# Draft Functional Package for IPsec


Version: 1.0
2022-03-11
**National Information Assurance Partnership**

## Revision History

| Version | Date | Comment |
|---|---|---|
| 1.0 | 2022-03-11 | Latest draft. |

## Contents

# 1 Introduction

## 1.1 Overview

Internet Protocol Security (IPsec) is a suite of open standards for ensuring private communications over public networks. It is typically used to encrypt Internet Protocol (IP) traffic between hosts in a network and to create a virtual private network (VPN). A VPN is a virtual network built on top of existing physical networks that provides a secure communications mechanism for data and control information transmitted between computers or networks. IPsec can also be used as a component that provides security for other internet protocols, such as the User Datagram Protocol (UDP).

The main components of IPsec are Encapsulating Security Protocol (ESP) and Internet Key Exchange (IKE). ESP is the protocol used to to transport encrypted and integrity-protected communications across the network. IKE is the protocol used to set up and manage IPsec connections.

This *Functional Package for IPsec* provides a collection of requirements and evaluation activities for IPsec implementations. The intent of this package is to provide PP, cPP, and PP-Module authors with a readily consumable collection of SFRs and EAs to be integrated into their documents. This Package can be used to to evaluate the IPsec functionality of TOEs that are not themselves VPN clients. For example, it could be used to evaluate the trusted channel functionality of an operating system that chooses to use IPsec rather than SSH or TLS to implement secure remote management. And of course, this Package can be used to encapsulate the IPsec-specific requirements in a VPN technology evaluation.

As such, this Package attempts to specify only requirements and evaluation activities for IPsec implementations as distinct from those for VPN implementations, such as VPN gateways and clients.

## 1.2 Terms

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

### 1.2.1 Common Criteria Terms

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

| | |
|---|---|
| Profile Configuration (PP-Configuration) | 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. |

### 1.2.2 Technical Terms

| | |
|---|---|
| Distinguished Name (DN) | A field in an X.509 certificate that uniquely identifies a person, organization, or business. |
| Elliptic Curve group modulo a Prime (ECP) | Elliptic Curve Group Modulo a Prime. |
| Encapsulating Security Payload (ESP) | The protocol used by IPsec to transport encrypted and integrity-protected communications across the network. |
| Extended Authentication (XAUTH) | An authentication scheme that supports an additional level of authentication by allowing the IPSec gateway to request extended authentication from remote users. |
| Extended Sequence Number (ESN) | An extension to the standard that allows IPsec to use 64-bit sequence numbers. |
| Extensible Authentication Protocol (EAP) | A framework for adding arbitrary authentication methods in a standardized way to any protocol. The most common EAP method used with IKEv2 is EAP-TLS. |
| Fully Qualified Domain Name (FQDN) | A domain name that specifies its exact location in the hierarchy of the Domain Name System (DNS). |
| Internet Key Exchange (IKE) | The protocol used by IPsec to set up and manage IPsec connections. This includes negotiating IPsec connection settings, authenticating endpoints to each other, defining the security parameters of IPsec-protected connections, and negotiating session keys. IKEv2 is the current version. |
| Internet Protocol Security (IPsec) | A suite of open standards for ensuring private communications over public networks. |
| Internet Security Association and Key Management Protocol (ISAKMP) | A protocol defined by [RFC 2408] for establishing Security Associations (SA) and cryptographic keys in an Internet environment. |
| Pre-Shared Key | A secret that is shared between two parties before it is used. |

(PSK)

| | |
|---|---|
| Security Association (SA) | The establishment of shared security attributes between two network entities to support secure communication. |
| Security Policy Database (SPD) | A set of rules that determines whether a packet is subject to IPsec processing. Each entry in the SPD represents a policy that defines how the set of traffic covered under the policy is to be processed. |
| User Datagram Protocol (UDP) | A communications protocol that is primarily used to establish low-latency and loss-tolerating connections between applications on the internet. |
| Virtual Private Network (VPN) | An extension of a private network across a public or shared network that allows users to exchange data as though they were connected directly to the private network. |

## 1.3 Compliant Targets of Evaluation

The Target of Evaluation (TOE) in this Functional Package (FP) is an IT product that includes an implementation of IPsec. Typically this is a VPN client or VPN gateway - for which IPsec functionality is fundamental. But the TOE could also be an operating system or other IT product for which IPsec functionality is ancillary. This FP describes the security functionality of IPsec in terms of [CC].

The contents of this FP must be appropriately incorporated into a PP, cPP, or PP-Module. When this Package is so incorporated, the ST must include selection-based requirements in accordance with the selections or assignments indicated in the incorporating document.

An ST must identify the applicable version of the PP, cPP, or PP-Module and this Functional Package in its conformance claims.

The PP, cPP, or PP-Module that incorporates this Package must typically include the following components in order to satisfy dependencies of this Package. It is the responsibility of the PP, cPP, or PP-Module author who incorporates this FP to ensure that dependence on these components is satisfied, either by the TOE or by assumptions about its Operational Environment.

Note that IKE defines its own key derivation function in [RFC 7296] (approved by NIST in [NIST SP 800-135 Rev. 1]). As a result, this Package does not require that the incorporating document claim a key derivation SFR (typically FCS_CKM_EXT.5 or FCS_CKM.5).

| Component | Explanation |
|---|---|
| FCS_CKM.1 | To support key generation for IPsec, the incorporating document must include the appropriate iterations of FCS_CKM.1 and specify the corresponding algorithms. |
| FCS_CKM.2 | To support key distribution for IPsec, the incorporating document must include FCS_CKM.2 and specify the corresponding algorithms. The standard requires that IKE implement a Diffie-Hellman key exchange. |
| FCS_COP.1 | To support the cryptography needed for IPsec communications, the incorporating document must include FCS_COP.1 (iterating as needed) to specify AES with corresponding key sizes and modes, digital signature generation and verification function (at least one of RSA or ECDSA), a cryptographic hash function, and a keyed-hash message authentication function. In particular, this Package requires that the TOE support AES-GCM-128 and AES-GCM-256 for ESP, and AES-CBC-128 and AES-CBC-256 for IKE. HMAC and SHA are required for the mandatory pseudo-random function and for integrity protections. |
| FCS_RBG_EXT.1 | To support random bit generation needed for IPsec key generation, the incorporating document must include a requirement that specifies the TOE's ability to invoke or provide random bit generation services, commonly identified as FCS_RBG_EXT.1. |
| FCS_TLS_EXT.1 | To support peer authentication over EAP, this Package requires support for the EAP-TLS or EAP-TTLS protocols. For this reason, the ST may need to incorporate the [Functional Package for TLS].<br><br>Required if:<br>• Pre-shared keys as specified in FIA_PSK_EXT.1 transmitted via EAP as specified in FCS_IPSEC_EXT.2, is selected from FCS_IPSEC_EXT.1.11 |
| FIA_PSK_EXT.1 | If the TOE uses pre-shared keys to establish IPsec connections, then this SFR must be claimed to specify requirements for the composition of pre-shared keys.<br><br>Required if:<br>• Pre-shared keys as specified in FIA_PSK_EXT.1 transmitted via means other than |

| | |
|---|---|
| | EAP, is selected from FCS_IPSEC_EXT.1.11<br>• Pre-shared keys as specified in FIA_PSK_EXT.1 transmitted via EAP as specified in FCS_IPSEC_EXT.2, is selected from FCS_IPSEC_EXT.1.11 |
| FIA_X509_EXT.1 | To support establishment of IPsec communications using a public key algorithm that includes X.509, the incorporating document must include FIA_X509_EXT.1. This documents requires that X.509v3 certificates be used in IKE peer authentication. |
| FIA_X509_EXT.2 | To support establishment of IPsec communications using a public key algorithm that includes X.509, the incorporating document must include FIA_X509_EXT.2 to specify the trusted channel protocols that use X.509 certificates. |
| FPT_STM.1 | To support establishment of IPsec communications using a public key algorithm that includes X.509, the incorporating document must include FPT_STM.1 or some other requirement that ensures reliable system time. Note however that support for time-based rekey thresholds is selectable and not mandatory.<br><br>Required if:<br>• length of time, is selected from FCS_IPSEC_EXT.1.7<br>• length of time, is selected from FCS_IPSEC_EXT.1.7<br>• length of time, is selected from FCS_IPSEC_EXT.1.7 |

# 2 Conformance Claims

**Conformance Statement**

An ST must claim exact conformance to this Package, as defined in the CC and CEM addenda for Exact Conformance, Selection-based SFRs, and Optional SFRs (dated May 2017).

**CC Conformance Claims**

This Package is conformant to Parts 2 (extended) and 3 (conformant) of Common Criteria Version 3.1, Revision 5.

**PP Claim**

This Package does not claim conformance to any Protection Profile.

**Package Claim**

This Package does not claim conformance to any packages.

# 3 Security Functional Requirements

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

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

## 3.1 Auditable Events for Mandatory SFRs

The auditable events specified in this Package are included in a Security Target if the incorporating PP, cPP, or PP-Module supports audit event reporting through FAU_GEN.1 and all other criteria in the incorporating document are met.

**Table 1: Auditable Events for Mandatory Requirements**

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|
| FCS_IPSEC_EXT.1 | Decisions to DISCARD or BYPASS network packets processed by the TOE. | Presumed identity of source subject.<br>The entry in the SPD that applied to the decision. |
| FCS_IPSEC_EXT.1 | Failure to establish an IPsec SA. | Identity of destination subject.<br>Reason for failure. |
| FCS_IPSEC_EXT.1 | Establishment/Termination of an IPsec SA. | Identity of destination subject.<br>Transport layer protocol, if applicable.<br>Source subject service identifier, if applicable.<br>Non-TOE endpoint of connection (IP address) for both successes and failures. |

## 3.2 Cryptographic Support (FCS)

### FCS_IPSEC_EXT.1 IPsec

FCS_IPSEC_EXT.1.1

The TSF shall implement IPsec as specified in [RFC 4301].

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

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

It is permissible for the TSF to receive configuration of IPsec behavior from an environmental source. For example, The SPD is established and populated through an administrative interface or application implemented by the entity that establishes the IPsec connection, such as a VPN gateway or client application. This interface or application is outside the scope of this FP.

FCS_IPSEC_EXT.1.2

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

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

FCS_IPSEC_EXT.1.3

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

FCS_IPSEC_EXT.1.4

The TSF shall implement the IPsec protocol ESP as defined by [RFC 4303] using the cryptographic algorithms

- *AES-GCM-128 as specified in [RFC 4106],*
- *AES-GCM-256 as specified in [RFC 4106],*

[**selection**:

- *AES-CBC with key size [**selection**: 128 bits, 256 bits] and message authentication using [**selection**: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] as specified in [RFC 3602],*
- *no other algorithms*

].

**Application Note:** [RFC 8221] requires that ESP support AES-CBC, AES-GCM, and NULL encryption. It recommends that AES-CCM be supported, but it is not permitted by this Package. If ESP traffic is encrypted using AES-CBC, then a separate authentication algorithm is required. [RFC 8221] requires HMAC-SHA-256 and HMAC-SHA-1, and recommends HMAC-SHA-512.

FCS_IPSEC_EXT.1.5

The TSF shall implement [**selection**:

- *IKEv1, using Main Mode for Phase I exchanges, as defined in [RFC 2407], [RFC 2408], [RFC 2409], [RFC 4109], [**selection**: [RFC 4304] for extended sequence numbers, no other RFCs for extended sequence numbers], [**selection**: [RFC 4868] for hash functions, no other RFCs for hash functions], and [**selection**: support for XAUTH, no support for XAUTH],*
- *IKEv2 as defined in [RFC 7296] [**selection**: with mandatory support for NAT traversal as specified in section 2.23, with no support for NAT traversal], and [RFC 8784], [RFC 8247], and [**selection**: [RFC 4868] for hash functions, no other RFCs for hash functions]*

].

**Application Note:** If the IPsec implementation is being used in a VPN application, then the ST author must claim "*with mandatory support for NAT traversal as specified in section 2.23*."

Validation Guidelines:

**Rule #1**: If "*IKEv1...*" is selected in FCS_IPSEC_EXT.1.5 then "*IKEv1...*" must be selected in FCS_IPSEC_EXT.1.7 and both "*IKEv1 Phase 1*" and "*IKEv1 Phase 2*" must be selected in FCS_IPSEC_EXT.13.

**Rule #2**: If "*IKEv2...*" is selected in FCS_IPSEC_EXT.1.5 then "*IKEv2...*" must be selected in FCS_IPSEC_EXT.1.7 and both "*IKEv2 IKE_SA*" and "*IKEv2 CHILD_SA*" must be selected in FCS_IPSEC_EXT.13.

**Rule #3**: If "*IKEv1...*" is selected in FCS_IPSEC_EXT.1.7 then "*IKEv1...*" must be selected in FCS_IPSEC_EXT.1.5.

**Rule #4**: If "*IKEv2...*" is selected in FCS_IPSEC_EXT.1.7 then "*IKEv2...*" must be selected in FCS_IPSEC_EXT.1.5.

**Rule #5**: If "*IKEv1 Phase 1*" or "*IKEv1 Phase 2*" is selected in FCS_IPSEC_EXT.1.13 then "*IKEv1...*" must be selected in FCS_IPSEC_EXT.1.5.

**Rule #6**: If "*IKEv2 IKE_SA*" or "*IKEv2 CHILD_SA*" is selected in FCS_IPSEC_EXT.1.13 then "*IKEv2...*" must be selected in FCS_IPSEC_EXT.5.

FCS_IPSEC_EXT.1.6

The TSF shall ensure the encrypted payload in the IKE protocol uses the cryptographic algorithms

- AES-CBC as specified in [RFC 6379] with key size [**selection**: *128 bits*, *256 bits*] and message authentication using [**selection**: *HMAC-SHA-1*, *HMAC-SHA-256*, *HMAC-SHA-384*, *HMAC-SHA-512*] as specified in [RFC 3602]

and [**selection**:

- *AES-GCM-128 as specified in [RFC 5282],*
- *AES-GCM-256 as specified in [RFC 5282],*
- *no other algorithm*

].

**Application Note:** [RFC 8247] requires that IKEv2 support AES-CBC-128/256 and recommends support for AES-GCM-128/256 for protecting IKE traffic.

FCS_IPSEC_EXT.1.7

The TSF shall ensure that [**selection**:

- *IKEv2 SA lifetimes can be configured based on [**selection**: number of packets/number of bytes, length of time] ,*
- *IKEv1 SA lifetimes [**selection**:*
  - *are configurable based on [**selection**: number of packets/number of bytes, length of time],*
  - *are fixed based on [**selection**: number of packets/number of bytes, length of time]*

  *]*

].

**Application Note:** The ST author is afforded a selection based on the version of IKE in their implementation.

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

The ST author chooses either the IKEv1 requirements or IKEv2 requirements (or both, depending on the selection in FCS_IPSEC_EXT.1.5. The IKEv1 requirement can be accomplished either by providing Authorized Administrator-configurable lifetimes (with appropriate instructions in documents mandated by AGD_OPE), or by “hard coding” the limits in the implementation. For IKEv2, there are no hard-coded limits, but in this case it is required that an administrator be able to configure the values. In general, instructions for setting the parameters of the implementation, including lifetime of the SAs, should be included in the operational guidance generated for AGD_OPE. It is appropriate to refine the requirement in terms of number of MB/KB instead of number of packets, as long as the TOE is capable of setting a limit on the amount of traffic that is protected by the same key (the total volume of all IPsec traffic protected by that key).

If the TOE is a VPN, then if a length of time is used for configuring SA lifetimes, then the assigned values should include at least one option that is 24 hours or less for Phase 1 SAs and 8 hours or less for Phase 2 SAs.

Validation Guidelines:

**Rule #1**: If "*IKEv1…*" is selected in FCS_IPSEC_EXT.1.5 then "*IKEv1…*" must be selected in FCS_IPSEC_EXT.1.7 and both "*IKEv1 Phase 1*" and "*IKEv1 Phase 2*" must be selected in FCS_IPSEC_EXT.13.

**Rule #2**: If "*IKEv2…*" is selected in FCS_IPSEC_EXT.1.5 then "*IKEv2…*" must be selected in FCS_IPSEC_EXT.1.7 and both "*IKEv2 IKE_SA*" and "*IKEv2 CHILD_SA*" must be selected in FCS_IPSEC_EXT.13.

**Rule #3**: If "*IKEv1…*" is selected in FCS_IPSEC_EXT.1.7 then "*IKEv1…*" must be selected in FCS_IPSEC_EXT.1.5.

**Rule #4**: If "*IKEv2…*" is selected in FCS_IPSEC_EXT.1.7 then "*IKEv2…*" must be selected in FCS_IPSEC_EXT.1.5.

FCS_IPSEC_EXT.1.8

The TSF shall ensure that all IKE protocols implement DH Groups

- 19 (256-bit Random ECP)
- 20 (384-bit Random ECP)

and [**selection**:

- *24 (2048-bit MODP with 256-bit POS),*
- *15 (3072-bit MODP),*
- *14 (2048-bit MODP),*
- *no other DH groups*

].

**Application Note:** The selection is used to specify additional DH groups supported. This applies to IKEv1 and IKEv2 exchanges. It should be noted that if

any additional DH groups are specified, they must comply with the requirements (in terms of the ephemeral keys that are established) listed in FCS_CKM.1.

Since the implementation may allow different Diffie-Hellman groups to be negotiated for use in forming the SAs, the assignments in FCS_IPSEC_EXT.1.9 and FCS_IPSEC_EXT.1.10 may contain multiple values. For each DH group supported, the ST author consults Table 2 in [NIST SP 800-57 Part 1 Rev. 5] to determine the “bits of security” associated with the DH group. Each unique value is then used to fill in the assignment (for 1.9 they are doubled; for 1.10 they are inserted directly into the assignment). For example, suppose the implementation supports DH group 14 (2048-bit MODP) and group 20 (ECDH using NIST curve P-384). From Table 2, the bits of security value for group 14 is 112, and for group 20 it is 192. For FCS_IPSEC_EXT.1.9, then, the assignment would read “[224, 384]” and for FCS_IPSEC_EXT.1.10 it would read “[112, 192]” (although in this case the requirement should probably be refined so that it makes sense mathematically).

Note that [RFC 6379] (2011) recommends using a "256-bit random ECP group" (Group 19) or a "384-bit random ECP group" (Group 20). [RFC 8247] (2017) requires support for DH Group 14 and recommends support for Group 19 in IKEv2. It discourages support for Groups 5, 2, 23, and 24. And forbids support for Groups 1 and 22.

FCS_IPSEC_EXT.1.9

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

FCS_IPSEC_EXT.1.10

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

**Application Note:** [RFC 7296] requires that all IKEv2 nonces be randomly generated and have a length of at least half the key size of the potentially negotiated pseudo-random function with the longest key size.

FCS_IPSEC_EXT.1.11

The TSF shall ensure that all IKE protocols perform peer authentication using

- [**selection**: *RSA*, *ECDSA*] with X.509v3 certificates that conform to [RFC 4945] as specified in FIA_X509_EXT.1, and

[**selection, choose one of**:

- *Pre-shared keys as specified in FIA_PSK_EXT.1 transmitted via EAP as specified in FCS_IPSEC_EXT.2*,
- *Pre-shared keys as specified in FIA_PSK_EXT.1 transmitted via means other than EAP*,
- *no other method*

]

**Application Note:** At least one public-key-based method for Peer Authentication using certificates is required in order to conform to this Package. One or more of the public key schemes is chosen by the ST author to reflect what is implemented (RSA or EDCSA). The ST author also ensures that appropriate FCS requirements reflecting the algorithms used (and key generation capabilities, if provided) are claimed to support those methods.

IKEv2 requires that RSA authentication be done using an RSA private key with the RSASSA-PKCS1-v1_5 signature scheme, see [RFC 7296] sec. 3.8. [RFC 8247] limits IKEv2 ECDSA authentication to "ECDSA with SHA-256 on the P-256 curve," "ECDSA with SHA-384 on the P-384 curve," and "ECDSA with SHA-512 on the P-521 curve." A more agile digital signature scheme for IKEv2 authentication is defined in [RFC 7427]. This Package requires only that RSA- or ECDSA-based digital signatures be used.

This Package does not permit use of Shared Key Message Integrity Code for peer authentication, although support is mandatory in the standard.

This Package requires that digital signature-based peer authentication use

X.509v3 certificates to verify the identity of the keys used in the signatures.

Peer authentication using certificates must be accomplished using mechanisms inherent in the IKE protocol. Authentication using pre-shared keys can be accomplished using methods specified in the IKE protocol, transmission through EAP, or through an out-of-band sharing mechanism.

If either "*Pre-shared keys as specified in FIA_PSK_EXT.1…*" selection is made, then the external requirement FIA_PSK_EXT.1 must be claimed. FIA_PSK_EXT.1 includes options for MFA solutions.

If "*Pre-shared keys as specified in FIA_PSK_EXT.1 transmitted via EAP as specified in FCS_IPSEC_EXT.2*," is selected, then FCS_IPSEC_EXT.2 must be claimed in addition to FIA_PSK_EXT.1. In the other selection, "*means other than EAP*" refers either to native IKE protocol mechanisms or to out-of-band mechanisms.

FCS_IPSEC_EXT.1.12

The TSF shall establish a SA only if the presented identifier in the received certificate matches the configured resource identifier, where the presented and reference identifiers are of the following fields and types:

[**selection**:

- *IP address*,
- *Fully Qualified Domain Name (FQDN)*,
- *user FQDN*,
- *Distinguished Name (DN)*

] and [**selection**:

- *[**assignment**: other supported reference identifier types]*,
- *no other reference identifier type*

] contained in a certificate does not match the expected values for the entity attempting to establish a connection.

**Application Note:** The reference identifier is the identifier the TOE expects to receive from the peer during IKE peer authentication. The presented identifier is the identifier that is contained within the peer certificate body. The TOE must support at least one of the following identifier types: IP address, Fully Qualified Domain Name (FQDN), user FQDN, or Distinguished Name (DN). In the future, the TOE will be required to support all of these identifier types. The TOE is expected to support as many IP address formats (IPv4 and IPv6) as IP versions supported by the TOE in general. The ST author may assign additional supported identifier types in the second selection.

At this time, only the comparison between the presented identifier in the peer's certificate and the peer's reference identifier is mandated by the testing below. However, in the future, this requirement will address two aspects of the peer certificate validation: 1) comparison of the peer's ID payload to the peer's certificate which are both presented identifiers, as required by RFC 4945 and 2) verification that the peer identified by the ID payload and the certificate is the peer expected by the TOE (per the reference identifier). At that time, the TOE will be required to demonstrate both aspects (i.e. that the TOE enforces that the peer's ID payload matches the peer's certificate which both match configured peer reference identifiers).

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

FCS_IPSEC_EXT.1.13

The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [**selection**: *IKEv1 Phase 1*, *IKEv2 IKE_SA*] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [**selection**: *IKEv1 Phase 2*, *IKEv2 CHILD_SA*] connection.

**Application Note:** The ST author chooses either or both of the IKE selections based on what is implemented by the TOE. Obviously, the IKE versions chosen should be consistent not only in this element, but with other choices for other

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

Validation Guidelines:

**Rule #1**: If "*IKEv1...*" is selected in FCS_IPSEC_EXT.1.5 then "*IKEv1...*" must be selected in FCS_IPSEC_EXT.1.7 and both "*IKEv1 Phase 1*" and "*IKEv1 Phase 2*" must be selected in FCS_IPSEC_EXT.13.

**Rule #2**: If "*IKEv2...*" is selected in FCS_IPSEC_EXT.1.5 then "*IKEv2...*" must be selected in FCS_IPSEC_EXT.1.7 and both "*IKEv2 IKE_SA*" and "*IKEv2 CHILD_SA*" must be selected in FCS_IPSEC_EXT.13.

**Rule #5**: If "*IKEv1 Phase 1*" or "*IKEv1 Phase 2*" is selected in FCS_IPSEC_EXT.1.13 then "*IKEv1...*" must be selected in FCS_IPSEC_EXT.1.5.

**Rule #6**: If "*IKEv2 IKE_SA*" or "*IKEv2 CHILD_SA*" is selected in FCS_IPSEC_EXT.1.13 then "*IKEv2...*" must be selected in FCS_IPSEC_EXT.5.

**Evaluation Activities**

*FCS_IPSEC_EXT.1*

***TSS***

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

***Guidance***

*The evaluator shall ensure that the operational guidance contains any appropriate information for ensuring that the IPsec implementation can be properly configured.*

***Tests***

*As a prerequisite for performing the Test EAs for the individual FCS_IPSEC_EXT.1 elements below, the evaluator must do the following:*
*The evaluator must create a test environment consisting of at least the components illustrated below. It is expected that the traffic generator will be used to construct network packets and will provide the evaluator with the ability manipulate fields in the ICMP, IPv4, IPv6, UDP, and TCP packet headers. The evaluator shall provide justification for any differences in the test environment.*

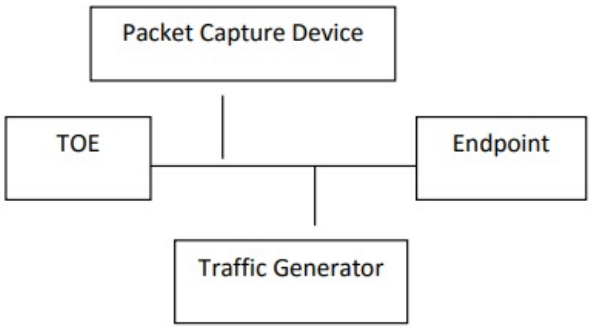


***Figure 1: Test Environment***

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

*FCS_IPSEC_EXT.1.1*

***TSS***

*The evaluator shall examine the TSS and ensure that it describes how the IPsec functionality is implemented.*

*The evaluator shall ensure that the TSS identifies any platform functionality that the TSF relies upon to support its IPsec implementation, if any (e.g. does it invoke cryptographic primitive functions from the platform's cryptographic library, enforcement of packet routing decisions by low-level network drivers).*

*The evaluator shall ensure that the TSS describes how the IPsec implementation interacts with the network stack of the platforms on which it can run (e.g., does the client insert itself within the stack via kernel modifications, does the IPsec implementation simply invoke APIs to gain access to network services).*

*The evaluator shall ensure that the TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes*

*the rules that are available and the resulting actions available after matching a rule. The TSS describes how the available rules and actions form the SPD using terms defined in [RFC 4301] such as BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet), and PROTECT (e.g., encrypt the packet). As noted in section 4.4.1 of [RFC 4301], the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.*

***Guidance***
*The evaluator shall examine the operational guidance to verify that it describes how the SPD is created and configured. If there is an administrative interface to the IPsec implementation, then the guidance describes how the administrator specifies rules for processing a packet. The description includes all three cases - a rule that ensures packets are encrypted/decrypted, dropped, and allowing a packet to flow in plaintext. The evaluator shall determine that the description in the operational guidance is consistent with the description in the TSS, and that the level of detail in the operational guidance is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.*

*If the IPsec implementation is configured by an external application, such as a VPN gateway, then the operational guidance should indicate this and provide a description of how IPsec is configured by the external application. The description should contain information as to how the SPD is established and set up in an unambiguous fashion. The description should also include what is configurable via the external application, how ordering of entries may be expressed, as well as the impacts that ordering of entries may have on the packet processing.*

*In either case, the evaluator ensures the description provided In the TSS is consistent with the capabilities and description provided in the operational guidance.*

***Tests***
*Depending on the implementation, the evaluator may be required to use a VPN gateway or some form of application to configure the client. For Test 2, the evaluator is required to choose an application that allows for the configuration of the full set of capabilities of the IPsec implementation. For example, if the IPsec implementation supports specification of wildcards, subnets, etc., it is unacceptable for the evaluator to specify only a single fully qualified IP address in the rule.*

*The evaluator shall perform the following tests:*

- ***Test 1:** The evaluator shall configure an SPD that is capable of the following: dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the IPsec endpoint with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule. The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed through without modification, were encrypted by the IPsec implementation.*
- ***Test 2:** The evaluator shall devise several tests that cover a variety of scenarios for packet processing. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and operational guidance. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the operational guidance.*

*FCS_IPSEC_EXT.1.2*
***TSS***
*The evaluator shall check the TSS to ensure it states that IPsec can be established to operate in tunnel mode or transport mode or both (as selected).*

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

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

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

- ***Test 1:** [conditional] If tunnel mode is selected, the evaluator uses the operational guidance*

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

- ***Test 2:*** *[conditional] If transport mode is selected, the evaluator uses the operational guidance to configure the TOE to operate in transport mode and also configures an IPsec peer to accept IPsec connections using transport mode. The evaluator configures the TOE and the endpoint device to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection from the TOE to connect to the remote endpoint. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.*
- ***Test 3:*** *[conditional] If both tunnel mode and transport mode are selected, the evaluator shall modify the testing for FCS_IPSEC_EXT.1 to include the supported mode for SPD PROTECT entries to show that they apply only to traffic that is transmitted or received using the indicated mode.*

*FCS_IPSEC_EXT.1.3*

***TSS***

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

***Guidance***

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

***Tests***

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

*FCS_IPSEC_EXT.1.4*

***TSS***

*The evaluator shall examine the TSS to verify that the algorithms AES-GCM-128 and AES-GCM-256 are implemented. If the ST author has selected either AES-CBC-128 or AES-CBC-256 in the requirement, then the evaluator verifies the TSS describes these as well. In addition, if either CBC mode is selected, the evaluator must ensure that the SHA-based HMAC algorithm conforms to the algorithms specified in the relevant iteration of FCS_COP.1 from the incorporating PP that applies to keyed-hash message authentication (often FCS_COP.1/KeyedHash or FCS_COP.1/HMAC).*

***Guidance***

*The evaluator checks the operational guidance to ensure it provides instructions on how the TOE is configured to use the algorithms selected in this component and whether this is performed through direct configuration, defined during initial installation, or defined by acquiring configuration settings from an environmental component.*

***Tests***

*The evaluator shall configure the TOE as indicated in the operational guidance configuring the TOE to using each of the AES-GCM-128 and AES-GCM-256 algorithms, and attempt to establish a connection using ESP. If the ST Author has selected either AES-CBC-128 or AES-CBC-256, the TOE is configured to use those algorithms and the evaluator attempts to establish a connection using ESP for those algorithms selected.*

*FCS_IPSEC_EXT.1.5*

***TSS***

*The evaluator shall examine the TSS to verify that IKEv1 or IKEv2 (or both) are implemented. If IKEv1 is implemented, the evaluator shall verify that the TSS indicates whether or not XAUTH is supported, and that aggressive mode is not used for IKEv1 Phase 1 exchanges (i.e. only main mode is used). It may be that these are configurable options.*

***Guidance***

*The evaluator shall check the operational guidance to ensure it instructs the administrator how to configure the TOE to use IKEv1 or IKEv2 (as selected), and uses the guidance to configure the TOE to perform NAT traversal for the test below. If XAUTH is implemented, the evaluator shall verify that the operational guidance provides instructions on how it is enabled or disabled.*

*If the TOE supports IKEv1, the evaluator shall verify that the operational guidance either asserts*

*that only main mode is used for Phase 1 exchanges, or provides instructions for disabling aggressive mode.*

***Tests***

- ***Test 1:*** *[conditional] If NAT traversal is supported, the evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and [RFC 7296], section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed. If the TOE supports IKEv1 with or without XAUTH, the evaluator shall verify that this test can be successfully repeated with XAUTH enabled and disabled in the manner specified by the operational guidance. If the TOE supports only IKEv1 with XAUTH, the evaluator shall verify that connections not using XAUTH are unsuccessful. If the TOE supports only IKEv1 without XAUTH, the evaluator shall verify that connections using XAUTH are unsuccessful.*
- ***Test 2:*** *[conditional] If the TOE supports IKEv1, the evaluator shall perform any applicable operational guidance steps to disable the use of aggressive mode and then attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator shall show that the TOE rejects a VPN gateway from initiating an IKEv1 Phase 1 connection in aggressive mode. The evaluator should then show that main mode exchanges are supported.*

*FCS_IPSEC_EXT.1.6*
***TSS***
*The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 or IKEv2 payload, and that the algorithms AES-CBC-128, AES-CBC-256 are specified, and if others are chosen in the selection of the requirement, those are included in the TSS discussion.*

***Guidance***
*The evaluator checks the operational guidance to ensure it provides instructions on how the TOE is configured to use the algorithms selected in this component and whether this is performed through direct configuration, defined during initial installation, or defined by acquiring configuration settings from an environmental component.*

***Tests***
*The evaluator shall use the operational guidance to configure the TOE (or to configure the Operational Environment to have the TOE receive configuration) to perform the following test for each ciphersuite selected for each version of IKE selected:*

*The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv1 or IKEv2 payload and establish a connection with a peer device, which is configured to accept the payload encrypted only using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation. The evaluator will confirm that the connection is successful by confirming that data can be passed through the connection once it is established. For example, the evaluator may connect to a webpage on the remote network and verify that it can be reached.*

*FCS_IPSEC_EXT.1.7*
***TSS***
*There are no TSS EAs for this requirement.*

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

***Tests***
*When testing this functionality, the evaluator needs to ensure that both IPsec endpoints are configured appropriately. From the RFC: "A difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying. If the two ends have the same lifetime policies, it is possible that both will initiate a rekeying at the same time (which will result in redundant SAs). To reduce the probability of this happening, the timing of rekeying requests SHOULD be jittered."*

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

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

- ***Test 1:*** *The evaluator shall configure a maximum lifetime in terms of the number of packets (or bytes) allowed following the operational guidance. The evaluator shall establish an SA and determine that once the allowed number of packets (or bytes) through this SA is exceeded, the connection is closed.*

- ***Test 2:*** *The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.*
- ***Test 3:*** *The evaluator shall perform a test similar to Test 2 for Phase 2 SAs, except that the lifetime will be 8 hours or less instead of 24 hours or less.*
- ***Test 4:*** *If a fixed limit for IKEv1 SAs is supported, the evaluator shall establish an SA and observe that the connection is closed after the fixed traffic or time value is reached.*

*FCS_IPSEC_EXT.1.8*
***TSS***
*The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.*

***Guidance***
*There are no AGD EAs for this requirement.*

***Tests***
*For each supported DH group, the evaluator shall test to ensure that all supported IKE protocols can be successfully completed using that particular DH group.*

*FCS_IPSEC_EXT.1.9*
***TSS***
*The evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating "x." The evaluator shall verify that the TSS indicates that the random number generated meets the requirements of this Package, and that the length of "x" meets the stipulations in the requirement.*

***Guidance***
*There are no AGD EAs for this requirement.*

***Tests***
*There are no test EAs for this requirement.*

*FCS_IPSEC_EXT.1.10*
***TSS***
*The evaluator shall check to ensure that, for all nonces generated for use in IKE, the TSS describes the process for generating nonces. The evaluator shall verify that the TSS indicates that the random number generated meets the requirements of this Package, and that the length of the nonce meets the stipulations in the requirement.*

***Guidance***
*There are no AGD EAs for this requirement.*

***Tests***
*There are no test EAs for this requirement.*

*FCS_IPSEC_EXT.1.11*
***TSS***
*The evaluator ensures that the TSS identifies RSA or ECDSA or both as being used to perform peer authentication.*

*The evaluator shall ensure that the TSS describes how the TOE compares the peer's presented identifier to the reference identifier. This description shall include whether the certificate presented identifier is compared to the ID payload presented identifier, which fields of the certificate are used as the presented identifier (DN, Common Name, or SAN) and, if multiple fields are supported, the logical order comparison. If the ST author assigned an additional identifier type, the TSS description shall also include a description of that type and the method by which that type is compared to the peer's presented certificate.*

*If any selection with pre-shared keys is chosen in the selection, the evaluator shall check to ensure that the TSS describes how those selections work in conjunction with authentication of IPsec connections.*

***Guidance***
*If any selection with "Pre-shared Keys" is selected, the evaluator shall check that the operational guidance describes any configuration necessary to enable any selected authentication mechanisms.*

*If any method other than "no other method" is selected, the evaluator shall check that the operational guidance describes any configuration necessary to enable any selected authentication mechanisms.*

*The evaluator ensures the operational guidance describes how to set up the TOE to use the cryptographic algorithms RSA or ECDSA, as selected.*

*In order to construct the environment and configure the TOE for the following tests, the evaluator will ensure that the operational guidance also describes how to configure the TOE to connect to a trusted CA, and ensure a valid certificate for that CA is loaded into the TOE as a trusted CA.*

*The evaluator shall also ensure that the operational guidance includes the configuration of the reference identifiers for the peer.*

***Tests***
*The following tests shall be repeated for each certificate-based peer authentication method supported:*

- ***Test 1:*** *The evaluator shall have the TOE generate a public-private key pair, and submit a CSR (Certificate Signing Request) to a CA (trusted by both the TOE and the peer VPN used to establish a connection) for its signature. The values for the DN (Common Name, Organization, Organizational Unit, and Country) will also be passed in the request. Alternatively, the evaluator may import to the TOE a previously generated private key and corresponding certificate.*
- ***Test 2:*** *The evaluator shall configure the TOE to use a private key and associated certificate signed by a trusted CA and shall establish an IPsec connection with the peer.*
- ***Test 3:*** *The evaluator shall test that the TOE can properly handle revoked certificates – conditional on whether CRL or OCSP is selected in FIA_X509_EXT.1; if both are selected, and then a test is performed for each method. The evaluator shall ensure that a valid certificate is used, and that the SA is established. The evaluator then attempts the test with a certificate that will be revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the TOE will not establish an SA*
- ***Test 4:*** *[conditional] For each selection made, the evaluator shall verify factors are required, as indicated in the operational guidance, to establish an IPsec connection with the server.*
  *For each supported identifier type (excluding DNs), the evaluator shall repeat the following tests:*
- ***Test 5:*** *For each field of the certificate supported for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the field in the peer's presented certificate and shall verify that the IKE authentication succeeds.*
- ***Test 6:*** *For each field of the certificate support for comparison, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to not match the field in the peer's presented certificate and shall verify that the IKE authentication fails.*
  *The following tests are conditional:*
- ***Test 7:*** *[conditional] If, according to the TSS, the TOE supports both Common Name and SAN certificate fields and uses the preferred logic outlined in the Application Note, the tests above with the Common Name field shall be performed using peer certificates with no SAN extension. Additionally, the evaluator shall configure the peer's reference identifier on the TOE to not match the SAN in the peer's presented certificate but to match the Common Name in the peer's presented certificate, and verify that the IKE authentication fails.*
- ***Test 8:*** *[conditional] If the TOE supports DN identifier types, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the subject DN in the peer's presented certificate and shall verify that the IKE authentication succeeds. To demonstrate a bit-wise comparison of the DN, the evaluator shall change a single bit in the DN (preferably, in an Object Identifier (OID) in the DN) and verify that the IKE authentication fails.* ***To demonstrate a comparison of DN values, the evaluator shall change any one of the four DN values and verify that the IKE authentication fails.***
- ***Test 9:*** *[conditional] If the TOE supports both IPv4 and IPv6 and supports IP address identifier types, the evaluator must repeat test 1 and 2 with both IPv4 address identifiers and IPv6 identifiers. Additionally, the evaluator shall verify that the TOE verifies that the IP header matches the identifiers by setting the presented identifiers and the reference identifier with the same IP address that differs from the actual IP address of the peer in the IP headers and verifying that the IKE authentication fails.*
- ***Test 10:*** *[conditional] If, according to the TSS, the TOE performs comparisons between the peer's ID payload and the peer's certificate, the evaluator shall repeat the following test for each combination of supported identifier types and supported certificate fields (as above). The evaluator shall configure the peer to present a different ID payload than the field in the peer's presented certificate and verify that the TOE fails to authenticate the IKE peer.*

*If EAP is used for peer authentication, then this is tested in FCS_IPSEC_EXT.2.*

*If the TOE implements peer authentication using pre-shared secrets, then generation of pre-shared secrets is tested in FIA_PSK_EXT.1, and peer authentication using pre-shared secrets is tested as follows:*

- ***Test 1:*** *The evaluator shall have the peer generate an AUTH value using the pre-shared secret and send it to the TOE. The TOE shall generate an AUTH value using the pre-shared secret and send it to the peer. The evaluator shall ensure that an IPsec connection is established.*

- ***Test 2:*** *The evaluator shall repeat the preceding test, but with the peer signing the AUTH value with a value other than the pre-shared secret. The evaluator shall ensure that an IPsec connection is not established.*
- ***Test 3:*** *The evaluator shall repeat the preceding test again, but with the peer signing an incorrectly calculated AUTH value with the pre-shared secret. The evaluator shall ensure that an IPsec connection is not established.*

*FCS_IPSEC_EXT.1.12*
*EAs for this element are tested through EAs for FCS_IPSEC_EXT.1.11.*
*FCS_IPSEC_EXT.1.13*
***TSS***
*The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the checks that are done when negotiating IKEv1 Phase 2 and IKEv2 CHILD_SA suites to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKE SA negotiation that is being protected.*

***Guidance***
*There are no AGD EAs for this requirement.*

***Tests***
*The evaluator follows the guidance to configure the TOE to perform the following tests for each version of IKE supported:*

- ***Test 1:*** *The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.*
- ***Test 2:*** *The evaluator shall attempt to establish an SA for ESP that selects an encryption algorithm with greater strength than that being used for the IKE SA (i.e., symmetric algorithm with a key size larger than that being used for the IKE SA). Such attempts should fail.*
- ***Test 3:*** *The evaluator shall attempt to establish an IKE SA using an algorithm that is not one of the supported algorithms and hash functions identified in the requirements. Such an attempt should fail.*
- ***Test 4:*** *The evaluator shall attempt to establish an SA for ESP (assumes the proper parameters where used to establish the IKE SA) that selects an encryption algorithm that is not identified in FCS_IPSEC_EXT.1.4. Such an attempt should fail.*

# Appendix A - Optional Requirements

As indicated in the introduction to this Package, the baseline requirements (those that must be performed by the TOE) are contained in the body of this Package. This appendix contains three other types of optional requirements that may be included in the ST, but are not required in order to conform to this Package. However, applied modules, packages and/or use cases may refine specific requirements as mandatory.

The first type (A.1 Strictly Optional Requirements) are strictly optional requirements that are independent of the TOE implementing any function. If the TOE fulfills any of these requirements or supports a certain functionality, the vendor is encouraged to include the SFRs in the ST, but are not required in order to conform to this Package.

The second type (A.2 Objective Requirements) are objective requirements that describe security functionality not yet widely available in commercial technology. The requirements are not currently mandated in the body of this Package, but will be included in the baseline requirements in future versions of this Package. Adoption by vendors is encouraged and expected as soon as possible.

The third type (A.3 Implementation-dependent Requirements) are dependent on the TOE implementing a particular function. If the TOE fulfills any of these requirements, the vendor must either add the related SFR or disable the functionality for the evaluated configuration.

## A.1 Strictly Optional Requirements

This Package does not define any Strictly Optional requirements.

## A.2 Objective Requirements

This Package does not define any Objective requirements.

## A.3 Implementation-dependent Requirements

This Package does not define any Implementation-dependent requirements.

# Appendix B - Selection-based Requirements

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

## B.1 Auditable Events for Selection-based Requirements

This document does not define any audit events for Selection-based Requirements.

## B.2 Cryptographic Support (FCS)

### FCS_IPSEC_EXT.2 IPsec Peer Authentication Over EAP

> ***The inclusion of this selection-based component depends upon selection in FCS_IPSEC_EXT.1.11.***

FCS_IPSEC_EXT.2.1

The TSF shall perform IPsec peer authentication over EAP using [**selection**:

- *EAP-TLS as specified in [RFC 5216]*,
- *EAP-TTLS as specified in [RFC 5281]*

] as updated by [RFC 8996] with TLS implemented using mutual authentication in accordance with the [Functional Package for TLS].

**Application Note:** EAP-TLS and EAP-TTLS with mutual authentication are the only two EAP methods allowed by this Package for IPsec peer authentication.

This Package allows EAP to be used for peer authentication using pre-shared keys only. Authentication using public-key cryptography and certificates must use IKEv2 mechanisms.

FCS_IPSEC_EXT.2.2

The TSF shall generate random values used in the EAP exchange using the RBG specified in FCS_RBG_EXT.1.

FCS_IPSEC_EXT.2.3

The TSF shall not forward a EAP-success response if the client certificate is not valid in accordance with FIA_X509_EXT.1.

FCS_IPSEC_EXT.2.4

The TSF shall use the MSK from the EAP-TLS or EAP-TTLS response as the IKEv2 shared secret in the authentication payload.

**Evaluation Activities**

*FCS_IPSEC_EXT.2*
***TSS***
*The evaluator shall verify that the TSS describes the use of EAP options for each of the selected peer authentication mechanisms, that TLS with mutual authentication is used, that the random values are from an appropriate source, and that the TSS describes that the EAP MSK is derived from the TLS master key and is used as the IKEv2 shared key.*

***Guidance***
*The evaluator shall verify that the guidance documents describe any configurable features of the EAP or TLS functionality, including instructions for configuration of the authenticators and registration processes for clients.*

***Tests***
*For each supported EAP method claimed in FCS_IPSEC_EXT.2.1 the evaluator shall perform the following tests:*

- ***Test 1:*** *The evaluator shall follow AGD guidance to configure the TSF to use the EAP method claimed. The evaluator shall follow AGD guidance to configure the TSF to use the authentication method claimed and, for EAP-TTLS, register an endpoint with appropriate key material required for the authentication method. The evaluator shall establish a connection using a test endpoint with a valid certificate and, for EAP-TTLS, configured to provide a correct value for the configured authenticator. The evaluator shall observe that the connection is successful.*
- ***Test 2:*** *[conditional] If EAP-TTLS is supported, the evaluator shall cause the test endpoint*

*with a valid certificate to send an invalid authenticator for the claimed authentication method:*

- *For HOTP, replay a HOTP value sent previously,*
- *For TOTP or other PSK, modify a byte of the properly constructed value,*

*and observe that the TSF aborts the connection.*

- ***Test 3:** The evaluator shall follow AGD guidance to configure the TSF to use a supported EAP method and register the user with key material for required for a supported authentication method. The evaluator shall configure a test endpoint to respond to an IKEv2 exchange with EAP-request, providing valid phase 1 handshake and valid TLS handshake, but computing the phase 2 shared key using standard (non-EAP) methods. The evaluator shall initiate an IPsec connection between the test endpoint and the TSF, and observe that the TSF aborts the connection.*

# Appendix C - Validation Guidelines

This appendix contains "rules" specified by the PP Authors that indicate whether certain selections require the making of other selections in order for a Security Target to be valid. For example, selecting "HMAC-SHA-3-384" as a supported keyed-hash algorithm would require that "SHA-3-384" be selected as a hash algorithm.

This appendix contains only such "rules" as have been defined by the PP Authors, and does not necessarily represent all such dependencies in the document.

## Rule #1

If "*IKEv1...*" is selected in FCS_IPSEC_EXT.1.5 then "*IKEv1...*" must be selected in FCS_IPSEC_EXT.1.7 and both "*IKEv1 Phase 1*" and "*IKEv1 Phase 2*" must be selected in FCS_IPSEC_EXT.13.

| | |
|---|---|
| IF | From FCS_IPSEC_EXT.1.5:<br>* select IKEv1, using Main Mode for Phase I exchanges, as defined in [RFC 2407], [RFC 2408], [RFC 2409], [RFC 4109], [**selection**: *[RFC 4304] for extended sequence numbers, no other RFCs for extended sequence numbers*], [**selection**: *[RFC 4868] for hash functions, no other RFCs for hash functions*], and [**selection**: *support for XAUTH, no support for XAUTH*] |

| | |
|---|---|
| THEN | From FCS_IPSEC_EXT.1.7:<br>* select IKEv1 SA lifetimes [**selection**:<br>• *are configurable based on [**selection**: number of packets/number of bytes, length of time],*<br>• *are fixed based on [**selection**: number of packets/number of bytes, length of time]*<br>]<br>From FCS_IPSEC_EXT.1.13:<br>* select IKEv1 Phase 1<br>* select IKEv1 Phase 2 |

## Rule #2

If "*IKEv2...*" is selected in FCS_IPSEC_EXT.1.5 then "*IKEv2...*" must be selected in FCS_IPSEC_EXT.1.7 and both "*IKEv2 IKE_SA*" and "*IKEv2 CHILD_SA*" must be selected in FCS_IPSEC_EXT.13.

| | |
|---|---|
| IF | From FCS_IPSEC_EXT.1.5:<br>* select IKEv2 as defined in [RFC 7296] [**selection**: *with mandatory support for NAT traversal as specified in section 2.23, with no support for NAT traversal*], and [RFC 8784], [RFC 8247], and [**selection**: *[RFC 4868] for hash functions, no other RFCs for hash functions*] |

| | |
|---|---|
| THEN | From FCS_IPSEC_EXT.1.7:<br>* select IKEv2 SA lifetimes can be configured based on [**selection**: *number of packets/number of bytes, length of time*]<br>From FCS_IPSEC_EXT.1.13:<br>* select IKEv2 IKE_SA<br>* select IKEv2 CHILD_SA |

## Rule #3

If "*IKEv1...*" is selected in FCS_IPSEC_EXT.1.7 then "*IKEv1...*" must be selected in FCS_IPSEC_EXT.1.5.

| | |
|---|---|
| IF | From FCS_IPSEC_EXT.1.7:<br>* select IKEv1 SA lifetimes [**selection**:<br>• *are configurable based on [**selection**: number of packets/number of bytes, length of time],*<br>• *are fixed based on [**selection**: number of packets/number of bytes, length of time]*<br>] |

| | |
|---|---|
| THEN | From FCS_IPSEC_EXT.1.5:<br>* select IKEv1, using Main Mode for Phase I exchanges, as defined in [RFC 2407], [RFC 2408], [RFC 2409], [RFC 4109], [**selection**: *[RFC 4304] for extended sequence numbers, no other RFCs for extended sequence numbers*], [**selection**: *[RFC 4868] for hash functions, no other RFCs for hash functions*], and [**selection**: *support for XAUTH, no support for XAUTH*] |

## Rule #4

If "*IKEv2...*" is selected in FCS_IPSEC_EXT.1.7 then "*IKEv2...*" must be selected in FCS_IPSEC_EXT.1.5.

| | |
|---|---|
| IF | From FCS_IPSEC_EXT.1.7:<br>* select IKEv2 SA lifetimes can be configured based on [**selection**: *number of packets/number of bytes, length of time*] |

| | |
|---|---|
| THEN | From FCS_IPSEC_EXT.1.5:<br>* select IKEv2 as defined in [RFC 7296] [**selection**: *with mandatory support for NAT traversal as specified in section 2.23, with no support for NAT traversal*], and [RFC 8784], [RFC 8247], and [**selection**: *[RFC 4868] for hash functions, no other RFCs for hash functions*] |

## Rule #5

If "*IKEv1 Phase 1*" or "*IKEv1 Phase 2*" is selected in FCS_IPSEC_EXT.1.13 then "*IKEv1...*" must be selected in FCS_IPSEC_EXT.1.5.

| | | |
|---|---|---|
| IF | DECISION A | **CHOICE A1**<br>From FCS_IPSEC_EXT.1.13:<br>* select IKEv1 Phase 1 |
| | | **CHOICE A2**<br>From FCS_IPSEC_EXT.1.13:<br>* select IKEv1 Phase 2 |

| | |
|---|---|
| THEN | From FCS_IPSEC_EXT.1.5:<br>* select IKEv1, using Main Mode for Phase I exchanges, as defined in [RFC 2407], [RFC 2408], [RFC 2409], [RFC 4109], [**selection**: *[RFC 4304] for extended sequence numbers, no other RFCs for extended sequence numbers*], [**selection**: *[RFC 4868] for hash functions, no other RFCs for hash functions*], and [**selection**: *support for XAUTH, no support for XAUTH*] |

## Rule #6

If "*IKEv2 IKE_SA*" or "*IKEv2 CHILD_SA*" is selected in FCS_IPSEC_EXT.1.13 then "*IKEv2...*" must be selected in FCS_IPSEC_EXT.5.

| | | |
|---|---|---|
| IF | DECISION B | **CHOICE B1**<br>From FCS_IPSEC_EXT.1.13:<br>* select IKEv2 IKE_SA |
| | | **CHOICE B2**<br>From FCS_IPSEC_EXT.1.13:<br>* select IKEv2 CHILD_SA |

| | |
|---|---|
| THEN | From FCS_IPSEC_EXT.1.5:<br>* select IKEv2 as defined in [RFC 7296] [**selection**: *with mandatory support for NAT traversal as specified in section 2.23, with no support for NAT traversal*], and [RFC 8784], [RFC 8247], and [**selection**: *[RFC 4868] for hash functions, no other RFCs for hash functions*] |

# Appendix D - Acronyms

| Acronym | Meaning |
|---|---|
| Base-PP | Base Protection Profile |
| CC | Common Criteria |
| CEM | Common Evaluation Methodology |
| DN | Distinguished Name |
| EAP | Extensible Authentication Protocol |
| ECP | Elliptic Curve group modulo a Prime |
| EP | Extended Package |
| ESN | Extended Sequence Number |
| ESP | Encapsulating Security Payload |
| FP | Functional Package |
| FQDN | Fully Qualified Domain Name |
| IKE | Internet Key Exchange |
| IPsec | Internet Protocol Security |
| ISAKMP | Internet Security Association and Key Management Protocol |
| OE | Operational Environment |
| PP | Protection Profile |
| PP-Configuration | Protection Profile Configuration |
| PP-Module | Protection Profile Module |
| PSK | Pre-Shared Key |
| SA | Security Association |
| SAR | Security Assurance Requirement |
| SFR | Security Functional Requirement |
| SPD | Security Policy Database |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| TSFI | TSF Interface |
| TSS | TOE Summary Specification |
| UDP | User Datagram Protocol |
| VPN | Virtual Private Network |
| XAUTH | Extended Authentication |
| cPP | Collaborative Protection Profile |

# Appendix E - Bibliography


| Identifier | Title |
|---|---|
| [Functional Package for TLS] | Functional Package for Transport Layer Security (TLS) |
| [NIST SP 800-135 Rev. 1] | Recommendation for Existing Application-Specific Key Derivation Functions |
| [NIST SP 800-57 Part 1 Rev. 5] | Recommendation for Key Management: Part 1 - General |
| [RFC 2407] | The Internet IP Security Domain of Interpretation for ISAKMP |
| [RFC 2408] | Internet Security Association and Key Management Protocol (ISAKMP) |
| [RFC 2409] | The Internet Key Exchange (IKE) |
| [RFC 3602] | The AES-CBC Cipher Algorithm and Its Use with IPsec |
| [RFC 4106] | The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP) |
| [RFC 4109] | Algorithms for Internet Key Exchange version 1 (IKEv1) |
| [RFC 4301] | Security Architecture for the Internet Protocol |
| [RFC 4303] | IP Encapsulating Security Payload (ESP) |
| [RFC 4304] | Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP) |
| [RFC 4868] | Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec |
| [RFC 4945] | The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX |
| [RFC 5216] | The EAP-TLS Authentication Protocol |
| [RFC 5281] | Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0) |
| [RFC 5282] | Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol |
| [RFC 6379] | Suite B Cryptographic Suites for IPsec |
| [RFC 7296] | Internet Key Exchange Protocol Version 2 (IKEv2) |
| [RFC 7427] | Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2) |
| [RFC 8221] | Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH) |
| [RFC 8247] | Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2) |
| [RFC 8784] | Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security |
| [RFC 8996] | Deprecating TLS 1.0 and TLS 1.1 |
| [CC] | Common Criteria for Information Technology Security Evaluation - <br>• Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017. <br>• Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017. <br>• Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017. |