Supporting Document
Mandatory Technical Document

PP-Module for Authentication Servers
Version: 1.0
2022-08-12
National Information Assurance Partnership

Foreword

This is a Supporting Document (SD), intended to complement the Common Criteria version 3 and the associated Common Evaluation Methodology for Information Technology Security Evaluation.

SDs may be “Guidance Documents”, that highlight specific approaches and application of the standard to areas where no mutual recognition of its application is required, and as such, are not of normative nature, or “Mandatory Technical Documents”, whose application is mandatory for evaluations whose scope is covered by that of the SD. The usage of the latter class is not only mandatory, but certificates issued as a result of their application are recognized under the CCRA.

Technical Editor:
National Information Assurance Partnership (NIAP)

Document history:

Version	Date	Comment
1.0	2022-08-12	Initial Release

General Purpose:
The purpose of this SD is to define evaluation methods for the functional behavior of Authentication Server products.

Acknowledgments:
This SD was developed with support from NIAP Authentication Servers Technical Community members, with representatives from industry, government agencies, Common Criteria Test Laboratories, and members of academia.

Table of Contents

1 Introduction

1.1 Technology Area and Scope of Supporting Document

The scope of the PP-Module for Authentication Servers is to describe the security functionality of Authentication Servers products in terms of [CC] and to define functional and assurance requirements for them. The PP-Module is intended for use with the following Base-PP:

- Network Device, version 2.2e

This SD is mandatory for evaluations of TOEs that claim conformance to a PP-Configuration that includes the PP-Module for :

- Authentication Servers, Version 1.0

As such it defines Evaluation Activities for the functionality described in the PP-Module as well as any impacts to the Evaluation Activities to the Base-PP(s) it modifies.

Although Evaluation Activities are defined mainly for the evaluators to follow, in general they also help developers to prepare for evaluation by identifying specific requirements for their TOE. The specific requirements in Evaluation Activities may in some cases clarify the meaning of Security Functional Requirements (SFR), and may identify particular requirements for the content of Security Targets (ST) (especially the TOE Summary Specification), user guidance documentation, and possibly supplementary information (e.g. for entropy analysis or cryptographic key management architecture).

1.2 Structure of the Document

Evaluation Activities can be defined for both SFRs and Security Assurance Requirements (SAR), which are themselves defined in separate sections of the SD.

If any Evaluation Activity cannot be successfully completed in an evaluation, then the overall verdict for the evaluation is a 'fail'. In rare cases there may be acceptable reasons why an Evaluation Activity may be modified or deemed not applicable for a particular TOE, but this must be approved by the Certification Body for the evaluation.

In general, if all Evaluation Activities (for both SFRs and SARs) are successfully completed in an evaluation then it would be expected that the overall verdict for the evaluation is a ‘pass’. To reach a ‘fail’ verdict when the Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

Similarly, at the more granular level of assurance components, if the Evaluation Activities for an assurance component and all of its related SFR Evaluation Activities are successfully completed in an evaluation then it would be expected that the verdict for the assurance component is a ‘pass’. To reach a ‘fail’ verdict for the assurance component when these Evaluation Activities have been successfully completed would require a specific justification from the evaluator as to why the Evaluation Activities were not sufficient for that TOE.

1.3 Terms

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

1.3.1 Common Criteria Terms

Assurance	Grounds for confidence that a TOE meets the SFRs [CC].
Base Protection Profile (Base-	Protection Profile used as a basis to build a PP-Configuration.

PP)	
Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
Distributed TOE	A TOE composed of multiple components operating as a logical whole.
Operational Environment (OE)	Hardware and software that are outside the TOE boundary that support the TOE functionality and security policy.
Protection Profile (PP)	An implementation-independent set of security requirements for a category of products.
Protection Profile Configuration (PP-Configuration)	A comprehensive set of security requirements for a product type that consists of at least one Base-PP and at least one PP-Module.
Protection Profile Module (PP-Module)	An implementation-independent statement of security needs for a TOE type complementary to one or more Base-PPs.
Security Assurance Requirement (SAR)	A requirement to assure the security of the TOE.
Security Functional Requirement (SFR)	A requirement for security enforcement by the TOE.
Security Target (ST)	A set of implementation-dependent security requirements for a specific product.
Target of Evaluation (TOE)	The product under evaluation.
TOE Security Functionality (TSF)	The security functionality of the product under evaluation.
TOE Summary Specification (TSS)	A description of how a TOE satisfies the SFRs in an ST.

1.3.2 Technical Terms

Assertion	A statement from the TOE to an RP that contains information about a subscriber. Assertions may also contain verified attributes. For the purposes of this PP-Module, Assertions containing authentication status and identity attributes are made by EAP response messages in accordance with EAP-TLS or EAP-TTLS.
Authentication Policy	A policy that specifies which authenticator types are required for a particular entity. The policy may be implicit for all entities, or configurable.
Authenticator	Something the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant’s identity.

Authenticator Output	The output value generated by an authenticator. The ability to generate valid authenticator outputs on demand proves that the claimant possesses and controls the authenticator. Protocol messages sent to the verifier are dependent upon the authenticator output, but they may or may not explicitly contain it.
Claimant	A subject whose identity is to be verified using one or more authentication protocols.
Credential	An object or data structure that authoritatively binds an identity - via an identifier or identifiers - and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber.
Federation Protocol	A protocol to establish a trusted relationship with a relying party, and for the purposes of this PP module, to communicate authentication status for entities requesting access to resources managed by the relying party. In this PP-module, Federation Protocols include RADIUS, DIAMETER, and other standard protocols used in direct communication between the relying party and the TOE. Federation protocols that only support bearer assertions are out of scope for this PP-Module.
Relying Party (RP)	An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.

2 Evaluation Activities for SFRs

The EAs presented in this section capture the actions the evaluator performs to address technology specific aspects covering specific SARs (e.g. ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, and ATE_IND.1) – this is in addition to the CEM workunits that are performed in Section 3 Evaluation Activities for SARs.

Regarding design descriptions (designated by the subsections labeled TSS, as well as any required supplementary material that may be treated as proprietary), the evaluator must ensure there is specific information that satisfies the EA. For findings regarding the TSS section, the evaluator's verdicts will be associated with the CEM workunit ASE_TSS.1-1. Evaluator verdicts associated with the supplementary evidence will also be associated with ASE_TSS.1-1, since the requirement to provide such evidence is specified in ASE in the PP.

For ensuring the guidance documentation provides sufficient information for the administrators/users as it pertains to SFRs, the evaluator's verdicts will be associated with CEM workunits ADV_FSP.1-7, AGD_OPE.1-4, and AGD_OPE.1-5.

Finally, the subsection labeled Tests is where the authors have determined that testing of the product in the context of the associated SFR is necessary. While the evaluator is expected to develop tests, there may be instances where it is more practical for the developer to construct tests, or where the developer may have existing tests. Therefore, it is acceptable for the evaluator to witness developer-generated tests in lieu of executing the tests. In this case, the evaluator must ensure the developer's tests are executing both in the manner declared by the developer and as mandated by the EA. The CEM workunits that are associated with the EAs specified in this section are: ATE_IND.1-3, ATE_IND.1-4, ATE_IND.1-5, ATE_IND.1-6, and ATE_IND.1-7.

2.1 Collaborative Protection Profile for NDs

The EAs defined in this section are only applicable in cases where the TOE claims conformance to a PP-Configuration that includes the NDcPP.

2.1.1 Modified SFRs

2.1.1.1 Identification and Authentication (FIA)

FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1/Rev
TSS
There are no additional TSS evaluation activities for this component beyond what the NDcPP requires.

Guidance
There are no additional guidance evaluation activities for this component beyond what the NDcPP requires.

Tests
There are no additional test evaluation activities for this component beyond what the NDcPP requires.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2

TSS
There are no additional TSS evaluation activities for this component beyond what the NDcPP requires.

Guidance
There are no additional guidance evaluation activities for this component beyond what the NDcPP requires.

Tests
There are no additional test evaluation activities for this component beyond what the NDcPP requires.

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3
TSS
There are no additional TSS evaluation activities for this component beyond what the NDcPP requires.

Guidance
There are no additional guidance evaluation activities for this component beyond what the NDcPP requires.

Tests
There are no additional test evaluation activities for this component beyond what the NDcPP requires.

2.2 TOE SFR Evaluation Activities

2.2.1 Security Audit (FAU)

FAU_GEN.1/AuthSvr Audit Data Generation

FAU_GEN.1/AuthSvr
TSS
There are no TSS evaluation activities for this SFR.

Guidance
The evaluator shall ensure that the operational guidance identifies the auditable events and includes representative examples of each event so that the presentation of each event can be identified.

Tests
The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records in accordance with the evaluation activities associated with the functional requirements in this PP-Module. 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.

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

2.2.2 Communications (FCO)

FCO_NRO.1 Selective Proof of Origin

FCO_NRO.1
TSS
The evaluator shall ensure that the ST includes a description of authentication assertions, security associations or sensitive data associated with a claimant that is provided to a relying party, and a description of each protocol that carries such data.

The evaluator shall ensure that the ST includes a description of support for pass-through methods and the method it uses to mutually authenticate to, external authentication servers.

The evaluator shall verify that the descriptions indicate how the TSF authenticates itself to the external entities via those protocols, and that no data is passed via an unauthenticated protocol.

The evaluator shall verify that the ST describes how the TSF handles session interruptions and resumptions to ensure the relying party is able to associate data associated with a claimant to the authentication request by the relying party and the authenticator provided by the claimant.

Guidance
The evaluator shall ensure that any instructions for configuring the TSF to meet the requirements are provided.

Tests
The evaluator shall perform the following tests:

- **Test 1:**
  - Step 1: The evaluator shall establish a connection with the TSF from two trusted relying parties RP1 and RP2 and verify that each of RP1 and RP2 are able to authenticate the TOE.
  - Step 2: The evaluator shall initiate an authentication request for a claimant C1 via RP1, providing valid authentication data, and verify that RP1 receives an authentication assertion via the authenticated channel indicating C1 is authenticated.
  - Step 3: The evaluator shall initiate an authentication request for a claimant C2 via RP2, providing invalid authentication data and confirm that the TOE does not provide an authentication assertion indicating C2 is authenticated via the authenticated channel.
  - Step 4: The evaluator shall send correct authentication data associated with claimant C2 via RP1 without sending a new authentication request and observe that the TOE ignores the request.
- **Test 2:** (conditional on support for pass-through). The intent of this test is to demonstrate the TSF is able to authenticate to external entities for registered users over a pass-through method, and ignores requests for non-registered users.
  - Step 1: The evaluator shall follow AGD instructions to configure the TOE to connect to an external authentication server using pass-through functionality, and initiate a request from a trusted relying party that results in the TSF exercising pass-through functionality to authenticate a registered claimant.
  - Step 2: The evaluator shall observe that the TSF authenticates to the external authentication server prior to sending any authentication requests.
  - Step 3: The evaluator shall then follow AGD guidance to de-register the claimant at the TOE, and ensure the claimant is still registered at the external authentication server. The evaluator shall repeat initiation of the authentication request for the claimant, and observe that the TSF associates the identifier of the request by dropping the request without forwarding.

FCO_NRR.1 Selective Proof of Receipt

FCO_NRR.1
TSS
The evaluator shall ensure that the ST includes a description of each messaging protocol and the specific messages provided to a relying party in response to authentication requests, to include any affirmative and negative responses, and requests for additional information.

The evaluator shall verify that the descriptions indicate how the TSF indicates the identity of the claimant associated with any responses to a request.

The evaluator shall verify that the ST describes how the TSF handles session interruptions and resumptions to ensure the relying party is able to associate data associated with a claimant to the authentication request by the relying party and the authenticator provided by the claimant.

Guidance
The evaluator shall ensure that any instructions for configuring the TSF to meet the requirements are provided.

Tests
For each messaging protocol supported, the evaluator shall perform the following test:

- **Test 1:** The evaluator shall establish a connection between a trusted relying party and the TOE and send an authentication request for a registered claimant, in accordance with the messaging protocol standard. The evaluator shall confirm the TOE responds to each message sent by the relying party with a message that appropriately identifies the claimant and confirms receipt of the request.

2.2.3 Cryptographic Support (FCS)

FCS_CKM.3 Cryptographic Key Access

FCS_CKM.3
TSS
The evaluator shall verify the ST includes a description of all persistent secret and private keys used by the TSF to perform functions in this PP-Module. The evaluator shall verify the ST describes mechanism(s) used to prevent unauthorized exposure of keys.

Guidance
The evaluator shall verify that any configuration required to meet the requirements are described.

Tests
The intent of these tests is to ensure keys are not accessible using common interfaces and functionality of the TSF. It is not intended for the evaluator to attempt to cause a system crash in order to read keys and critical security parameters directly from memory or to modify functionality of the TSF.

The evaluator shall perform the following tests:

- **Test 1:** The evaluator shall attempt to export each key and critical security parameter using available interfaces and verify the mechanism is effective at preventing exposure of the key in plaintext.

- **Test 2:** The evaluator shall assume each of the privileged user roles and attempt to gain read access each of the keys and critical security parameters via available interfaces.

FCS_EAPTLS_EXT.1 EAP-TLS Protocol

FCS_EAPTLS_EXT.1

FCS_EAPTLS_EXT.1 EAP-TLS Protocol

FCS_EAPTLS_EXT.1
TSS
TBD

Guidance
TBD

Tests
TBD

FCS_CKM.2/PMK Cryptographic Key Distribution (PMK)

FCS_CKM.2/PMK
TSS
The evaluator will examine the TSS to determine that it describes how the PMK is transferred (that is, through what EAP attribute) to the TOE.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator will establish a session between the TOE and a RADIUS server according to the configuration guidance provided. The evaluator will then examine the traffic that passes between the RADIUS server and the TOE during a successful attempt to connect a wireless client to the TOE to determine that the PMK is not exposed.

2.2.4 Identification and Authentication (FIA)

FIA_8021X_EXT.1 802.1X Port Access Entity (Authenticator) Authentication

FIA_8021X_EXT.1
TSS
In order to show that the TSF implements the 802.1X-2010 standard correctly, the evaluator will ensure that the TSS contains the following information:

- The sections (clauses) of the standard that the TOE implements
- For each identified section, any options selected in the implementation allowed by the standards are specified
- For each identified section, any non-conformance is identified and described, including a justification for the non-conformance

Because the connection to the RADIUS server will be contained in an IPsec or RadSec (TLS) tunnel, the security mechanisms detailed in the RFCs identified in the requirement are not relied on to provide protection for these communications. Consequently, no extensive analysis of the RFCs is required. However, the evaluator will ensure that the TSS describes the measures (documentation, testing) that are taken by the product developer to ensure that the TOE conforms to the RFCs listed in this requirement.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator will perform the following tests:

- **Test 1:** The evaluator will demonstrate that a wireless client has no access to the test network. After successfully authenticating with a RADIUS server through the TOE, the evaluator will demonstrate that the wireless client does have access to the test network.
- **Test 2:** The evaluator will demonstrate that a wireless client has no access to the test network. The evaluator will attempt to authenticate using an invalid client certificate, such that the EAP-TLS negotiation fails. This should result in the wireless client still being unable to access the test network.
- **Test 3:** The evaluator will demonstrate that a wireless client has no access to the test network. The evaluator will attempt to authenticate using an invalid RADIUS certificate, such that the EAP-TLS negotiation fails. This should result in the wireless client still being unable to access the test network.

Note: Tests 2 and 3 above are not tests that "EAP-TLS works," although that is a by-product of the test. The

test is actually that a failed authentication (under two failure modes) results in denial of access to the network, which demonstrates the enforcement of FIA_8021X_EXT.1.3.

FIA_UAU.6 Re-Authenticating

FIA_UAU.6
TSS
There are no TSS evaluation activities for this component.

Guidance
There are no guidance evaluation activities for this component.

Tests
The evaluator will attempt to change their password as directed by the operational guidance. While making this attempt, the evaluator will verify that re-authentication is required.

If other re-authentication conditions are specified, the evaluator will cause those conditions to occur and verify that the TSF re-authenticates the authenticated user.

2.2.5 Security Management (FMT)

FMT_SMF.1/AccessSystem Specification of Management Functions (WLAN Access Systems)

FMT_SMF.1/AccessSystem
TSS
The evaluator will confirm that the TSS includes which security types (e.g., WPA3), authentication protocol (e.g., SAE), and frequency bands the WLAN AS supports. The evaluator will confirm that the TSS includes how connection attempts from clients that are not operating on an approved security type are handled.

Guidance
The evaluator will confirm that the operational guidance includes instructions for configuring the WLAN AS for each feature listed.

Tests

- **Test 1:** For each security type specified in the TSS, configure the network to the approved security type and verify that the client can establish a connection. Maintaining the same SSID, change the security type of the client to a non-approved security type and attempt to establish a connection. Verify that the connection was unsuccessful.
- **Test 2:** For each authentication protocol specified in the TSS, configure the network accordingly per the AGD. Verify that the client connection attempt is successful when using the correct client credentials and that the connection is unsuccessful when incorrect authentication credentials are used.
- **Test 3:** Configure the SSID to be broadcasted. Using a network sniffing tool, capture a beacon frame and confirm that the SSID is included. Configure the SSID to be hidden. Using a network sniffing tool, capture a beacon frame and confirm that the SSID is not listed.
- **Test 4:** The evaluator will configure the AS to operate in each of the selected frequency bands and verify using a network sniffing tool.
- **Test 5:** The evaluator will demonstrate that the client can establish a connection to the AS on the default power level. After disconnecting, the power level should be adjusted and then the client should be able to successfully connect to the AS again.

FMT_SMR_EXT.1 No Administration from Client

FMT_SMR_EXT.1
TSS
There are no TSS evaluation activities for this component.

Guidance
The evaluator will review the operational guidance to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration. The evaluator will confirm that the TOE does not permit remote administration from a wireless client by default.

Tests
The evaluator will demonstrate that after configuring the TOE for first use from the operational guidance, it is possible to establish an administrative session with the TOE on the “wired” portion of the device. They will then demonstrate that an identically configured wireless client that can successfully connect to the TOE cannot be used to perform administration.

2.2.6 Protection of the TSF (FPT)

FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1
TSS
The evaluator will examine the TSS to determine that the TOE's implementation of the fail secure functionality is documented. The evaluator will examine the TSS to ensure that it describes all failure conditions and how a secure state is preserved if any of these failures occur. The evaluator will ensure that the definition of a secure state is suitable to ensure the continued protection of any key material and user data.

Guidance
The evaluator will examine the operational guidance to verify that it describes applicable recovery instructions for each TSF failure state.

Tests
For each failure mode specified in the ST, the evaluator will ensure that the TOE attains a secure state (e.g., shutdown) after initiating each failure mode type.

2.2.7 TOE Access (FTA)

FTA_TSE.1 TOE Session Establishment

FTA_TSE.1
TSS
The evaluator will examine the TSS to determine that all of the attributes on which a client session can be denied are specifically defined.

Guidance
The evaluator will examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS.

Tests
For each supported attribute, the evaluator will perform the following test:

- **Test 1:** The evaluator successfully establishes a client session with a wireless client. The evaluator then follows the operational guidance to configure the system so that the client's access is denied based on a specific value of the attribute. The evaluator will then attempt to establish a session in contravention to the attribute setting (for instance, the client is denied WLAN access based upon the TOE interface (e.g. WLAN AP) it is connecting to, or that the client is denied access based upon the time-of-day or day-of-week it is attempting connection on). The evaluator will observe that the access attempt fails.

2.2.8 Trusted Path/Channels (FTP)

FTP_ITC.1/Client Inter-TSF Trusted Channel (WLAN Client Communications)

FTP_ITC.1/Client
This component is adequately evaluated when performing the evaluation activities for FTP_ITC.1 in the Network Device, version 2.2e base-PP.

2.3 Evaluation Activities for Optional SFRs

2.3.1 Cryptographic Support (FCS)

FCS_CKM.2/DISTRIB Cryptographic Key Distribution (802.11 Keys)

FCS_CKM.2/DISTRIB
TSS
The evaluator will examine the TSS to determine that it describes which keys are distributed outside the TOE, where they are sent, and the purpose for this transfer.

Guidance
If this function is dependent on TOE configuration, the evaluator will confirm that the operational guidance contains instructions for how to configure that the keys are adequately protected.

Tests
This requirement will be tested in conjunction with the tests for the cryptographic primitives, the secure protocols, and FPT_ITT.1 (Base-PP).

2.4 Evaluation Activities for Selection-Based SFRs

2.4.1 Cryptographic Support (FCS)

FCS_RADSEC_EXT.1 RadSec

FCS_RADSEC_EXT.1
TSS
The evaluator will verify that the TSS description includes the use of RADIUS over TLS, as described in RFC 6614.

If X.509v3 certificates is selected, the evaluator will ensure that the TSS description includes the use of client-side certificates for TLS mutual authentication.

Guidance
The evaluator will verify that any configuration necessary to meet the requirement must be contained in the guidance.

Tests
The evaluator will demonstrate the ability to successfully establish a RADIUS over TLS connection with a RADIUS server. This test will be performed with X.509v3 certificates if selected and performed with pre-shared keys if selected.

FCS_RADSEC_EXT.2 RadSec using Pre-Shared Keys

FCS_RADSEC_EXT.2
TSS
The evaluator will check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator will check the TSS to ensure that the ciphersuites specified are identical to those listed for this component. The evaluator will also verify that the TSS contains a description of the denial of old SSL and TLS versions.

The evaluator will examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality) and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.

Guidance
The evaluator will verify that any configuration necessary to meet the requirement must be contained in the guidance.

The evaluator will also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that RADIUS over TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

The evaluator will confirm the operational guidance contains instructions for either entering bit-based pre-shared keys or generating a bit-based pre-shared key (or both).

Tests

FCS_RADSEC_EXT.3 RadSec using Pre-Shared Keys and RSA

FCS_RADSEC_EXT.3
TSS
The evaluator will ensure that the TSS describes the client’s method of establishing all reference identifiers from the administrator and 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 TOE.

Guidance
The evaluator will verify that the operational guidance includes instructions for setting the reference identifier to be used for the purposes of certificate validation in TLS.

Tests
The evaluator will perform the following tests:

- **Test 1:** 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 2:** 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 3:** 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 will verify that the connection fails. The evaluator will repeat this test

for each supported SAN type.
- **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 5:** [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 does mandate the presence of the SAN extension, this test will be omitted.
- **Test 6:** [conditional] If wildcards are supported by the TOE, the evaluator will perform the following tests:
  - 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.
  - 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). The evaluator will 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.
  - 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 7:** [conditional] If wildcards are not supported by the TOE, the evaluator will present a server certificate containing a wildcard and verify that the connection fails.
- **Test 8:** [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.

2.4.2 Identification and Authentication (FIA)

FIA_PSK_EXT.1 Pre-Shared Key Composition

FIA_PSK_EXT.1
TSS
The evaluator will verify that the TSS describes

1. the protocols that can use pre-shared keys and that these are consistent with the selections made in FIA_PSK_EXT.1.1.
2. the allowable values for pre-shared keys and that they are consistent with the selections made in FIA_PSK_EXT.1.2.
3. the way bit-based pre-shared keys are procured and that it is consistent with the selections made in FIA_PSK_EXT.1.3.

Guidance
The evaluator will examine the operational guidance to determine that it provides guidance to administrators on the composition of strong text-based pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the range of lengths supported. The guidance must specify the allowable characters for pre-shared keys, and that list must be a superset of the list contained in FIA_PSK_EXT.1.2.

The evaluator will confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement or for generating a bit-based pre-shared key (or both).

Tests
The evaluator will also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case.

- **Test 1:** The evaluator will compose a pre-shared key of 22 characters that contains a combination of the allowed characters in accordance with the operational guidance and demonstrates that a successful protocol negotiation can be performed with the key.
- **Test 2:** [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator will repeat Test 1 using the minimum length; the maximum length; a length inside the allowable range; and invalid lengths beyond the supported range (both higher and lower). The minimum, maximum, and included length tests should be successful, and the invalid lengths must be rejected by the TOE.
- **Test 3:** [conditional]: If the TOE does not generate bit-based pre-shared keys, the evaluator will obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator will then demonstrate that a successful protocol negotiation can be performed with the key.

- **Test 4:** [conditional]: If the TOE does generate bit-based pre-shared keys, the evaluator will generate a bit-based pre-shared key of the appropriate length and use it according to the instructions in the operational guidance. The evaluator will then demonstrate that a successful protocol negotiation can be performed with the key.

2.5 Evaluation Activities for Objective SFRs

The PP-Module does not define any objective requirements.

3 Evaluation Activities for SARs

The PP-Module does not define any SARs beyond those defined within the base NDcPP to which it must claim conformance. It is important to note that a TOE that is evaluated against the PP-Module is inherently evaluated against this Base-PP as well. The NDcPP includes a number of Evaluation Activities associated with both SFRs and SARs. Additionally, the PP-Module includes a number of SFR-based Evaluation Activities that similarly refine the SARs of the Base-PPs. The evaluation laboratory will evaluate the TOE against the Base-PP and supplement that evaluation with the necessary SFRs that are taken from the PP-Module.

4 Required Supplementary Information

This Supporting Document has no required supplementary information beyond the ST, operational guidance, and testing.

Appendix A - References

Identifier	Title
[CC]	Common Criteria for Information Technology Security Evaluation - • Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. • Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. • Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020
[NDcPP SD]	Supporting Document - Evaluation Activities for Network Device cPP, Version 2.2, December 2019