Network Device Interpretation # 201718rev3

Updating FCS_IPSEC_EXT.1.14 Tests 1-3

Status: ☒ *Active* ☐ *Inactive*

Date: *5-Jul-2018*

End of proposed Transition Period (to be updated after TR2TD process): *6-Sep-2018*

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): *ND SD V2.0*

Affected Section(s): *FCS_IPSEC_EXT.1.14 Tests 1-3*

Superseded Interpretation(s): *RfI#201718rev2*

Issue:

RFC 201709 "Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4" updated identifier tests for TLS and DTLS. This RFI propagates these changes to the IPsec protocol.

The current wording for FCS_IPSEC_EXT.1.14 Test 1, Test 2, and Test 3 is as follows:

> For each supported identifier type (excluding DNs), the evaluator shall repeat the following tests:
>
> Test 1: 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 2: 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 not match the field in the peer's presented certificate and shall verify that the IKE authentication fails.
>
> Test 3: (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.

Proposed Resolution:

It is suggested to make X.509v3 identifier testing consistent across supported protocols.

Resolution:

Due to disagreement within the iTC with the original NIT proposal to resolve RfI#201718 this resolution has been developed and approved by the RfI#201718 ad hoc Task Force (TF).

The RfI#201718 Task Force (TF) acknowledges the lack of adequate testing of IPSEC protocol described in the 'Issue' section above, but disagrees that mandating support for a SAN extension via an evaluation activity is the appropriate solution. The TF is also concerned that mandating SAN use may prevent a number of existing IPSEC implementations from certifying.

NDcPP V2.0, FWcPP V2.0, FCS_IPSEC_EXT.1.14

FCS_IPSEC_EXT.1.14 shall be modified to read as follows:

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [selection: *SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), SAN: user FQDN, CN: IP address, CN: Fully Qualified Domain Name (FQDN), CN: user FQDN, Distinguished Name (DN)]* and *[selection: no other reference identifier type, [assignment: other supported reference identifier types]*].

FCS_IPSEC_EXT.1.14 Application Note 89 shall be modified to read as follows:

<old> When using RSA or ECDSA certificates for peer authentication, the reference and presented identifiers take the form of either a DN, IP address, FQDN or user FQDN. The reference identifier is the identifier the TOE expects to receive from the peer during IKE authentication. The presented identifier is the identifier that is contained within the peer certificate body. The ST author shall select the presented and reference identifier types supported and may optionally assign additional supported identifier types in the second selection. 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.

The preferred method for verification is the Subject Alternative Name using DNS names, URI names, or Service Names. Verification using the Common Name is required for the purposes of backwards compatibility. Additionally, support for use of IP addresses in the Subject Name or Subject Alternative name is discourage as against best practices but may be implemented. </old>

<new> When using RSA or ECDSA certificates for peer authentication, the reference and presented identifiers take the form of either a DN, IP address, FQDN or user FQDN. The reference identifier is the identifier the TOE expects to receive from the peer during IKE authentication. The presented identifier is the identifier that is contained within the peer certificate body. The ST author shall select the presented and reference identifier types supported and may optionally assign additional supported identifier types in the second selection. 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.

The critical requirement of X.509 identifiers is the ability to bind the public key uniquely to an identity. This can be achieved by using strongly-typed identifiers or controlling the CA and certificate issuance. One recommended method for identity verification is supporting the use of the Subject Alternative Name (SAN)

extension using DNS names, URI names, or Service Names. However, the support for a SAN extension is optional as long as identifier uniqueness can be achieved by other means.

In a future version of this cPP, SAN and/or DN support might be required for all TOEs, support for CN might be optional, and the "other supported referenced identifier types" selection might be removed. In a future version of this cPP, it might also be required that the SAN (when present) shall take precedence over CN.</new>

ND Supporting Document V2.0, FCS_IPSEC_EXT.1.14

FCS_IPSEC_EXT.1.14 TSS Evaluation Activity shall be modified to read as follows:

<old>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 which field(s) of the certificate are used as the presented identifier (DN, Common Name, or SAN). 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.</old>

<new>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 which field(s) of the certificate are used as the presented identifier (DN, Common Name, or SAN). If the TOE simultaneously supports the same identifier type in the CN and SAN, the TSS shall describe how the TOE prioritizes the comparisons (e.g. the result of comparison if CN matches but SAN does not). If the location (e.g. CN or SAN) of non-DN identifier types must explicitly be configured as part of the reference identifier, the TSS shall state this. 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, including what field(s) are compared and which fields take precedence in the comparison.

FCS_IPSEC_EXT.1.14 Guidance Evaluation Activity shall be modified to read as follows:

<old> The evaluator shall ensure the operational guidance includes the configuration of the reference identifier(s) for the peer</old>

<new> The evaluator shall ensure that the operational guidance describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not, and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). If the identifier scheme implemented by the TOE does not guarantee unique identifiers, the evaluator shall ensure that the operational guidance provides a set of warnings and/or CA policy recommendations that would result in secure TOE use. </new>

ND Supporting Document V2.0, FCS_IPSEC_EXT.1.14

FCS_IPSEC_EXT.1.14 Test Evaluation Activity shall be modified to read as follows:

<new>

In the context of the tests below, a valid certificate is a certificate that passes FIA_X509_EXT.1 validation checks but does not necessarily contain an authorized subject.

The evaluator shall perform the following tests:

- Test 1: (conditional) For each CN/identifier type combination selected, 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. If the TOE prioritizes CN checking over SAN (through explicit configuration of the field when specifying the reference identifier or prioritization rules), the evaluator shall also configure the SAN so it contains an incorrect identifier of the correct type (e.g. the reference identifier on the TOE is example.com, the CN=example.com, and the SAN:FQDN=otherdomain.com) and verify that IKE authentication succeeds.
- Test 2: (conditional) For each SAN/identifier type combination selected, 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. If the TOE prioritizes SAN checking over CN (through explicit specification of the field when specifying the reference identifier or prioritization rules), the evaluator shall also configure the CN so it contains an incorrect identifier formatted to be the same type (e.g. the reference identifier on the TOE is DNS-ID; identify certificate has an identifier in SAN with correct DNS-ID, CN with incorrect DNS-ID (and not a different type of identifier)) and verify that IKE authentication succeeds.
- Test 3: (conditional) For each CN/identifier type combination selected, the evaluator shall:
    a) Create a valid certificate with the CN so it contains the valid identifier followed by '\0'. If the TOE prioritizes CN checking over SAN (through explicit specification of the field when specifying the reference identifier or prioritization rules) for the same identifier type, the evaluator shall configure the SAN so it matches the reference identifier.
    b) Configure the peer's reference identifier on the TOE (per the administrative guidance) to match the CN without the '\0' and verify that IKE authentication fails.
- Test 4: (conditional) For each SAN/identifier type combination selected, the evaluator shall:
    a) Create a valid certificate with an incorrect identifier in the SAN. The evaluator shall configure a string representation of the correct identifier in the DN. If the TOE prioritizes CN checking over SAN (through explicit specification of the field when specifying the reference identifier or prioritization rules) for the same identifier type, the addition/modification shall be to any non-CN field of the DN. Otherwise, the addition/modification shall be to the CN.
    b) Configure the peer's reference identifier on the TOE (per the administrative guidance) to match the correct identifier (expected in the SAN) and verify that IKE authentication fails.
- Test 5: (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.
- Test 6: (conditional) If the TOE supports DN identifier types, to demonstrate a bit-wise comparison of the DN, the evaluator shall create the following valid certificates and verify that the IKE authentication fails when each certificate is presented to the TOE:
    a) Duplicate the CN field, so the otherwise authorized DN contains two identical CNs.
    b) Append '\0' to a non-CN field of an otherwise authorized DN.

</new>

Rationale:

Open PKI, or Web PKI, assumes that the identity of the other end point is unknown or not part of the same enterprise network and therefore has to be robustly verified, and applies a set of controls to the application of trust. A Closed PKI assumes that both end points and the issuing CA belong to the same enterprise network and offloads many of these controls onto the CA or the administrators. Fundamentally, Open PKI is concerned with securing "known to unknown" over public channels, and Closed PKI concerned with securing "known to known" over public channels. An informal survey of IPSEC use cases among iTC vendors indicates that a substantial number of use cases are Closed PKI systems. The TF believes that such use cases should be supported at least throughout the current version of the PP.

Test 5: Compare two DNs (this is defined in RFC 2252 as being a match type of "distinguishedNameMatch"). This is a standard match type defined in X501, which states that a presented DN matches a target DN if, and only if:

- *the number of RDNs is the same*
- *each corresponding RDN has the same number of attribute value pairs*
- *each of the attribute pairs that are of the same type have matching values as determined by the match rule for that type*

Note that the order of the attribute pairs within an RDN does not matter.

Further Action:

The TF recommends consultation with the wider iTC on the feasibility of mandating SAN support for IPSEC in future versions of the PP.

Action by Network iTC:

The TF recommends that the NDcPP maintenance team or the wider iTC considers revising the X.509 requirements to provide for separation of Closed PKI and Open PKI use cases.

Open PKI and Close PKI separation is especially relevant for a mixed-use systems, where a trusted Closed PKI CA could be abused to issue flawed certificates that in turn could be used to compromise an Open PKI components that is not necessarily part of the TOE. Addressing such vulnerabilities is outside the scope of this RFI, but the TF proposes a number of recommendations:

a. *Consider mandating separate trust store for any Closed PKI TOE that does not support a SAN. By doing so, certificates issued by a corresponding Closed PKI CA are limited in use to that system.*

b. *Consider revising the FIA_X509_EXT.3 requirements to mandate specifying all supported extensions as part of CSR generation by the TOE, and mandating an explicit check of a signed CSR for presence of a SAN. That is, if the TOE does not support the usage of a SAN, it should warn*

the administrator if the CA is appending a SAN extension to a certificate at the time of signing said certificate. The goal is to minimize the possibility of creating a flawed certificate that would have different identifiers when used in a Closed PKI versus an Open PKI.

The TF also recommends clarifying supported identifier types and acceptable identifier locations as part of FCS_IPSEC_EXT.1.14 and moving away from open-ended "[assignment: other supported reference identifier types]" wording in the SFR.