Network Device Interpretation # 202115

Clarification of public key user authentication for SSH

Status: ☒ *Active* □ *Inactive*

Date: *13-Oct-2021*

End of proposed Transition Period (to be updated after TR2TD process): *13-Nov-2021*

Type of Change: □ Immediate application ☒ Minor change □ Major change

Type of Document: ☒ *Technical Decision* □ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

Affected Document(s): *NDcPPv2.2e, ND SD v2.2*

Affected Section(s): *FCS_SSHC_EXT.1*

Superseded Interpretation(s): *None*

Issue:

Issue (Testing of key-based user authentication for SSH):

RFI 201832 requested clarification on the role of “public key” testing in FCS_SSHC_EXT.1.5 which resulted in an intent statement being provided in the Test AA. However, it appears that there is still an unresolved ambiguity in FCS_SSHC_EXT.1.2 about what it means to require “public key” or optional “password” authentication when you read it within the context of the Test AAs in the SD.

Specifically, in the NDcPP v2.2e SD, for FCS_SSHC_EXT.1.2, we see the following:

Test 1: If password-based authentication methods have been selected in the ST then using the guidance documentation, the evaluator shall configure the TOE to perform password-based authentication to an SSH server and demonstrate that a Security Administrator can be successfully authenticated by the TOE to an SSH server using a password as an authenticator.

Note: Public key authentication is tested as part of testing for FCS_SSHC_EXT.1.5

In the above, the test case for passwords clearly shows that the intent is to authenticate a user to a non-TOE SSH server using a password. This specific test case is clearly about user authentication. (Even the SFR element points the reader to RFC 4252 which is about user auth [RFC 4253 contains details on host key auth].) However, public key testing is deferred to FCS_SSHC_EXT.1.5 which is (as modified by RFI 201832) completely about how the TOE validates the non-TOE server and has nothing to do with user authentication.

Test 1: The evaluator shall establish an 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 objective: The purpose of this positive test is to check the authentication of the server by the client (when establishing the transport layer connection), and not for checking generation of the authentication message from the client (in the User Authentication Protocol). The evaluator shall therefore establish sufficient separate SSH connections (with an appropriately configured server) to cause the TOE to demonstrate use of all public key algorithms claimed in FCS_SSHC_EXT.1.5 in the ST.

This discrepancy in the Test AAs means that it is unclear whether a conforming TOE requires its in-scope SSH client to implement user-based public key authentication or whether password-based user authentication is sufficient and what algorithms the host key and user-key are allowed to claim.

(Note that other AAs in the SD refer to password-based user authentication vs. user public key authentication such as FCS_SSHC_EXT.1.9 test cases. TSS and AGD also refer interchangeably to user-based auth and host-based auth.)

Proposed resolution:

FCS_SSHC_EXT.1.2 and FCS_SSHC_EXT.1.5 should be reconciled. Such an effort seems to be non-trivial, however, and we defer to the NIT to handle how such a clarification should be structured and communicated.

Resolution:

The NIT acknowledges the ambiguity of public key requirements.

To summarize expectations in the NDcPP: any conforming SSH client implementation must be capable of validating a SSH server's public key and in turn authenticate itself with a user-key; any conforming SSH server implementation must be capable of presenting its own public key and in turn both validate SSH client's public key and bind it with a specific user identity.

NDcPP v2.2e, FCS_SSHC_EXT.1 'SSH Client' shall be modified as follows:

<old>
FCS_SSHC_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: *password-based, no other method*].
</old>

Shall be replaced with:

<new>
FCS_SSHC_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [selection: *password-based, no other method*].

Application Note *

The intent of this element is to specify user authentication mechanism(s) that the TOE supports when acting as an SSH client. The TOE is required to implement the capability to generate user-based authentication keys in accordance with FCS_CKM.1 as specified by FMT_SMF.1 via

"Ability to manage the cryptographic keys". While no specific public key algorithms are mandatory to implement, the use of public key algorithms must be consistent with FCS_CKM.1, FCS_COP.1/Hash, and FCS_COP.1/SigGen.

If the TOE implements password-based authentication, the option 'password-based' must be selected. If the TOE can only authenticate itself with a public key, the option 'no other method' must be chosen.
</new>

FCS_SSHC_EXT.1.5 Application Note 93 shall be prepended with:

<new>

Application Note 93

The intent of this element is to specify peer (SSH server) authentication mechanism(s) that the TOE supports when acting as an SSH client. The TOE is required to implement the capability to verify the host's public key as described in RFC 4251 Section 4.1.

If x509v3-ssh-rsa…
</new>

ND SD v2.2, FCS_SSHC_EXT.1 'SSH Client' TSS shall be modified as follows:

<old>
TSS FCS_SSHC_EXT.1.2

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.1.5. and ensure that if password-based authentication methods have been selected in the ST then these are also described.
</old>

Shall be replaced with:

<new>
TSS FCS_SSHC_EXT.1.2

The evaluator shall check to ensure that the TSS contains a list of the public key algorithms that are acceptable for use for user authentication and that this list is consistent with asymmetric key generation algorithms selected in FCS_CKM.1, hashing algorithms selected in FCS_COP.1/Hash, and signature generation algorithms selected in FCS_COP.1/SigGen. The evaluator shall confirm the TSS is unambiguous in declaring the TOE's ability to authenticate itself to a remote endpoint with a user-based public key.

If password-based authentication method has been selected in the FCS_SSHC_EXT.1.2, then the evaluator shall confirm it is also described in the TSS.

</new>

<old>
TSS FCS_SSHC_EXT.1.5

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the public key algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the public key algorithms specified are identical to those listed for this component.

If x509v3-based…
</old>

Shall be replaced with:

<new>
TSS FCS_SSHC_EXT.1.5

The evaluator shall confirm the TSS describes how a host-key public key (i.e., SSH server's public key) is associated with the server identity.

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the host-key public key algorithms supported by the TOE are specified as well. The evaluator shall check the TSS to ensure that the host-key public key algorithms specified are identical to those listed for this component.

If x509v3…
</new>

ND SD v2.2, FCS_SSHC_EXT.1 'SSH Client' Guidance shall be modified as follows:

<new>
Guidance FCS_SSHC_EXT.1.2

The evaluator shall check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed mechanisms are used in SSH connections initiated by the TOE.
</new>

ND SD v2.2, FCS_SSHC_EXT.1.2 Tests shall be modified as follows:

<old>
Test 1: If password-based authentication methods have been selected in the ST then using the guidance documentation, the evaluator shall configure the TOE to perform password-based authentication to an SSH server and demonstrate that a Security Administrator can be successfully authenticated by the TOE to an SSH server using a password as an authenticator.

Note: Public key authentication is tested as part of testing for FCS_SSHC_EXT.1.5
</old>

Shall be replaced with:

<new>
Test objective: The purpose of these tests is to check the authentication of the client to the server using each claimed authentication method.

Test 1: For each claimed public-key authentication method, the evaluator shall configure the TOE to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH server to demonstrate the use of all claimed public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test.

Test 2: [Conditional] If password-based authentication method has been selected in the FCS_SSHC_EXT.1.2, then following the guidance documentation the evaluator shall configure the TOE to perform password-based authentication with a remote SSH server to demonstrate that the TOE can successfully authenticate using a password as an authentication method.
</new>

Rationale:

See Resolution section.

In addition, the choice was made to avoid adding new SFR elements to FCS_SSHC_EXT.1 to account for claiming applicable user-based public key algorithms. Because it is the responsibility of the non-TOE endpoint to validate the user-based public key sent by the TOE, the set of algorithms the non-TOE server may accept does not need to be restricted. The TOE is mandated to be able to generate and use keys using claimed algorithms, and therefore there is a reliance on FCS_CKM.1 for the purposes of generating user-based public/private keys and FCS_COP.1/Hash and FCS_COP.1/SigGen for the purposes of using these keys to produce user authentication signature messages. The changes are designed to be consistent with both traditional user-based public/private key authentication in RFC 4252 section 7 as well as RFC 6187 for user-based X.509 certificates.

Further Action:

None

Action by Network iTC:

Consider to replace the current SSH requirements by the SSH requirements defined by the CCUF Crypto WG.