Network Device Interpretation # 201838

Application Notes for FIA_X509_EXT.1 iterations

Status: ☒ *Active* ☐ *Inactive*

Date: *8-May-2019*

End of proposed Transition Period (to be updated after TR2TD process): *8-Jun-2019*

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): *NDcPP V2.0e, NDcPP V2.1, FWcPP V2.0*

Affected Section(s): *FIA_X509_EXT.1/Rev, FIA_X509_EXT.1/ITT*

Superseded Interpretation(s): *None*

Issue:

NDcPPv2.1 Section B, Table 5 lists expanded requirement for X.509 auditing (a similar entry exists for V2.0e):

FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store

Application Note 48(V2.1; corresponding Application Note 49 in V2.0e)

The audit event for FIA_X509_EXT.1/Rev is based on the TOE not being able to complete the certificate validation by ensuring the following:

- *the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.*
- *Verification of the digital signature of the trusted hierarchical CA*
- *read/access the CRL or access the OCSP server (according to selections in the ST).*

If any of these checks fails, then an audit event with the failure should be written to the audit log.

There is a corresponding entry for audit events as well as a corresponding Application Note for FIA_X509_EXT.1/ITT in Table 4 (Application Note 40 in V2.1 / 39 in V2.0e).

My understanding of this requirement is that you need to audit:

1. Any case of rejecting certificate used for authentication (TLS),
    a. Explicitly log that CA certificate doesn't have basicConstraints flag set
    b. Explicitly log when signature verification failed, but only if it is for hierarchical CA
    c. Explicitly log when access to CRL or OCSP server failed, but only when it results in rejection of certificate
2. Any case of adding, removing, or update of trusted CAs

Problem: This list is oddly specific in not being exhaustive (i.e. identifier mismatch doesn't have to be audited with specific reason) and very narrow (i.e. log signature verification check as a reason, but only for CA).

This is likely unintentional combination of "If any of these checks fails, then an audit event with the failure should be written to the audit log." plus "Reason for failure of certificate validation" and some unintentional specificity. Please clarify this requirement by specifying what kinds of reasons for failure need to be audited. Additionally, please improve definition of certificate validation if it is to be used to define what has to be audited.

Resolution:

The NIT comes to the conclusion that most parts of the application notes described above are more related to FIA_X509_EXT.1 itself than to the required auditing events. The conditions for successful and failed certificate validation need to be part of the SFRs and Application Notes for the FIA_X509_EXT.1 iterations which are currently under revision by the X.509 working group of the Network iTC. The intention remains that the "Reason for failure of certificate validation" will be logged, whatever that reason may be (see also the resolution for RfI#201839). To avoid conflicting definitions and to avoid confusion by the Application Notes listed above, the Application Notes 40(V2.1)/V39(V2.0e) and 48(V2.1)/49(V2.0e) shall be modified as follows.

<old>*The audit event for [FIA_X509_EXT.1/ITT, FIA_X509_EXT.1/Rev] is based on the TOE not being able to complete the certificate validation by ensuring the following:*

- *the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.*
- *Verification of the digital signature of the trusted hierarchical CA*
- *read/access the CRL or access the OCSP server (according to selection in the ST).*

If any of these checks fails, then an audit event with the failure should be written to the audit log.</old>

Shall be replaced by

<new>The audit event "Unsuccessful attempt to validate a certificate" for [FIA_X509_EXT.1/ITT, FIA_X509_EXT.1/Rev] requires the Additional Audit Record Contents of "Reason for failure (of certificate validation)." An error message telling the Security Administrator that 'something is wrong with the certificate' is not considered as presenting sufficient information about the 'reason for failure', because basic information to resolve the issue is missing from the audit record. The log message should inform the Security Administrator at least about the type of error (e.g. that there is a 'Trust issue' with the certificate, e.g. due to failed path validation, in contrast to the use of an 'expired certificate'). The level of detail that needs to be provided to enable the Security Administrator to fix issues based on the information in audit events usually depends on the complexity of the underlying use case. In simple scenarios with only one underlying root cause a single error message might be sufficient whereas in more complex scenarios the granularity of error messages should be higher. The NDcPP only specifies a general guidance on the subject to avoid specifying requirements which are not implementation independent.</new>

FIA_X509_EXT.1/ITT shall be used for Application Note 40(V2.1)/V39(V2.0e) and FIA_X509_EXT.1/Rev shall be used for 48(V2.1)/49(V2.0e).

Rationale:

See Resolution section. The defined changes are intended to make the cPP consistent with the changes defined for the SD in the resolution for RfI#201839.

Further Action:

Revise FIA_X509_EXT.1 iterations and corresponding application notes in X.509 WG.

Action by Network iTC:

None.