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
1.2 Structure of the Document
1.3 Terms
1.3.1 Common Criteria Terms
1.3.2 Technical Terms
2 Evaluation Activities for SFRs
2.1 Collaborative Protection Profile for NDs
2.1.1 Modified SFRs
2.1.1.1 Identification and Authentication (FIA)
2.2 TOE SFR Evaluation Activities
2.2.1 Security Audit (FAU)
2.2.2 Communications (FCO)
2.2.3 Cryptographic Support (FCS)
2.2.4 Identification and Authentication (FIA)

2.2.5 Security Management (FMT)
2.2.6 TOE Access (FTA)
2.2.7 Trusted Path/Channels (FTP)
2.3 Evaluation Activities for Optional SFRs
2.3.1 Cryptographic Support (FCS)
2.4 Evaluation Activities for Selection-Based SFRs
2.4.1 Cryptographic Support (FCS)
2.4.2 Identification and Authentication (FIA)
2.5 Evaluation Activities for Objective SFRs
3 Evaluation Activities for SARs
4 Required Supplementary Information
Appendix A - References

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-PP)	Protection Profile used as a basis to build a PP-Configuration.

Collaborative Protection Profile (cPP)	A Protection Profile developed by international technical communities and approved by multiple schemes.
Common Criteria (CC)	Common Criteria for Information Technology Security Evaluation (International Standard ISO/IEC 15408).
Common Criteria Testing Laboratory	Within the context of the Common Criteria Evaluation and Validation Scheme (CCEVS), an IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.
Common Evaluation Methodology (CEM)	Common Evaluation Methodology for Information Technology Security Evaluation.
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.
	The output value generated by an authenticator. The ability to generate valid authenticator

Authenticator Output	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 to each of the keys and critical security parameters via available interfaces.

FCS_EAPTLS_EXT.1 EAP-TLS Protocol

FCS_EAPTLS_EXT.1
TSS
The evaluator shall examine the ST to ensure the EAP protocol is described in accordance with the claimed RFC and, for each supported mode, the evaluator ensures the ST describes the following:

- The mechanism to authenticate a claimant uses (D)TLS with client certificate authentication in combination with any other supported authenticator outputs, and any configurable features.
- The source of randomness meets FCS_RBG_EXT.1 for use in key and nonce generation for the underlying (D)TLS channel and supported authentication methods.

The evaluator shall also verify that the ST contains a description of the user access policy, including which authenticator outputs are required under the default configuration and which features of the user access policy are configurable.

Guidance
The evaluator shall ensure that the operational guidance includes any instructions for configuring the TOE to support the claimed functions.

If any features of the access control policy are configurable (e.g. the supported authentication mechanism), the evaluator shall confirm that the operational guidance describes how to configure these features.
Tests
The evaluator shall perform the following tests:

- **Test 1:** TLS/DTLS testing is performed as part of FCS_TLSS_EXT.1 and .2 or FCS_DTLSS_EXT.1 and .2. When TLS/DTLS cannot be invoked directly using available TOE interfaces, the test procedures are modified in the following manner:
  - When required to send a client handshake to the TOE, the evaluator shall establish a connection with the test relying party and sends the specified TLS client handshake messages in response to requests from the test relying party.
  - The evaluator ensures the test relying party encapsulates the TLS handshake messages received from the test client and forwards the EAP messages to the TOE. Alternatively the evaluator may use a test relying party to modify client handshake messages as specified. When required to observe TLS server responses produced by the TOE, the evaluator shall ensure the test relying party properly extracts the TLS messages from the EAP messages, and shall observe the response received at the test TLS client to verify that the TOE responds as indicated in test procedures. Alternatively, the evaluator may extract and reconstruct TLS responses received within the EAP messages received from the TOE at the test relying party.
- **Test 2:** EAP testing: For each EAP mode supported, the evaluator shall perform any configuration of the TOE necessary to select the desired mode according to AGD instructions, and perform the following tests:
  - Test 2a: The evaluator shall determine the user access policy enforced by the TOE (if the TOE has a configurable user access policy, the evaluator may configure the TOE according to operational guidance to require claimant authentication using only a certificate to simplify subsequent test procedures). The evaluator shall initiate an authentication request from a test relying party to the TOE for a valid claimant registered with the TOE. The evaluator shall observe that once the EAP identity is established, the TOE sends an EAP request indicating the expected EAP mode (EAP-TLS or EAP-TTLS) and having the start-bit set.

    The evaluator shall ensure a TLS client hello message from the valid claimant at a test client is EAP encapsulated by the test relying party and provided to the TOE. The evaluator shall observe that the TOE responds with an EAP encapsulated hello messages to include a certificate request message.

    The evaluator shall ensure the test client successfully completes the TLS handshake, and the test relying party properly encapsulates the TLS messages, to include the client finished message, and observes that the TOE that the TOE responds in a manner indicating the TLS channel was successfully established. Note – if the user access policy is to only require certificate verification, then the expected response is an EAP-success message. If the user access policy requires additional factors as supported under EAP-TTLS, additional EAP-TTLS messages are sent to the test relying party to request additional factors from the test client that are encrypted under the TLS tunnel established between the claimant and the TOE. In this case the evaluator observes these requests at the test client to confirm the certificate verification was successful.
  - Test 2b: The evaluator shall initiate an authentication request from the test relying party for a valid claimant registered with the TOE, different than the claimant used for Test 2a if performed. The evaluator shall send appropriate encapsulated TLS handshake messages to the TOE, to include a valid certificate response, but send an EAP-encapsulation of a modified client finished message to the TOE. The evaluator shall observe that the TOE does not send an EAP-success message; the TOE is allowed either to send an EAP-request message to initiate a new TLS handshake or an EAP-Failure message.
  - Test 2c [conditional on support for additional authentication factors under EAP-TTLS]: For each combination of authentication factors supported by the TOE’s user authentication policy, the

evaluator shall follow the operational guidance to configure the TOE's user access policy to require the desired combination. The evaluator shall initiate an authentication request from a test client with a registered claimant having valid credentials for all factors. The evaluator shall observe that the TOE responds to the authentication request with an exchange of EAP-requests to successfully establish a mutually authenticated TLS/DTLS tunnel and that on completion, the TOE provides additional EAP-requests that when decrypted at the test client results in prompts for additional factors.

For each additional factor in the combination, the evaluator shall input an incorrect value for requested authentication factors and observe that the TOE responds with an EAP-request that prompts the claimant to re-enter the value. The evaluator shall then input the correct value and observe that the TOE responds with an EAP-request resulting in a prompt for the next factor. The evaluator shall continue, in turn entering first, invalid, and then valid entries until all factors have been successfully provided. The evaluator shall confirm that on successful submission of valid factors, the TOE sends an EAP-Success message to the test relying party.

FCS_RADIUS_EXT.1 Authentication Protocol

FCS_RADIUS_EXT.1
TSS
The evaluator shall review the ST to ensure the supported protocols are described and that the description includes the following:

- Types of claimant-held keys that can be used by the relying party for key-holder verification in accordance with the supported EAP mode claimed in FCS_EAPTLS_EXT.1
- How information provided by the TOE to the relying party allows the relying party to perform key-holder verification using the key
- How key related information provided by the TOE is protected in transit to the relying party.

Guidance
The evaluator shall verify that all configurable features of the TSF are described and instructions are provided to meet the requirements.

Tests
The evaluator shall perform the following test in conjunction with testing for FCS_EAP-TLS_EXT.1 after successful authentication:

- **Test 1:** For each type of claimant held key supported, the evaluator shall confirm that communication between the test client and the test relying party encrypted using the indicated key is successful.

FCS_RADIUS_EXT.1 Authentication Protocol

FCS_RADIUS_EXT.1
TSS
The evaluator shall verify the TSS includes a description of protected key storage.

Guidance
The evaluator shall verify that the operational guidance includes any information needed to configure the TOE to meet this requirement.

Tests
There are no test EAs for this component.

2.2.4 Identification and Authentication (FIA)

FIA_AFL.1/AuthSvr Authentication Failure Handling (Claimant)

FIA_AFL.1/AuthSvr
TSS
The evaluator shall examine the TSS to verify that it contains a description of how successive unsuccessful authentication attempts by claimants are detected and tracked. The evaluator shall verify that the TSS describes the method by which the offending claimant is prevented from successfully being authenticated by the TOE, and the actions necessary to restore this ability.

Guidance
The evaluator shall examine the operational guidance to verify that it describes how to configure the threshold for unsuccessful claimant authentication attempts and how to perform any actions that affect claimants that are limited in this manner (e.g. instructions for configuring the lockout period or for manually unlocking the offending claimant).

Tests
The evaluator shall perform the following tests in conjunction with testing for FCS_EAPTLS_EXT.1 test 2a and, if applicable, test 2c for each claimant authentication method:

- **Test 1:** The evaluator shall follow the operational guidance to configure a number of failed attempts that will cause lockout behavior to be enforced against a claimant. The evaluator shall establish a registered user and provide invalid input for the authentication method repeatedly to reach the configured limit. The evaluator shall then observe the configured penalty is imposed.
- **Test 2:** If the administrator action selection is claimed in FIA_AFL.1.2/AuthSvr, the evaluator shall ensure that following the operational guidance for restoring access to a locked-out claimant will subsequently allow that claimant to be authenticated.

  If the time period selection is claimed in FIA_AFL.1.2/AuthSvr, the evaluator shall follow the operational guidance to configure a certain lockout time for claimants that are locked out due to excessive authentication failures. The evaluator shall cause a claimant to be locked out in this manner, wait for a time period that is just less than the configured value, and verify that an authentication attempt using valid credentials still does not result in successful access. The evaluator shall then repeat this behavior but wait for just after the configured time period has elapsed to show that an authentication attempt using valid credentials results in successful access.

FIA_X509_EXT.1/AuthSvr X.509 Certificate Validation (Claimant)

FIA_X509_EXT.1/AuthSvr
TSS
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.
Guidance
The evaluator shall ensure that instructions for any configurable features of the validation process are included. If the ST includes provisions for exception processing of certificate revocation status information, the evaluator shall ensure the operational guidance contains instructions on how the indicated options are configured.

If the TOE supports processing of the policy constraints extension and the TOE requires configuration to validate the policy of a claimant certificate, the evaluator shall verify that the operational guidance includes instructions for configuring this behavior.
Tests
The evaluator shall perform the following tests. The tests for the extendedKeyUsage rules, name constraints and policy constraints, if supported, are performed in conjunction with the uses that require those rules.

- **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
  - 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
  - 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 2:** The evaluator shall demonstrate that validating an expired certificate results in the function failing.
- **Test 3:** The evaluator shall test that the TOE can properly handle revoked certificates – conditional on the revocation method that is selected; if multiple methods are selected, then the test is repeated for each method. The evaluator tests revocation for each certificate in the trust chain which advertises certificate status information. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator shall then attempt the test with a certificate that will be revoked (for each method chosen in the selection) and verify that the validation function fails.
- **Test 4:** If any OCSP option is selected, the evaluator shall present a delegated OCSP 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 5:** [conditional] If the TOE supports EC certificates, then 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.
- **Test 6:** [conditional] If the TOE supports EC certificates, then the evaluator shall replace the intermediate certificate in the certificate chain for Test 5 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 5, 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 7:** The evaluator shall test the following name constraints:
  - Test 7a: For each name type supported, the evaluator shall establish a valid certificate for a registered entity. The evaluator shall ensure the certificate has a valid path length of at least 3, consisting of a trusted root, an issuing CA that is not a trust anchor, and the leaf certificate

representing the entity. The evaluator shall ensure that the leaf certificate includes a single name of the supported name type and no other DN or SAN entries. The evaluator shall initiate an application requiring authentication of that entity using the certificate and verify the TSF successfully authenticates the entity.
    - Test 7b: For each leaf certificate used in test 7a, the evaluator shall establish a new leaf certificate that includes the same name and name type, but which is issued by a different subordinate CA asserting an allowed-list that does not include the name for the name-type. The evaluator shall ensure the subordinate CA is included in a valid chain to the same trusted root. The evaluator shall initiate the same application attempt as in test 7a for the new certificate and observe that the TSF indicates the certificate is invalid.
    - Test 7c: For each leaf certificate used in test 7a, the evaluator shall establish a new leaf certificate that includes the same name and name type, but which is issued by a different subordinate CA asserting a deny-list matching the name for the name type. The evaluator shall ensure the subordinate CA is included in a valid certificate path to the same trusted root. The evaluator shall initiate the same application attempt as in test 7a using the new certificate and observe that the TSF indicates the certificate is invalid.
- **Test 8:** [conditional] If the TOE supports processing of the policy constraints extension, then for each distinct purpose and within the constraints indicated in the ST (claimant authentication and any other supported subject types), the evaluator shall follow the operational guidance as necessary to configure the TOE to require the subject's certificate to assert a specific certificate policy. The evaluator shall perform the following sub-tests:
    - Test 8a: The evaluator shall establish a certificate for the subject asserting the certificate policy OID required, issued by a Certification Authority also specifying the required certificate policy. The evaluator shall present the established certificate for authentication and verify that the TSF successfully validates the certificate.
    - Test 8b: The evaluator shall repeat test 8a using a certificate asserting the required policy but issued by a Certification Authority only asserting the 'anyPolicy' OID (value {2 5 29 32 0}) in its policy constraints extension. The evaluator shall observe that the TSF successfully validates the certificate.
    - Test 8c: [conditional] If the ST indicates support for the policy mapping extension, the evaluator shall repeat test 8a using a certificate asserting a new policy OID that does not match the required policy OID, which is issued by a CA asserting the new policy OID in the policy constraints extension, and which is in turn issued by a CA asserting the required OID in its certificate constraints extension and containing a policy mapping extension including the mapping of the asserted policy to the required policy. The evaluator shall observe that the TSF successfully validates the certificate.

      Note that installing a root CA trusted by the TOE with the required policy constraints and policy mapping extensions may be required if the TSF limits the path length of certificate chains.
    - Test 8d: [conditional] If the ST indicates support for both policy mapping and policy constraints extensions and also supports certificate chains of length 4 or more, the evaluator shall establish a certificate for the subject asserting a new policy OID that does not match the required policy OID, which is issued by a CA asserting the new policy OID, which in turn is issued by a CA which includes the policy mapping extension mapping the required policy OID to the new policy OID, which is in turn issued by a CA with the extension policy constraints with the inhibitPolicyMapping field having value 0. The evaluator shall present the certificate to the TSF for authentication and observe that the TSF indicates the certificate is invalid.
    - Test 8e: [conditional] If the ST indicates support for both policy mapping and policy constraints extensions, the evaluator shall select a policy OID not required for authentication in the TOE's current configuration. The evaluator shall establish a certificate for the subject that does not assert the (non-required) policy, which is issued by a CA also asserting the new policy OID, which in turn, is issued by a CA asserting the 'anyPolicy' OID and having a critical policy constraints extension with explicitPolicy field with value 0. The evaluator shall present the certificate to the TSF for authentication and observe that the TSF indicates the certificate is invalid.
    - Test 8f: The evaluator shall establish a certificate for the subject asserting the required policy but issued by a Certification Authority that does not include any certificate policy related extensions. The evaluator shall present the certificate for authentication and observe that the TSF indicates the certificate is invalid.
    - Test 8g: The evaluator shall establish a certificate for the subject asserting the required certificate policy issued by a Certification Authority that includes only asserts a single, non-matching policy OID in its policy related extensions (i.e. the CA certificate does not include the matching OID, 'anyPolicy' assertions or assert an OID that is mapped to the required OID via policy matching extensions by previous Certification Authorities in the certificate chain, if supported). The evaluator shall present the certificate to the TSF for authentication and observe the TSF indicates the certificate is invalid.
    - Test 8h: [conditional] If the ST indicates the inhibitAnyPolicy extension is supported, the evaluator shall establish a certificate for the subject asserting the required policy issued by a CA asserting the 'anyPolicy' OID, which is in turn issued by a CA with an inhibitAny extension with value 0. The evaluator shall present the certificate to the TSF for authentication and observe the TSF indicates the certificate is invalid.

      Note that installing a root CA trusted by the TOE with the inhibitAny extension may be required if the TSF limits the path length of certificate chains.

FIA_UAU.6 Re-Authenticating

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

Guidance
The evaluator shall ensure that the operational guidance includes instructions on how an administrator of the TOE can change their own password.

Tests
The evaluator will access the TOE using a particular administrative account and then attempt to change the password of that account 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 shall cause those conditions to occur and verify that the TSF re-authenticates the authenticated user.

2.2.5 Security Management (FMT)

FMT_SMF.1/AuthSvr Specification of Management Functions (Authentication Server)

FMT_SMF.1/AuthSvr
TSS
The evaluator shall verify that the TSS identifies all of the security-relevant management functions that apply to the security functions the TOE claims from this PP-Module.

Guidance
For each claimed management function, the evaluator shall ensure that the operational guidance contains instructions for how to configure the function.

Tests
For each claimed management function, the evaluator shall follow the operational guidance to configure the behavior of that function and ensure that applying the configuration settings have the intended effect. Note that some or all of these functions may be tested in the course of performing the test activities for other claimed SFRs.

2.2.6 TOE Access (FTA)

FTA_TSE.1 TOE Session Establishment

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

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

Tests
The evaluator shall successfully have a claimant be authenticated by the TOE. For each attribute claimed in the SFR, the evaluator shall configure the TOE to deny user access based on a specific value of that attribute. The evaluator shall then attempt to establish a new session in contravention to the attribute setting while still providing valid authentication data. The evaluator shall observe that the access attempt fails.

2.2.7 Trusted Path/Channels (FTP)

FTP_ITC.1/NAS Inter-TSF Trusted Channel (Relying Party Communications)

FTP_ITC.1/NAS
TSS
The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.
Guidance
The evaluator shall confirm that the guidance documentation contains instructions for establishing and reestablishing the allowed protocols with each authorized IT entity.
Tests
For each claimed trusted channel mechanism, the evaluator shall configure the TOE to interact with a relying party using that channel and verify using packet captures that the claimed mechanism is used.

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