draft-ietf-pki4ipsec-ikecert-profile-01.txt

Brian Korver briank@briank.com
Gregory M Lebovitz
gregory@juniper.net

Overview

- Changes from -04 to -00
- Changes from -00 to -01
- Open Issues
  - KU/EKU
- Critical Bit?
- 2401bis sync'ing?
- CDP / AIA ?

Changes from -00 to -01

- Editorial changes to make the text conform with the summary table in 3.1, especially in the text following the table in 3.1. Particular note should be paid to changes in section 3.1.5 (ID_DER_ASN1_DN)
- Sect 3.1.1 – ID=IPaddr - editorial changes to aid in clarification. Added text on when deployers might consider using IP addr, but strongly RECOMMENDED NOT use IP as ID.
- Sect 3.1.8 - removed IP address from list of practically used ID types

…Changes -00 to -01

- 3.1.9. Transitively Binding Identity to Policy – totally overhauled per Kivinen, July 18) – pls read.

- 3.2 - added IKEv2's Hash and URL of x.509 to list of those profiled and gave it its own section, now 3.2.5
  - added note in CRL/ARL section about revocation occurring OOB of IKE
  - deleted ARL as its own section and collapsed it into Revocation
  - Lists (CRL and ARL) for consciseness. Renumbered accordingly.

Empty Cert Req - #34

- 3.2.6.2 –
  - MAY send empty cert req
  - Use case scenario thoroughly described
  - Rule out sending all certs due to processing overhead, fragmentation.
  - Responder: do all you can to send CertReq
    - Check IP in SPD, default CA(s) config'd,
  - If cannot send CertReq, then configurably do one of:
    - Terminate negotiation w/ appropriate error msg
    - Send empty CertReq
  - Appendix C - more use cases and explanation from list

… -00 to -01

3.3 – Cert Payload - clarified that sending CRLs and chaining certs is deprecated.

3.3.10.2 - sending chaining becomes SHOULD NOT. title changed.

4.1.3.3 - if receive cert w/ PKUP, SHOULD ignore it.

4.1.3.13 - CDP changed text to represent SHOULD , and how important CDP becomes when we do not send CRLs in-band. Added SHOULD for CDPs actually being resolvable (Reilly email).

-00 to -01, NITs

- Changed ISAKMP references in Abstract and Intro to IKE

4.1.2 – Subject Name - added text to explicity call out support for CN, C, O, OU

Big Open Issues

- 22 open issues
- 4 or so are “Big”

KU & EKU Handling #36

- Background
  - CAs aren't flexible enough with what they do/don't allow to be configured for (E)KU. Therefore, we can't depend on it.

… KU / EKU

- PROPOSAL: Add to 4.1.3.2 Key Usage:

IKE uses an end-entity certificate in the authentication process. The CA can impose some constraints on the manner that a public key ought to be used. The key usage and extended key usage extensions apply in this situation.

Since we are talking about using the public key to validate a signature, if the key usage extension is present, then at least one of the digitalSignature (0) or the nonRepudiation (1) bit in the key usage extension MUST be set (both can be set as well). It is also fine if other key usage bits are set.

… KU / EKU

- Proposal: 4.1.3.12 Extended Key Usage – change to

The CA SHOULD NOT include the extended key usage extension in certificates for use with IKE. Note that there were three IPsec related object identifiers that were assigned in 1999. The semantics of these values were never clearly defined so they are deprecated and SHOULD NOT be used. The use of these three ExtendedKeyUsage values in IKE/IPsec is obsolete and explicitly deprecated by this specification. (For historical reference only, those values were id-kp-ipsecEndSystem, id-kp-ipsecTunnel, and id-kp-ipsecUser.

If a CA includes a critical extended key usage extension, it could mean that the public key ought to be used exclusively with another application, and is not supposed to be used for IKE. In this case the IKE peer SHOULD terminate negotiation with an appropriate error.

Summary KU / EKU

for peer cert validation

- if told to ignore KU/EKU, accept.
- If no KU extension & no EKU extension, accept
- if KU present and doesn't mention digitalSig or nonRepudiation, reject (both, in addition to others, is also fine)
- if EKU present and doesn't mention "all uses“, reject.
- if none of the above, accept cert.

HTTP_Cert_Lookup ? #38

- IKEv2 specifies a HTTP_CERT_LOOKUP_SUPPORTED notification that tells a peer that certificates don't need to be sent.
- We already have a mechanism for that (don't send a CERTREQ), so is this a useful feature or should we deprecate it?

Sync to 2401bis

- #7 - ID Payload MAY be used for SPD Lookup. 2401bis stating MUST.
- #8 – Substring matching alignment w/ 2401bis
- #9 - Replace SPD lookup reference with PAD lookup
- #10 - Change IP support to IPv4 (MUST) IPv6(MAY) – “If Implementation supports v6, MUST support ID_v6Addr ”

Others?

- Come to Microphone

Next Steps

- Gregory will release a -02 at the end of this week, with conclusions reached in the last three weeks
- Hammer open issues over next 1.5 mo.
- End Sept – Brian K to release -03 w/ any changes.
  - LAST CALL CANDIDATE !!

Let’s rev and go to WG last call!