Network Device Interpretation # 201607

Mandatory requirement for CSR (Certificate Signing Request) generation

Status: ☒ *Active* ☐ *Inactive*

Date: *24-Mar-2016*

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

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

Affected Document(s): *NDcPP v1.0, FWcPP v1.0*

Affected Section(s): *FIA_X509_EXT.3*

Superseded Interpretation(s): *None*

Issue:

NDcPP's FIA_X509_EXT.3 requires on-board key and CSR (Certificate Signing Request) generation. Most network devices currently do not offer this and instead allow the administrator to load keys and certificates. From a security perspective, network devices, unlike smartcard credentials or mobile devices (which can easily fall into the hands attackers), enjoy secure initialization and (most often) physical protection both of which diminish the extent of gains provided by on-board key gen.

For these reasons, this requirement should be made objective to allow vendors time to transition (as well as to allow the TC to add an application note to clarify additional facets of the requirement: e.g., is CSR generation mandatory for all keys, or just an extra option beyond loading).

Resolution:

The NIAP TRRT responded to this request for interpretation as follows:

"This requirement was discussed and mandated by the iTC, which had vendor participation. No objections to making this capability mandatory were raised at that time, so the TRRT does not feel that it is appropriate that they make this requirement objective. Vendors that want to see this change made should work through the iTC; the requirement for now will remain mandatory."

The NIT believes that it is worth making some additional clarifications in their response as follows:

- The RfI mentions on-board key generation, but this is not a part of FIA_X509_EXT.3. Key generation according to FCS_CKM.1 is always a required capability of the TOE in v1.0 of the cPPs
- The requirement for RFC 2986 Certificate Request generation by the TOE remains a mandatory requirement in v1.0 of the cPPs. There is one exception case for this: where a TOE uses only SSH with "ssh-rsa" for its secure channels (i.e. it does not use protocols that require certificates) and

the TOE does not use digital certificates for trusted updates (FPT_TUD_EXT.1) or self-test (FPT_TST_EXT.2), then the FIA_X509_EXT family is not required (see the response to RfI#10)

- It is currently expected that v2.0 of the cPPs will support distributed TOEs, and each component of a distributed TOE will be required either to perform on-board key generation and RFC 2986 Certificate Request generation, or else to receive its keys and certificates, generated on some other component of the TOE, using a secure registration channel at the point where the component is joined to the TOE. Certificate request generation will be required from either the component that generates the key or the component that receives the key. (The exception described above for TOEs that only support ssh-rsa and do not use certificates will continue to apply in v2.0.) A new draft of the ND cPP is expected to be published shortly for public commenting, and it will therefore be possible to submit further comments for discussion of the v2.0 content as part of this review.

Rationale:

On-board key generation is required as part of the intention to improve the secure handling of keys used on network devices.

As noted in the NIAP response, the FIA_X509_EXT SFRs were discussed and agreed for the original version of the cPPs: no visible change has occurred since then that justifies modifying this position for single-component TOEs. For distributed TOEs in v2.0 of the cPPs, it is intended that any component that uses certificate-based protocols would also have to meet this SFR as described above, in order that no other component is required to have access to the private key for signing the certification requires. As noted above, the forthcoming public review of the updated cPP provides an opportunity for requests to be made for this v2.0 requirement to be modified.

Further Action:

The NIT believes that the additional clarifications, particularly with regard to distributed TOE components in cPP v2.0 should be discussed and agreed with the wider iTC before making a final Technical Decision on this RfI.

It seems important to continue to require on-board key generation for the TOE as a whole. This means, for a distributed TOE, that keys must either be generated on each component, or else that some component generates keys and distributes them securely to other components over a secure registration channel (for the initial keys) or secure inter-component channel (if the keys are being replaced). A mixed approach in which some components generate their own keys and some receive keys from another component would also be allowed. More explicit clarification of this can be added to the next draft update to the ND cPP (the current internal draft under review by the iTC is v1.0.3).

It does not seem critical that the TOE is capable of generating the certification request message structure: this could be created and submitted from some other entity (either another component of the TOE or external to the TOE) provided that the signature on the message is created by the TOE (because this uses the private key, which we want to remain accessible only to the TOE component). However, if the TOE has to provide an interface to sign the request message, then it does not seem to

be significantly harder to require the generation of the complete request message (with signature) on the TOE. (Indeed, having a component provide a general signing interface could be more dangerous than requiring it only to be capable of generating certification requests.) Therefore v2.0 of the cPPs will take the position described in the Resolution above, requiring that the certification request is generated either on the component that generates the keys or on the component that receives the keys. This will need to be added in the next draft update of the ND cPP.

Action by Network iTC:

Review the Further Action above; confirm agreement with the NIT suggested resolution and rationale, or else define the necessary replacement text to create a formal Technical Decision.