Functional Package for Secure Shell (SSH)

This page is best viewed with JavaScript enabled!

Version: 1.0
2020-01-05
National Information Assurance Partnership

Revision History

Version	Date	Comment
1.0	2021-01-05	DRAFT: First publication as a Functional Package

Contents

1 Introduction

1.1 Overview

Secure Shell (SSH) is a protocol for secure remote login and other secure network services over an untrusted network.SSH software can act as a client, server, or both.

This *Functional Package for Secure Shell* defines functional requirements for the implementation of theSSH protocol. The requirements are intended to improve the security of products by enabling their evaluation.

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 aPP-Configuration.
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 theTOE 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 oneBase-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 Protection Profiles.
Security Assurance Requirement (SAR)	A requirement to assure the security of theTOE.
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.

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.
Target of Evaluation (TOE)	The product under evaluation.

1.2.2 Technical Terms

Secure Shell (SSH)	Cryptographic network protocol for initiating text-based shell sessions on remote systems.

1.3 Compliant Targets of Evaluation

The Target of Evaluation (TOE) in this Functional Package is a product which acts as an SSH client, SSH server, or both. This FP describes the extended security functionality of SSH in terms of [CC].

The contents of this Functional Package must be appropriately combined with a PP or PP-Module. When a PP or PP-Module instantiates this Package, the Package must include selection-based requirements in accordance with the selections or assignments indicated in the PP or PP-Module.

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

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

Component	Explanation
FCS_CKM.1	To support key generation for SSH, the PP or PP-Module must include FCS_CKM.1 and specify the corresponding algorithm.
FCS_CKM.2	To support key establishment for SSH, the PP or PP-Module must include FCS_CKM.2 and specify the corresponding algorithm.
FCS_COP.1	To support the cryptography needed for SSH communications, the PP or PP-Module 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, the PP or PP-Module must support AES-CTR as defined in NIST SP 800-38A with key sizes of both 128 and 256 bits.
FCS_RBG_EXT.1	To support random bit generation needed for SSH key generation, the PP or PP-Module 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.
FIA_X509_EXT.1	To support establishment of SSH communications using a public key algorithm that includes X.509, the PP or PP-Module must include FIA_X509_EXT.1. Note however that support for X.509 is selectable and not mandatory.
FIA_X509_EXT.2	To support establishment of SSH communications using a public key algorithm that includes X.509, the PP or PP-Module must include FIA_X509_EXT.2. Note however that support for X.509 is selectable and not mandatory.
FPT_STM.1	To support establishment of SSH communications using a public key algorithm that includes X.509, the PP or PP-Module 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.

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 or PP-Module supports audit event reporting through FAU_GEN.1 and all other criteria in the incorporating PP or PP-Module are met.

Table 1: Auditable Events for Mandatory SFRs

Requirement	Auditable Events	Additional Audit Record Contents
FCS_SSH_EXT.1	No events specified	

3.2 Cryptographic Support (FCS)

FCS_SSH_EXT.1 SSH Protocol

FCS_SSH_EXT.1.1
The TOE shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254 and [**selection**: *5647*, *5656*, *6187*, *6668*, *8332*, *no other RFCs*] as a [**selection**: *client*, *server*].
Application Note:

The ST author selects which of the additional RFCs to which conformance is being claimed. An SSH product can implement additional RFCs, but only those listed in the selection can be claimed as conformant under CC. The RFC selections for this requirement need to be consistent with selections in later elements of this Functional Package (e.g., cryptographic algorithms permitted).

RFC 4253 indicates that certain cryptographic algorithms are "REQUIRED." This means that from the Internet Engineering Task Force's (IETF's) perspective the implementation must include support, not that the algorithms must be enabled for use. For the purposes of this SFR's evaluation activity and this Functional Package overall, it is not necessary to ensure that algorithms listed as "REQUIRED" by the RFC but not listed in later elements of this Functional Package are actually implemented.

RFC 5647 must be selected when AEAD_AES_128_GCM or AEAD_AES_256_GCM is selected as an encryption algorithm in FCS_SSHC_EXT.1.3 or FCS_SSHS_EXT.1.3 and as a MAC algorithm in FCS_SSHC_EXT.1.5 or FCS_SSHS_EXT.1.5.

RFC 5656 must be selected when ecdsa-sha2-nistp256 or ecdsa-sha2-nistp384 is selected as a public key algorithm in FCS_SSHC_EXT.1.4 or FCS_SSHS_EXT.1.4, or when ecdh-sha2-nistp256, ecdh-sha2-nistp384, or ecdh-sha2-nistp521 is selected as a key exchange algorithm in FCS_SSHC_EXT.1.6 or FCS_SSHS_EXT.1.6.

RFC 6187 must be selected when x509v3-ecdsa-sha2-nistp256 or x509v3-ecdsa-sha2-nistp384 is selected as a public key algorithm in FCS_SSHC_EXT.1.4 or FCS_SSHS_EXT.1.4.

RFC 6668 must be selected when hmac-sha2-256 or hmac-sha2-512 is selected as a MAC algorithm in FCS_SSHC_EXT.1.5 or FCS_SSHS_EXT.1.5.

RFC 8332 must be selected when rsa-sha2-256 or rsa-sha2-512 is selected as a public key algorithm in FCS_SSHC_EXT.1.4 or FCS_SSHS_EXT.1.4.

If "client" is selected, then the ST must include FCS_SSHC_EXT.1.

If "server" is selected, then the ST must include FCS_SSHS_EXT.1.

Evaluation Activity
TSS
The evaluator shall ensure that the selections indicated in the ST are consistent with selections in the dependent components.
Guidance
There are no guidance evaluation activities for this component.

Tests
There are no test evaluation activities for this component.

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 theTOE implementing any function. If the TOE fulfills any of these requirements or supports a certain functionality, the vendor is encouraged to included 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-based Requirements) are dependent on the TOE implementing a particular function. If the TOE fulfills any of these requirements, the vendor must either add the relatedSFR 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-based Requirements

This Package does not define any Implementation-based requirements.

Appendix B - Selection-based Requirements

As indicated in the introduction to this Package, the baseline requirements (those that must be performed by theTOE 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

The auditable events in the table below are included in a Security Target if both the associated requirement is included and the incorporating PP or PP-Module supports audit event reporting through FAU_GEN.1 and any other criteria in the incorporating PP or PP-Module are met.

Table 2: Auditable Events for Selection-based Requirements
RequirementAuditable EventsAdditional Audit Record Contents

FCS_SSHC_EXT.1

[selection: *Failure to establish a session, None*]Reason for failure.

Non-TOE endpoint of attempted connection (IP Address).

FCS_SSHC_EXT.1**[selection:** *Establishment of a session, None*]Non-TOE endpoint of connection (IP Address).

FCS_SSHC_EXT.1**[selection:** *Termination of a session, None*]Non-TOE endpoint of connection (IP Address).

FCS_SSHS_EXT.1**[selection:** *Failure to establish a session, None*]Reason for failure.

Non-TOE endpoint of attempted connection (IP Address).

FCS_SSHS_EXT.1**[selection:** *Establishment of a session, None*]Non-TOE endpoint of connection (IP Address).

FCS_SSHS_EXT.1**[selection:** *Termination of a session, None*]Non-TOE endpoint of connection (IP Address).

~~B.2 Cryptographic Support (FCS)~~

~~FCS_SSHC_EXT.1~~ SSH Protocol - Client

~~The inclusion of this~~ This is a selection-based component. Its inclusion depends upon ~~a~~ selection ~~in~~ from FCS_SSH_EXT.1.1.

FCS_SSHC_EXT.1.1

The SSH client shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based and [**selection**: *password-based*, *no other method*].

Evaluation Activity

TSS

The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication and that this list conforms to FCS_SSHC_EXT.1.4. The evaluator shall also ensure that password-based authentication methods, if supported, are described.

Guidance

If the SSH client supports password-based authentication, the evaluator shall examine the guidance to determine that it includes instructions on how to configure whether the TSF uses password-based or public key-based authentication.

Tests

- ***Test 1:** The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection to an SSH server. Any configuration activities required to support this test shall be performed according to instructions in the guidance documentation.*
- ***Test 2:** [conditional]: TOE supports password-based authentication] Using the guidance documentation, the evaluator shall configure the TOE to perform password-based authentication to an SSH server, and demonstrate that a user can be successfully authenticated by the TOE to an SSH server using a password as an authenticator.*

FCS_SSHC_EXT.1.2

The SSH client shall ensure that, as described in RFC 4253, packets greater than [**assignment**: number of bytes] bytes in an SSH transport connection are dropped.

Application Note: RFC 4253 provides for the acceptance of “large packets” with the caveat that the packets should be of “reasonable length” or dropped. The assignment should be filled in by the ST author with the maximum packet size accepted, thus defining “reasonable length” for the TOE.

Evaluation Activity

TSS

The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.

Guidance

There are no guidance evaluation activities for this element.

Tests

The evaluator shall perform the following test:

- ***Test 1:** The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this element, the packet is dropped.*

FCS_SSHC_EXT.1.3

The SSH client shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: aes128-ctr, aes256-ctr, [**selection**: *aes128-cbc*, *aes256-cbc*, *AEAD_AES_128_GCM*, *AEAD_AES_256_GCM*, *aes128@openssh.com*, *aes256@openssh.com*, *no other algorithms*].

Application Note:

RFC 5647 specifies the use of the AEAD_AES_128_GCM and AEAD_AES_256_GCM algorithms in SSH. As described in RFC 5647, AEAD_AES_128_GCM and AEAD_AES_256_GCM can only be chosen as encryption algorithms when the same algorithm is being used as the MAC algorithm.

If AES-GCM is selected, there should be corresponding FCS_COP entries in the ST.

RFC 5647 applies only to the RFC-compliant implementation of GCM. A TOE that implements only the “@openssh.com” variant of GCM should not select 5647-compliant algorithms in FCS_SSHC_EXT.1.1. aes*-gcm@openssh.com is specified in Section 1.6 of the OpenSSH Protocol Specification (https://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/PROTOCOL?rev=1.31).

Evaluation Activity

TSS

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that it specifies the supported encryption algorithms and any optional characteristics. The evaluator shall also check the TSS to ensure that the encryption algorithms specified are identical to those listed for this element.

Guidance

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

Tests

The evaluator shall perform the following tests:

- ***Test 1:** The evaluator shall establish an SSH connection using each of the encryption algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of this test.*
- ***Test 2:** The evaluator shall configure an SSH server to only allow the 3des-cbc encryption algorithm and no other encryption algorithms. The evaluator shall attempt to establish an SSH connection from the TOE to the SSH server and observe that the connection is rejected.*

FCS_SSHC_EXT.1.4
The SSH client shall ensure that the SSH transport implementation uses [**selection**: *ssh-rsa*, *rsa-sha2-256*, *rsa-sha2-512*, *ecdsa-sha2-nistp256*] and [**selection**: *ecdsa-sha2-nistp384*, *x509v3-ecdsa-sha2-nistp256*, *x509v3-ecdsa-sha2-nistp384*, *no other public key algorithms*] as its public key algorithm(s) and rejects all other public key algorithms.
Application Note:

Implementations that select only ssh-rsa will not achieve the 112-bit security strength in the digital signature generation for SSH authentication as is recommended in NIST SP 800-131A. Future versions of this document may remove ssh-rsa as a selection. If "x509v3-ecdsa-sha2-nistp256" or "x509v3-ecdsa-sha2-nistp384" are selected, then the list of trusted certification authorities must be selected in FCS_SSHC_EXT.1.8. RFC 8332 specifies the use of rsa-sha2-256 or rsa-sha2-512 in SSH.

The SFRs for cryptographic key generation and certificate validation are inherited from the PP or PP-Module that includes this Package.

Evaluation Activity
TSS
The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that it specifies the supported public key algorithms and any optional characteristics. The evaluator shall also check the TSS to ensure that the encryption algorithms specified are identical to those listed for this element.
Guidance
The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
Tests
The evaluator shall perform the following tests:

- ***Test 1:** The evaluator shall establish a SSH connection using each of the public key algorithms specified by the requirement to authenticate an SSH server to the TOE. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.*
- ***Test 2:** The evaluator shall configure an SSH server to only allow the ssh-dsa public key algorithm and no other public key algorithms. The evaluator shall attempt to establish an SSH connection from the TOE to the SSH server and observe that the connection is rejected.*

FCS_SSHC_EXT.1.5
The SSH client shall ensure that the SSH transport implementation uses [**selection**: *hmac-sha1*, *hmac-sha1-96*, *hmac-sha2-256*, *hmac-sha2-512*] and [**selection**: *AEAD_AES_128_GCM*, *AEAD_AES_256_GCM*, *implicit*, *no other MAC algorithms*] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).
Application Note:

RFC 5647 specifies the use of the AEAD_AES_128_GCM and AEAD_AES_256_GCM algorithms in SSH. As described in RFC 5647, AEAD_AES_128_GCM and AEAD_AES_256_GCM can only be chosen as MAC algorithms when the same algorithm is being used as the encryption algorithm. RFC 6668 specifies the use of the sha2 algorithms in SSH.

The SFRs for cryptographic operations, encryption, and hashing are inherited from the PP or PP-Module that includes this Package.

The ST author selects “implicit” if and only if aes*-gcm@openssh.com is selected as an encryption algorithm. When aes*-gcm@openssh.com is negotiated as the encryption algorithm, the MAC algorithm field is ignored and GCM is implicitly used as the MAC. “implicit” is not an SSH algorithm identifier and will not be seen on the wire; however, the negotiated MAC might be decoded as “implicit”.

Evaluation Activity
TSS
The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms and that this list corresponds to the list in this element.
Guidance
The evaluator shall check the guidance documentation to ensure that it includes instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed).
Tests
The evaluator shall perform the following tests:

- ***Test 1:** The evaluator shall establish a SSH connection using each of the integrity algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of*

this test.

- ***Test 2:*** *The evaluator shall configure an SSH server to only allow the "none" MAC algorithm. The evaluator shall attempt to connect from the TOE to the SSH server and observe that the attempt fails.*
- ***Test 3:*** *The evaluator shall configure an SSH server to only allow the hmac-md5 MAC algorithm. The evaluator shall attempt to connect from the TOE to the SSH server and observe that the attempt fails. To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*- gcm@openssh.com encryption algorithm is negotiated while performing this test.*

FCS_SSHC_EXT.1.6
The SSH client shall ensure that [**selection**: *diffie-hellman-group14-sha1*, *ecdh-sha2-nistp256*] and [**selection**: *ecdh-sha2-nistp384*, *ecdh-sha2-nistp521*, *no other methods*] are the only allowed key exchange methods used for the SSH protocol.
Evaluation Activity
TSS
The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms and that this list corresponds to the list in this element.
Guidance
The evaluator shall check the guidance documentation to ensure that it includes instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.
Tests
The evaluator shall perform the following test:

- ***Test 1:*** *The evaluator shall configure an SSH server to permit all allowed key exchange methods. The evaluator shall then attempt to connect from the TOE to the SSH server using each allowed key exchange method and observe that each attempt succeeds.*

FCS_SSHC_EXT.1.7
The SSH client shall ensure that the SSH connection be rekeyed after [**selection**: *no more than 2^{28} packets have been transmitted*, *no more than 1 gigabyte of data has been transmitted*, *no more than 1 hour*] using that key.
Evaluation Activity
TSS
There are no TSS evaluation activities for this element.
Guidance
There are no guidance evaluation activities for this element.
Tests
The evaluator shall perform the following test for each rekeying method claimed in the ST:

The evaluator shall perform the following test:

- ***Test 1:*** *The evaluator will configure the TOE to create a log entry when a rekey occurs. The evaluator will connect to the TOE with an SSH client and cause a rekey to occur according to the selection(s) in the ST, and subsequently the evaluator uses available methods and tools to verify that rekeying occurs. This could be done, e.g., by checking that a corresponding audit event has been generated by the TOE, if the TOE supports auditing of rekey events.*

FCS_SSHC_EXT.1.8
The SSH client shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key or [**selection**: *a list of trusted certification authorities*, *no other methods*] as described in RFC 4251 section 4.1.
Application Note: The selection for "a list of trusted certification authorities" can only be chosen if "x509v3-ecdsa-sha2-nistp256" or "x509v3-ecdsa-sha2-nistp384" are selected in FCS_SSHC_EXT.1.4.
Evaluation Activity
TSS
There are no TSS evaluation activities for this element.
Guidance
There are no guidance evaluation activities for this element.
Tests
The evaluator shall perform the following tests:

- ***Test 1:*** *The evaluator shall delete all entries in the TOE's list of recognized SSH server host keys and, if selected, all entries in the TOE's list of trusted certification authorities. The evaluator shall then initiate a connection from the TOE to an SSH server. The evaluator shall ensure that the TOE either rejects the connection or displays the SSH server's public key (either the key bytes themselves or a hash of the key using any allowed hash algorithm) and prompts the user to accept or deny the key before continuing the connection.*
- ***Test 2:*** *The evaluator shall add an entry associating a host name with a public key into the TOE's local database. The evaluator shall then replace, on the corresponding SSH server, the server's host key with a different host key. The evaluator shall initiate a connection from the TOE to the SSH server using password-based authentication, shall ensure that the TOE rejects the connection, and shall ensure that the password was not transmitted to the SSH server (for example, by instrumenting the SSH server with a debugging capability to output received passwords).*

FCS_SSHS_EXT.1 SSH Protocol - Server

~~The inclusion of this~~ This is a selection-based component. Its inclusion depends upon ~~a~~ selection ~~in~~ from FCS_SSH_EXT.1.1.
FCS_SSHS_EXT.1.1

The SSH server shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based and [**selection**: *password-based*, *no other method*].
Evaluation Activity
TSS
The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication and that this list conforms to FCS_SSHS_EXT.1.4. The evaluator shall also ensure that password-based authentication methods, if supported, are described.
Guidance
If the SSH server supports password-based authentication, the evaluator shall examine the guidance to determine that it includes instructions on how to configure whether the TSF uses password-based or public key-based authentication.
Tests
The evaluator shall perform the following tests:

- ***Test 1:** The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection from an SSH client. Any configuration activities required to support this test shall be performed according to instructions in the guidance documentation.*
- ***Test 2:** The evaluator shall choose one public key algorithm supported by the TOE. The evaluator shall generate a new key pair for that algorithm without configuring the TOE to recognize the public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails.*
- ***Test 3:** [conditional]: TOE supports password-based authentication] Using the guidance documentation, the evaluator shall configure the TOE to perform password-based authentication on a client and demonstrate that a user can be successfully authenticated by the TOE using a password as an authenticator.*
- ***Test 4:** [conditional]: TOE supports password-based authentication] The evaluator shall use an SSH client to enter an incorrect password to attempt to authenticate to the TOE and demonstrate that the authentication fails.*

FCS_SSHS_EXT.1.2
The SSH server shall ensure that, as described in RFC 4253, packets greater than [**assignment**: number of bytes] bytes in an SSH transport connection are dropped.
Application Note: RFC 4253 provides for the acceptance of “large packets” with the caveat that the packets should be of “reasonable length” or dropped. The assignment should be filled in by the ST author with the maximum packet size accepted, thus defining “reasonable length” for the TOE.
Evaluation Activity
TSS
The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.
Guidance
There are no guidance evaluation activities for this element.
Tests

The evaluator shall perform the following test:

- ***Test 1:** The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this element, the packet is dropped.*

FCS_SSHS_EXT.1.3
The SSH server shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: aes128-ctr, aes256-ctr, [**selection**: *aes128-cbc*, *aes256-cbc*, *AEAD_AES_128_GCM*, *AEAD_AES_256_GCM*, *aes128-gcm@openssh.com*, *aes256-gcm@openssh.com*, *no other algorithms*].
Application Note:

RFC 5647 specifies the use of the AEAD_AES_128_GCM and AEAD_AES_256_GCM algorithms in SSH. As described in RFC 5647, AEAD_AES_128_GCM and AEAD_AES_256_GCM can only be chosen as encryption algorithms when the same algorithm is being used as the MAC algorithm.

RFC 5647 applies only to the RFC compliant implementation of GCM. A TOE that implements only the “@openssh.com” variant of GCM should not select 5647-compliant algorithms in FCS_SSHS_EXT.1.1. aes*-gcm@openssh.com is specified in Section 1.6 of the OpenSSH Protocol Specification (https://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/PROTOCOL?rev=1.31).

Evaluation Activity
TSS
The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that it specifies the supported encryption algorithms and any optional characteristics. The evaluator shall also check the TSS to ensure that the encryption algorithms specified are identical to those listed for this element.
Guidance
The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
Tests
The evaluator shall perform the following tests:

- ***Test 1:** The evaluator shall initiate an SSH connection using each of the encryption algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of this test.*

- ***Test 2:*** *The evaluator shall configure an SSH client to only propose the 3des-cbc encryption algorithm and no other encryption algorithms. The evaluator shall attempt to establish an SSH connection from this client to the TOE server and observe that the connection is rejected.*

FCS_SSHS_EXT.1.4
The SSH server shall ensure that the SSH transport implementation uses [**selection**: *ssh-rsa*, *rsa-sha2-256*, *rsa-sha2-512*, *ecdsa-sha2-nistp256*] and [**selection**: *ecdsa-sha2-nistp384*, *x509v3-ecdsa-sha2-nistp256*, *x509v3-ecdsa-sha2-nistp384*, *no other public key algorithms*] as its public key algorithm(s) and rejects all other public key algorithms.
Application Note:

Implementations that select only ssh-rsa will not achieve the 112-bit security strength in the digital signature generation for SSH authentication as is recommended in NIST SP 800-131A. Future versions of this document may remove ssh-rsa as a selection. RFC 8332 specifies the use of rsa-sha2-256 or rsa-sha2-512 in SSH.

The SFRs for cryptographic key generation and certificate validation are inherited from the PP or PP-Module that includes this Package.

Evaluation Activity
TSS
The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that it specifies the supported public key algorithms and any optional characteristics. The evaluator shall also check the TSS to ensure that the encryption algorithms specified are identical to those listed for this element.
Guidance
The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
Tests
The evaluator shall perform the following tests:

- ***Test 1:*** *Using an appropriately configured client, the evaluator shall establish an SSH connection using each of the public key algorithms specified by the requirement to authenticate to the TOE. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of this test.*
- ***Test 2:*** *The evaluator shall configure an SSH client to propose only the ssh-dsa public key algorithm and no other public key algorithms. Using this client, the evaluator shall attempt to establish an SSH connection to the TOE and observe that the connection is rejected.*

FCS_SSHS_EXT.1.5
The SSH server shall ensure that the SSH transport implementation uses [**selection**: *hmac-sha1*, *hmac-sha1-96*, *hmac-sha2-256*, *hmac-sha2-512*] and [**selection**: *AEAD_AES_128_GCM*, *AEAD_AES_256_GCM*, *implicit*, *no other MAC algorithms*] as its MAC algorithm(s) and rejects all other MAC algorithm(s).
Application Note:

RFC 5647 specifies the use of the AEAD_AES_128_GCM and AEAD_AES_256_GCM algorithms in SSH. As described in RFC 5647, AEAD_AES_128_GCM and AEAD_AES_256_GCM can only be chosen as MAC algorithms when the same algorithm is being used as the encryption algorithm. RFC 6668 specifies the use of the sha2 algorithms in SSH.

The SFRs for cryptographic operations, encryption and hashing, are inherited from the PP or PP-Module that includes this Package.

The ST author selects “implicit” if and only if aes*-gcm@openssh.com is selected as an encryption algorithm. When aes*-gcm@openssh.com is negotiated as the encryption algorithm, the MAC algorithm field is ignored and GCM is implicitly used as the MAC. “implicit” is not an SSH algorithm identifier and will not be seen on the wire; however, the negotiated MAC might be decoded as “implicit”.

Evaluation Activity
TSS
The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms and that this list corresponds to the list in this element.
Guidance
The evaluator shall check the guidance documentation to ensure that it includes instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” and "hmac-md5" MAC algorithms are not allowed).
Tests
The evaluator shall perform the following tests:

- ***Test 1:*** *Using an appropriately configured client, the evaluator shall establish a SSH connection with the TOE using each of the integrity algorithms specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.*
- ***Test 2:*** *The evaluator shall configure an SSH client to only propose the “none” MAC algorithm. Using this client, the evaluator shall attempt to connect to the TOE and observe that the attempt fails.*
- ***Test 3:*** *The evaluator shall configure an SSH client to only propose the hmac-md5 MAC algorithm. Using this client, the evaluator shall attempt to connect to the TOE and observe that the attempt fails. To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*- gcm@openssh.com encryption algorithm is negotiated while*

performing this test.

FCS_SSHS_EXT.1.6
The SSH server shall ensure that [**selection**: *diffie-hellman-group14-sha1*, *ecdh-sha2-nistp256*] and [**selection**: *ecdh-sha2-nistp384*, *ecdh-sha2-nistp521*, *no other methods*] are the only allowed key exchange methods used for the SSH protocol.
Evaluation Activity
TSS
The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms and that this list corresponds to the list in this element.
Guidance
The evaluator shall check the guidance documentation to ensure that it includes instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections to the TOE.
Tests
The evaluator shall perform the following tests:

- ***Test 1:*** *For each of the allowed key exchange methods, the evaluator shall configure an SSH client to propose only that method and then attempt to connect to the TOE. The evaluator shall confirm that each attempt succeeds.*
- ***Test 2:*** *The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to use this SSH client to connect to the TOE and confirm that this attempt fails.*

FCS_SSHS_EXT.1.7
The SSH server shall ensure that the SSH connection be rekeyed after [**selection**: *no more than 2^{28} packets have been transmitted*, *no more than 1 gigabyte of data has been transmitted*, *no more than 1 hour*] using that key.
Evaluation Activity
TSS
There are no TSS evaluation activities for this element.
Guidance
If the TOE has the ability to generate a log when an SSH rekey occurs, the evaluator shall examine the operational guidance to verify that it describes any configuration that is needed for this to be performed.
Tests
The evaluator shall perform the following test for each rekeying method claimed in the ST:

The evaluator shall perform the following test:

- ***Test 1:*** *The evaluator will configure the TOE to create a log entry when a rekey occurs. The evaluator will connect to the TOE with an SSH client and cause a rekey to occur according to the selection(s) in the ST, and subsequently the evaluator uses available methods and tools to verify that rekeying occurs. This could be done, e.g., by checking that a corresponding audit event has been generated by the TOE, if the TOE supports auditing of rekey events.*

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 included 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-based 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-based Requirements

This Package does not define any Implementation-based requirements.

Appendix B - Selection-based Requirements

As indicated in the introduction to this Package, the baseline requirements (those that must be performed by theTOE 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

The auditable events in the table below are included in a Security Target if both the associated requirement is included and the incorporating PP or PP-Module supports audit event reporting through FAU_GEN.1 and any other criteria in the incorporating PP or PP-Module are met.

Table 2: Auditable Events for Selection-based Requirements

Requirement	Auditable Events	Additional Audit Record Contents
FCS_SSHC_EXT.1	**[selection:** *Failure to establish a session, None***]**	Reason for failure. Non-TOE endpoint of attempted connection (IP Address).
FCS_SSHC_EXT.1	**[selection:** *Establishment of a session, None***]**	Non-TOE endpoint of connection (IP Address).
FCS_SSHC_EXT.1	**[selection:** *Termination of a session, None***]**	Non-TOE endpoint of connection (IP Address).
FCS_SSHS_EXT.1	**[selection:** *Failure to establish a session, None***]**	Reason for failure. Non-TOE endpoint of attempted connection (IP Address).
FCS_SSHS_EXT.1	**[selection:** *Establishment of a session, None***]**	Non-TOE endpoint of connection (IP Address).
FCS_SSHS_EXT.1	**[selection:** *Termination of a session, None***]**	Non-TOE endpoint of connection (IP Address).

Appendix C - 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.
[GPOSPP]	Protection Profile for General Purpose Operating Systems
[MDMPP]	Protection Profile for Mobile Device Management
[AppPP]	Protection Profile for Application Software
[VirtPP]	Protection Profile for Virtualization

Appendix D - Acronyms

Acronym	Meaning
Base-PP	Base Protection Profile
CC	Common Criteria
CEM	Common Evaluation Methodology
OE	Operational Environment
PP	Protection Profile
PP-Configuration	Protection Profile Configuration

PP-Module	Protection Profile Module
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification