Network Device Interpretation # 202113A

Clarification of public key authentication for SSH Server

Status: ☒ *Active* ☐ *Inactive*

Date: *10-Mar-2022*

End of proposed Transition Period (to be updated after TR2TD process): *10-Apr-2022*

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 SDv2.2*

Affected Section(s): *FCS_SSHS_EXT.1, FMT_SMF.1*

Superseded Interpretation(s): *None*

Issue:

Issue: SSHS Public-Key Authentication - A

We are seeking confirmation (or correction) on the following interpretation of the SSH requirements in NDcPPv2.2e.

1. When SSH Server is claimed, the TOE is required to support host-key (and/or X.509v3 cert) authentication:

a. FCS_SSHS_EXT.1.5, Application Note 101 states “An SSH server implementation that claims to support x509v3-based public key authentication algorithms is expected to comply with RFC 6187 Section 4 recommendations when identifying itself with an x.509v3 certificate to SSH clients”. “…when identifying itself with an x.509v3 certificate to SSH clients” clearly refers to server authentication.

b. FCS_SSHS_EXT.1.5, Test 1 states “The evaluator shall establish an SSH connection using each of the public key algorithms specified by the requirement to authenticate the TOE to an SSH client”. “…authenticate the TOE to an SSH client” suggests server authentication using host-key (or X.509v3 certificates).

i. Note that this interpretation requires the TOE to support generation of its own SSH host-key pair(s). And if X.509 is claimed for this TSF, then support for generating of Certificate Signing Requests is required.

c. FTP_TRP.1.1/Admin requires the selectable protocols to provide “assured identification its end points”. In SSH, this is achieved by public-key/password-based authentication of the user to the server, and by ‘explicit server authentication’ of the server to the client using host-keys (X.509 methods present

an alternative but they these alternatives still rely on cryptographic means to provide assurance of identity).

Resolution:

The NIT acknowledges the ambiguity of public key requirements in SSH.

To summarize expectations outlined 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_SSHS_EXT.1 shall be modified as follows:

<old>
FCS_SSHS_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*].

Application Note 98

If the TOE supports password-based authentication, the option 'password-based' must be selected. If the TOE supports only public key-based authentication, the option 'no other method' must be chosen.
</old>

Shall be replaced with:

<new>
FCS_SSHS_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 98

The intent of this element is to specify user authentication mechanism(s) that the TOE acting as an SSH server accepts from connecting SSH clients. The TOE is required to implement the capability to validate presented authentication keys. When SSH Server is used as part of FTP_TRP.1/Admin, it is expected the TOE is capable of verifying each presented key against a database of trusted user identities as specified by FMT_SMF.1. While no specific public key algorithms are mandatory to support, the use of public key algorithms must be consistent with signature verification as specified in 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_SSHS_EXT.1.5 Application Note 101 shall be prepended with:

<new>
Application Note 101

The intent of this element is to specify public-key server authentication mechanism(s) that the TOE implements. The TOE is required to implement the capability to generate its own host authentication key(s) in accordance with FCS_CKM.1 as specified by FMT_SMF.1 via "Ability to manage the cryptographic keys".

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_SSHS_EXT.1.2 TSS shall be modified as follows:

<old>
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.1.5. 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>
The evaluator shall check to ensure that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with signature verification algorithms selected in FCS_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims).

The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file.

If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, then the evaluator shall confirm its role in the authentication process is described in the TSS.
</new>

ND SD v2.2, FCS_SSHS_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 accept password-based authentication and demonstrate that user authentication succeeds when the correct password is provided by the user.

Test 2: If password-based authentication methods have been selected in the ST then the evaluator shall use an SSH client, enter an incorrect password to attempt to authenticate to the TOE, and demonstrate that the authentication fails.

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

Shall be replaced with:

<new>

Test objective: The purpose of these tests is to verify server supports each claimed client authentication method.

Test 1: For each supported client public-key authentication algorithm, the evaluator shall configure a remote client 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 client to demonstrate the use of all applicable 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: The evaluator shall choose one client public key authentication algorithm supported by the TOE. The evaluator shall generate a new client key pair for that supported algorithm without configuring the TOE to recognize the associated 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] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication succeeds when the correct password is provided by the connecting SSH client.

Test 4: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication fails when the incorrect password is provided by the connecting SSH client.
</new>

ND SD v2.2, FCS_SSHS_EXT.1.5 TSS shall be modified as follows:

<old>

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.

The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file.

</old>

Shall be replaced with:

<new>

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the SSH server's host public key algorithms supported are specified and that they are identical to those listed for this component.

</new>

ND SD v2.2, FCS_SSHS_EXT.1.5 Test shall be modified as follows:

<old>
Test 1: The evaluator shall establish an SSH connection using each of the public key algorithms specified by the requirement to authenticate the TOE to an SSH client. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.
</old>

Shall be replaced with:

<new>
Test objective: This test case is meant to validate that the TOE server will support host public keys of the claimed algorithm types.

Test 1: The evaluator shall configure (only if required by the TOE) the TOE to use each of the claimed host public key algorithms. The evaluator will then use an SSH client to confirm that the client can authenticate the TOE server public key using the claimed algorithm. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.
</new>

<old>
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 objective: The purpose of this negative test is to verify that the server rejects authentication attempts of clients that present a public key that does not match public key(s) associated by the TOE with the identity of the client (i.e. the public keys are unknown to the server). To demonstrate correct functionality, it is sufficient to determine that an SSH connection was not established after using a valid username and an unknown key of supported type.
</old>

Has effectively been moved to FCS_SSHS_EXT.1.2.

<old>
Test 3: The evaluator shall configure an SSH client to only allow a public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the SSH client to the TOE and observe that the connection is rejected.
</old>

Shall be replaced with:

<new>
Test objective: This negative test case is meant to validate that the TOE server does not support host public key algorithms that are not claimed.

Test 2: The evaluator shall configure a non-TOE SSH client to only allow it to authenticate an SSH server host public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the non-TOE SSH client to the TOE SSH server and observe that the connection is rejected.
</new>

NDcPP v2.2e, FMT_SMF.1 'Specification of Management Functions' shall be appended as follows:

<new>
FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

…

[selection:

…

- Ability to manage the trusted public keys database;
- No other capabilities].

Application Note 24

…

If the TOE offers ability for a remote authorized IT entities or authorized remote Administrators to connect via an interface secured with SSH, then the ST author must select the option "Ability to manage the trusted public keys database" to account for management of public key authentication. It is acceptable for this management function to be implemented as part of general TOE user management functionality or as a standalone management function.
</new>

Rationale:

The choice was made to avoid adding new SFR elements to FCS_SSHS_EXT.1 to account for claiming applicable public key algorithms. The TOE is mandated to be able to generate its own keys using claimed algorithms and therefore there is a reliance on FCS_CKM.1 for the purposes of generating public/private keys and FCS_COP.1/SigGen for the purposes of authenticating connecting users.

Further Action:

The NiT recommends adapting SSH Package in the future version of the NDcPP.

Action by Network iTC:

None