Expected Test Results	• The TOE should be capable of providing the management function selected in the ST.
Pass/Fail with Explanation	Pass. The TOE can provide the management function selected in the ST. The remaining management functions were tested in conjunction with FMT_MOF_EXT.1 Test #1

6.1.63 FPT_ACF_EXT.1.1 Test#1

Item	Data
Test Assurance Activity	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): • **Test 1:** The evaluator will attempt to modify all kernel drivers and modules.
Test Steps	• Attempt to modify all kernel drivers and modules using an unprivileged account • Show the TOE denies the modification
Expected Test Results	• The TOE should not allow an unprivileged user to modify kernel drivers and modules.
Pass/Fail with Explanation	Pass. The TOE does not allow an unprivileged user to modify kernel drivers and modules.

6.1.64 FPT_ACF_EXT.1.1 Test#2

Item	Data
Test Assurance Activity	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): • **Test 2:** The evaluator will attempt to modify all security audit logs generated by the logging subsystem.
Test Steps	• Attempt to modify all security audit logs using an unprivileged account • Show the TOE denies the modification
Expected Test Results	• The TOE should not allow an unprivileged user to modify security audit logs.
Pass/Fail with Explanation	Pass. The TOE does not allow an unprivileged user to modify security audit logs.

6.1.65 FPT_ACF_EXT.1.1 Test#3

Item	Data
Test Assurance Activity	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): • **Test 3:** The evaluator will attempt to modify all shared libraries that are used throughout the system.
Test Steps	• Attempt to modify all shared libraries using an unprivileged account • Show the TOE denies the modification
Expected Test Results	• The TOE should not allow an unprivileged user to modify shared libraries.
Pass/Fail with Explanation	Pass. Shared libraries are not accessible to users.

6.1.66 FPT_ACF_EXT.1.1 Test#4

Item	Data
Test Assurance Activity	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): • **Test 4:** The evaluator will attempt to modify all system executables.
Test Steps	• Attempt to modify all system executables using an unprivileged account • Show the TOE denies the modification
Expected Test Results	• The TOE should not allow an unprivileged user to modify system executables.
Pass/Fail with Explanation	Pass. The TOE does not allow an unprivileged user to modify system executables.

6.1.67 FPT_ACF_EXT.1.1 Test#5

Item	Data
Test Assurance Activity	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): • **Test 5:** The evaluator will attempt to modify all system configuration files.
Test Steps	• Attempt to modify all system executables using an unprivileged account • Show the TOE denies the modification
Expected Test Results	• The TOE should not allow an unprivileged user to modify system configuration files.
Pass/Fail with Explanation	Pass. The TOE does not allow an unprivileged user to modify system configuration files.

6.1.68 FPT_ACF_EXT.1.1 Test#6

Item	Data
Test Assurance Activity	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): • **Test 6:** The evaluator will attempt to modify any additional components selected.

Pass/Fail with Explanation	Pass. The ST does not include a selection for any additional components. This activity is met trivially.

6.1.69 FPT_ACF_EXT.1.2 Test#1

Item	Data
Test Assurance Activity	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): • **Test 1:** The evaluator will attempt to read security audit logs generated by the auditing subsystem
Test Steps	• Attempt to read security audit logs using an unprivileged account • Show the TOE denies the action
Expected Test Results	• The TOE should not allow an unprivileged user to read the security audit logs.
Pass/Fail with Explanation	Pass. Unprivileged users do not have read/write execution for security logs. This meets the testing requirements.

6.1.70 FPT_ACF_EXT.1.2 Test#2

Item	Data
Test Assurance Activity	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): • **Test 2:** The evaluator will attempt to read system-wide credential repositories
Test Steps	• Attempt to read system-wide credential repositories using an unprivileged account • Show the TOE denies the action
Expected Test Results	• The TOE should not allow an unprivileged user to read system-wide credential repositories.
Pass/Fail with Explanation	Pass. System-wide credential repositories are not accessible to users.

6.1.71 FPT_ACF_EXT.1.2 Test#3

Item	Data
Test Assurance Activity	The evaluator will create an unprivileged user account. Using this account, the evaluator will ensure that the following tests result in a negative outcome (i.e., the action results in the OS denying the evaluator permission to complete the action): • **Test 3:** The evaluator will attempt to read any other object specified in the assignment
Pass/Fail with Explanation	Pass. No other objects are specified in the assignment.

6.1.72 FPT_ASLR_EXT.1 Test#1

Item	Data
Test Assurance Activity	The evaluator will select 3 executables included with the TSF. If the TSF includes a web browser it must be selected. If the TSF includes a mail client it must be selected. For each of these apps, the evaluator will launch the same executables on two separate instances of the OS on identical hardware and compare all memory mapping locations. The evaluator will ensure that no memory mappings are placed in the same location. If the

	rare chance occurs that two mappings are the same for a single executable and not the same for the other two, the evaluator will repeat the test with that executable to verify that in the second test the mappings are different. This test can also be completed on the same hardware and rebooting between application launches.
Test Steps	• Log into the TOE as root and run the ASLR command to view the memory mapping locations • Reboot the TOE • Repeat step 1 • Verify the numbers are different
Expected Test Results	• The memory location of executables is not the same after reboot.
Pass/Fail Explanation	Pass. The memory location of executables is not the same after reboot. This meets the testing requirements.

6.1.73 FPT_SBOP_EXT.1 Test#1

Item	Data
Test Assurance Activity	The evaluator will also preform the following test: • **Test 1:** The evaluator will inventory the kernel, libraries, and application binaries to determine those that do not implement stack-based buffer overflow protections. This list should match up with the list provided in the TSS.
Test Steps	• Unbundle an OTA update. Search through the INTEGRITY monolith to find the programs. • Once the programs are found, use the offset values to search for the string of bytes that indicate the beginning of a stack check followed by the expected instruction that indicate that stack-based buffer overflow protection is used. • The results should match the list in the ST.
Expected Test Results	• The TSS list should match the result of programs that do not implement stack-based buffer overflow protection.
Pass/Fail with Explanation	Pass. The TSS list matches the result of programs that do not implement stack-based buffer overflow protection.

6.1.74 FPT_TST_EXT.1 Test#1

Item	Data
Test Assurance Activity	The evaluator will also perform the following test: • **Test 1:** The evaluator will perform actions to cause TSF software to load and observe that the integrity mechanism does not flag any executables as containing integrity errors and that the OS properly boots.
Test Steps	• Reboot the device. • Verify after boot that the OS loaded properly and does not flag any integrity errors
Expected Test Results	• The TOE successfully boots when the integrity mechanism does not flag any executables as containing integrity errors
Pass/Fail with Explanation	Pass. The TOE successfully boots when the integrity mechanism does not flag any executables as containing integrity errors. This meets the testing requirements.

6.1.75 FPT_TST_EXT.1 Test#2

Item	Data
Test Assurance Activity	The evaluator will also perform the following test:

	• **Test 2:** The evaluator will modify a TSF executable that is part of the bootchain verified by the TSF (i.e. Not the first-stage bootloader) and attempt to boot. The evaluator will ensure that an integrity violation is triggered and the OS does not boot (Care must be taken so that the integrity violation is determined to be the cause of the failure to load the module, and not the fact that in such a way to invalidate the structure of the module.).
Test Steps	• Modify a boot file to generate an integrity violation • Show the TOE detects the violation
Expected Test Results	• When a boot file fails the integrity test, the TOE enters an error state.
Pass/Fail with Explanation	Pass. When a boot file fails the integrity test, the TOE enters an error state. This meets the testing requirements.

6.1.76 FPT_TST_EXT.1 Test#3 [TD0493]

Item	Data
Test Assurance Activity	The evaluator will also preform the following test: ***Test 3[conditional]***: If the ST author indicates that the integrity verification is performed using a public key *in an X509 certificate*, the evaluator will verify that the boot integrity mechanism includes a certificate validation according to FIA_X509_EXT.1 or all certificates in the chain from the certificate used for boot integrity to a certificate in the trust store that are not themselves in the trust store. This means that, for each X509 certificate in this chain that is not a trust store element, the evaluator must ensure that revocation information is available to the TOE during the bootstrap mechanism (before the TOE becomes fully operational).
Pass/Fail with Explanation	Pass. The TOE does not use X509 certificates for boot integrity validation. This activity is met trivially.

6.1.77 FPT_TUD_EXT.1.1 Test#1 [TD0463]

Item	Data
Test Assurance Activity	The evaluator will check for an update using procedures described in the documentation and verify that the OS provides a list of available updates. Testing this capability may require installing and temporarily placing the system into a configuration in conflict with secure configuration guidance which specifies automatic update. The evaluator is also to ensure that the response to this query is authentic by using a digital signature scheme specified in FCS_COP.1(3). The digital signature verification may be performed as part of a network protocol as described in FTP_ITC_EXT.1.) If the signature verification is not performed as part of a trusted channel, the evaluator shall send a query response with a bad signature and verify that the signature verification fails. The evaluator shall then send a query response with a good signature and verify that the signature verification is successful.
Test Steps	• Initiate an update attempt from the TOE to a server with a bad update • Verify the TOE initiated the request over TLS via wire capture • Verify the TOE initiated the request over TLS via log • Verify that the TOE rejected the update attempt
Expected Test Results	• The TOE rejects update attempts when there is a signature problem with the request
Pass/Fail with Explanation	Pass. The TOE rejects update attempts when the verification request has a bad signature. This meets the testing requirements.

6.1.78 FPT_TUD_EXT.1.2 Test#1

Item	Data
Test Assurance Activity	For the following tests, the evaluator will initiate the download of an update and capture the update prior to installation. The download could originate from the vendor's website, an enterprise-hosted update repository, or another system (e.g. network peer). All supported origins for the update must be indicated in the TSS and evaluated. • **Test 1:** The evaluator will ensure that the update has a digital signature belonging to the vendor prior to its installation. The evaluator will modify the downloaded update in such a way that the digital signature is no longer valid. The evaluator will then attempt to install the modified update. The evaluator will ensure that the OS does not install the modified update.
Test Steps	• Create a bad update by modifying the signature of a good update • Initiate an update attempt from the TOE to a server with a bad update • Verify the TOE initiated the request over TLS via wire capture • Verify the TOE initiated the request over TLS via log • Verify that the TOE rejected the update attempt
Expected Test Results	• The TOE rejects update attempts when there is a signature problem with the image
Pass/Fail with Explanation	Pass. The TOE rejects update attempts when the image has a bad signature. This meets the testing requirements.

6.1.79 FPT_TUD_EXT.1.2 Test#2

Item	Data
Test Assurance Activity	For the following tests, the evaluator will initiate the download of an update and capture the update prior to installation. The download could originate from the vendor's website, an enterprise-hosted update repository, or another system (e.g. network peer). All supported origins for the update must be indicated in the TSS and evaluated. • **Test 2:** The evaluator will ensure that the update has a digital signature belonging to the vendor. The evaluator will then attempt to install the update (or permit installation to continue). The evaluator will ensure that the OS successfully installs the update.
Test Steps	• Initiate an update using an image with a valid signature • Verify that the TOE was able to be updated
Expected Test Results	• The TOE will update with an image with a valid signature
Pass/Fail with Explanation	Pass. The TOE is able to be updated with an image that has a valid signature.

6.1.80 FPT_TUD_EXT.2.1 Test#1 [TD0463]

Item	Data
Test Assurance Activity	The evaluator will check for updates to application software using procedures described in the documentation and verify that the OS provides a list of available updates. Testing this capability may require temporarily placing the system into a configuration in conflict with secure configuration guidance which specifies automatic update. The evaluator is also to ensure that the response to this query is authentic by using a digital signature scheme specified in FCS_COP.1(3). The digital signature verification may be performed as part of a network protocol as described in FTP_ITC_EXT.1.) If the signature verification is not performed as part of a trusted channel, the evaluator shall

	send a query response with a bad signature and verify that the signature verification fails. The evaluator shall then send a query response with a good signature and verify that the signature verification is successful.
Test Steps	• Initiate an application update attempt from the TOE to a server with a bad update • Verify the TOE initiated the request over TLS via wire capture • Verify the TOE initiated the request over TLS via log • Verify that the TOE rejected the update attempt
Expected Test Results	• The TOE rejects update attempts when there is a signature problem with the request
Pass/Fail with Explanation	Pass. The TOE rejects an application update attempt when the verification request has a bad signature. This meets the testing requirements.

6.1.81 FPT_TUD_EXT.2.2 Test#1

Item	Data
Test Assurance Activity	The evaluator will initiate an update to an application. This may vary depending on the application, but it could be through the application vendor's website, a commercial app store, or another system. All origins supported by the OS must be indicated in the TSS and evaluated. However, this only includes those mechanisms for which the OS is providing a trusted installation and update functionality. It does not include user or administrator-driven download and installation of arbitrary files. • **Test 1:** The evaluator will ensure that the update has a digital signature which chains to the OS vendor or another trusted root managed through the OS. The evaluator will modify the downloaded update in such a way that the digital signature is no longer valid. The evaluator will then attempt to install the modified update. The evaluator will ensure that the OS does not install the modified update.
Test Steps	• Create a bad application update by modifying the signature of a good update • Initiate an update attempt from the TOE to a server with a bad application update • Verify the TOE initiated the request over TLS via wire capture • Verify the TOE initiated the request over TLS via log • Verify that the TOE rejected the update attempt
Expected Test Results	• The TOE rejects update attempts when there is a signature problem with the image
Pass/Fail with Explanation	Pass. The TOE rejects application update attempts when the application has a bad signature. This meets the testing requirements.

6.1.82 FPT_TUD_EXT.2.2 Test#2

Item	Data
Test Assurance Activity	The evaluator will initiate an update to an application. This may vary depending on the application, but it could be through the application vendor's website, a commercial app store, or another system. All origins supported by the OS must be indicated in the TSS and evaluated. However, this only includes those mechanisms for which the OS is providing a trusted installation and update functionality. It does not include user or administrator-driven download and installation of arbitrary files. • **Test 2:** The evaluator will ensure that the update has a digital signature belonging to the OS vendor or another trusted root managed through the OS.

	The evaluator will then attempt to install the update. The evaluator will ensure that the OS successfully installs the update.
Test Steps	• Perform an update of the TOE • Ensure the update was successful
Expected Test Results	• The TOE will be able to perform an update using a well-formed and signed image.
Pass/Fail with Explanation	Pass. The TOE can perform an application update using a well-formed and signed image. This meets the testing requirements.

6.1.83 FTA_TAB.1 Test#1

Item	Data
Test Assurance Activity	The evaluator will configure the OS, per instructions in the OS manual, to display the advisory warning message "TEST TEST Warning Message TEST TEST". The evaluator will then log out and confirm that the advisory message is displayed before logging in can occur.
Test Steps	• Perform an update of the TOE • Ensure the update was successful
Expected Test Results	• The TOE will be able to perform an update using a well-formed and signed image.
Pass/Fail with Explanation	Pass. The TOE can perform an application update using a well-formed and signed image. This meets the testing requirements.

6.1.84 FTP_ITC_EXT.1 Test#1

Item	Data
Test Assurance Activity	The evaluator will configure the OS to communicate with another trusted IT product as identified in the second selection. The evaluator will monitor network traffic while the OS performs communication with each of the servers identified in the second selection. The evaluator will ensure that for each session a trusted channel was established in conformance with the protocols identified in the first selection.
Pass/Fail with Explanation	Pass. This test is completed in conjunction with FCS_TLSC_EXT.1. The evaluator monitored the network traffic while the TOE established a successful connection with an external TLS server and verified that the TOE established a trusted channel with the TLS webserver in accordance with FCS_TLSC_EXT.1.

6.1.85 FTP_TRP.1 Test#1

Item	Data
Test Assurance Activity	The evaluator will also perform the following tests: • **Test 1:** The evaluator will ensure that communications using each 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.
Pass/Fail with Explanation	Pass. This test is completed in conjunction with FCS_TLSC_EXT.1. The tester verified that connections to the Administration Server were encrypted used TLS.

6.1.86 FTP_TRP.1 Test#2

Item	Data
Test Assurance Activity	The evaluator will also perform the following tests:

	• **Test 2:** For each method of remote administration supported, the evaluator will 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.
Pass/Fail with Explanation	Pass. This test is completed in conjunction with FCS_TLSC_EXT.1. The tester verified that connections to the Administration Server were encrypted used TLS. Remote administration sessions are initiated by the TOE. There is not a method to initiate an insecure session.

6.1.87 FTP_TRP.1 Test#3

Item	Data
Test Assurance Activity	The evaluator will also perform the following tests: • **Test 3:** The evaluator will ensure, for each method of remote administration, the channel data is not sent in plaintext.
Pass/Fail with Explanation	Pass. This test is completed in conjunction with FCS_TLSC_EXT.1. The tester verified that connections to the Administration Server were encrypted used TLS.

6.1.88 FTP_TRP.1 Test#4

Item	Data
Test Assurance Activity	The evaluator will also perform the following tests: • **Test 4:** The evaluator will ensure, for each method of remote administration, modification of the channel data is detected by the OS.
Pass/Fail with Explanation	Pass. This test was performed in conjunction with FCS_TLSC_EXT.1.1 Test #5.3, FCS_TLSC_EXT.1.1 Test #5.4, and FCS_TLSC_EXT.1.1 Test #5.5. Each time there was a modification to the TLS connection. The TOE rejected the connection.

7 Security Assurance Requirements

7.1 ADV_FSP.1 Development

There are no specific evaluation activities associated with these SARs, except ensuring the information is provided. The functional specification documentation is provided to support the evaluation activities described in Section 5.1 Security Functional Requirements, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other evaluation activities being performed; if the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.	
Evaluator Findings	Per this PP, the Evaluation Activities for this family focus on understanding the interfaces presented in the TSS in response to the functional requirements and the interfaces presented in the AGD documentation. No additional 'functional specification' documentation is necessary to satisfy the Evaluation Activities specified in the ST. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2 AGD_OPE.1 Guidance 1

Some of the contents of the operational guidance are verified by the evaluation activities in Section 5.1 Security Functional Requirements, and evaluation of the OS according to the [CEM]. The following additional information is also required. If cryptographic functions are provided by the OS, the operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the OS. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the OS. The documentation must describe the process for verifying updates to the OS by verifying a digital signature – this may be done by the OS or the underlying platform. The evaluator will verify that this process includes the following steps: Instructions for obtaining the update itself. This should include instructions for making the update accessible to the OS (e.g., placement in a specific directory). Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the hash/digital signature. The OS will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities.	
Evaluator Findings	Section 2 of AGD “Installation” provides instructions for configuring the TOE into its CC configuration. As part of this configuration, all cryptographic algorithms are limited to only the allowed algorithms. The section titled “Administration” of AGD “Installation”, “Updates”, “Configure Automatic Software Updates” of AGD provides instructions to the Administrator for performing an update. Step by step instructions are provided for the administrator to follow including downloading the image, copying it to the TOE and installing it. This includes integrity verification. The entirety of the guidance documentation identifies the evaluated capabilities of the TOE by describing how to configure each for Common Criteria. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3 AGD_PRE.1 Guidance 1

As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support OS functional requirements. The evaluator shall check to ensure that the guidance provided for the OS adequately addresses all platforms claimed for the OS in the ST.	
Evaluator Findings	The evaluator used the guidance documentation when configuring the TOE. The completeness of the documentation is addressed by its use in the AA's carried out in the evaluation.
Verdict	Pass

7.4 ALC_CMC.1 TSS 1

The evaluator will 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. Further, the evaluator will check the AGD guidance and OS 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 OS, the evaluator will examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.	
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same versions and software. The information is specific enough to procure the TOE and it includes software versions. The evaluator checked the TOE software version during testing by examining the actual machines used for testing.
Verdict	Pass

7.5 ALC_CMS.1 Guidance 1

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 OS is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the evaluation activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component. Life-cycle support is targeted aspects of the developer's life-cycle and instructions to providers of applications for the developer's devices, rather than an in-depth examination of the TSF manufacturer's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation. The evaluator will ensure that the developer has identified (in guidance documentation for application developers concerning the targeted platform) one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the developer shall provide information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment(s) are invoked (e.g., compiler and linker flags). The evaluator will ensure that this documentation also includes an indication of whether such protections are on by default, or have to be specifically enabled. The evaluator will ensure that the TSF is uniquely identified (with respect to other products from the TSF vendor), and that documentation provided by the developer in association with the requirements in the ST is associated with the TSF using this unique identification.	
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same product versions and software. The information is specific enough to procure the TOE and it includes software versions. The evaluator checked the TOE software version during testing by examining the actual machines used for testing. The section "Application Developers" of AGD provides instructions to create programs that have buffer overflow and ASLR protections enabled.
Verdict	Pass

7.6 ALC_TSU_EXT.1 TSS 1

The evaluator will verify that the TSS contains a description of the timely security update process used by the developer to create and deploy security updates. The evaluator will verify that this description addresses the entire application. The evaluator will also verify that, in addition to the OS developer's process, any third party processes are also addressed in the description. The evaluator will also verify that each mechanism for deployment of security updates is described. The evaluator will verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the OS patching this vulnerability, to include any third-party or carrier delays in deployment. The evaluator will verify that this time is expressed in a number or range of days. The evaluator will verify that this description includes the publicly available mechanisms (including either an email address or website) for reporting security issues related to the OS. The evaluator shall verify that the description of this mechanism includes a method for protecting the report either using a public key for encrypting email or a trusted channel for a website.	
Evaluator Findings	The evaluator verified that the TSS contains a description of the timely security update process used by the developer to create and deploy security updates. The TSS of the ST was used to determine the verdict of this activity. Upon, investigation, the evaluator found that vulnerabilities are submitted via a secure web portal. Additionally, the evaluator found that that the time between reporting and resolution of the vulnerability is no more than 90 days.
Verdict	Pass

7.7 ATE_IND.1 Test 1

The evaluator will prepare a test plan and report documenting the testing aspects of the system, including any application crashes during testing. The evaluator shall determine the root cause of any application crashes and include that information in the report. The test plan covers all of the testing actions contained in the [CEM] and the body of this PP's evaluation activities. While it is not necessary to have one test case per test listed in an evaluation activity, the evaluator must document in the test plan that each applicable testing requirement in the ST is covered. The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary. The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the OS and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS). The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.	
Evaluator Findings	The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator

	found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities.
Verdict	Pass

7.8 AVA_VAN.1 Test 1

The evaluator will 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 find vulnerabilities that have been found in similar applications with a particular focus on network protocols the application uses and document formats it parses. 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. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.	
Evaluator Findings	The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE. The sources of the publicly available information are provided below. • www.idtec.com • https://nvd.nist.gov/view/vuln/search • https://cve.mitre.org/cve • http://www.kb.cert.org/vuls/html/search • www.exploitsearch.net • www.securiteam.com • http://nessus.org/plugins/index.php?view=search • http://www.zerodayinitiative.com/advisories • https://www.exploit-db.com/ • https://www.rapid7.com/db/vulnerabilities The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on 4/11/2022. • INTEGRITY Enterprise OS • Intel Core i5-8365U • INTEGRITY Crypto Library (ICL) • Archon Security The evaluator selected the search key words based upon the following criteria. • The vendor name was searched, • The product name was searched, • The software running on the TOE devices were searched. Further, the version the TOE software in evaluation was searched, The date of the vulnerability search was 4/11/22.

	No vulnerabilities for the TOE or associated components were found.
Verdict	Pass

8 Conclusions

The testing shows that all test cases required for conformance have passed testing.

---End of Document---