LAMPS virtual interim on 30 August 2021 at 17:30 UTC

The virtual interim was focused on issues with EST CSR Attrs.

CSR Attributes

(https://datatracker.ietf.org/meeting/interim-2021-lamps-02/materials/slides-interim-2021-lamps-02-sessa-csr-attrs-description-00)

Dan Harkins, as one of the authors of EST (RFC 7030), described the intent of the CSR Attributes. CSR Attributes were included in EST to tell certificate requestors what to include in the CSR regarding cipher suites, key sizes, elliptic curve, and so on.

ACP and BRSKI requirements for certificate enrollment

(https://datatracker.ietf.org/meeting/interim-2021-lamps-02/materials/slides-interim-2021-lamps-02-sessa-problem-statementrequirements-from-acpbrski-on-csrattrs-00)

Michael Richardson, as author of BRSKI (RFC 8995), described the requirements from the perspective of Autonomic Control Plane (ACP) and BRSKI. ACP requires the SubjectAltName to contains an other name form, which includes an IPv6 prefix. The CSR is the only interface to some devices to get a certificate.

To kick off the discussion, Michael Richardson offered four possible ways to proceed:

1. Fix RFC 7030 CSR Attrs to reflect the ACP/BRSKI understanding.
2. Extend RFC 7030 CSR Attrs ASN.1 to create new mechansim to specify values.
3. Obsolete ASN.1 CSR Attrs, and create new mechanism using CBOR or JSON.
4. Have RFC 8994 and RFC 8995 use a new BRSKI-specific mechansim to specify SubjectAltName, ignoring EST CSR Attrs.

Discussion

Dan Harkins: How are #1 and #2 different?

Michael Richardson: It could be that the ASN.1 was wrong in RFC 7030 (i.e., it didn't include SubjectAltName by mistake). If #1 was correct, then it could be extended to do #2.

Toerless Eckert: I need more information to understand the situation.

Dan Harkins: Not opposed to what BRSKI is doing, he's just explaining how it was intended to be used.

Eliot Lear: There are two problems. First, clients having difficulty parsing the attributes due to library issues. Second, how does the Registration Authority (RA) add attributes.

Max Pritikin: There are multiple cryptography-related attributes to communicate to the client. The intent was for the device to use the CSR attributes to inform its response. He doesn't have an objection to an out-of-band mechanism, but does not see a problem using the CSR attributes to meet the needs of ACP and BRSKI.

Russ Housley: I hear you calling for a clarification document which explains how the CSR Attributes are used to meet the original requirements and the ones from BRSKI. Is that the proposed way forward?

Max Pritikin: Yes.

Dan Harkins: Yes.

Eliot Lear: Yes.

Michael Richardson: Yes, but that may not address the library issue. Perhaps doing this clarification will lead to the needed library support.

Toerless Eckert: Can you clarify? Are you proposing an update to RFC 7030? Are you proposing a standards-track document or an informational document?

Russ Housley: I'd expect a standards-track update to RFC 7030.

Deb Cooley: The update should also deprecate the use of TLS 1.1.

(It was pointed out in the chat that RFC 8996 already accomplishes this.)

Russ Housley: Are their volunteers to work on the document?

(Michael Richardson and Dan Harkins agreed to be authors. Toerless Eckert agreed to help as well.)

Russ Housley (to Roman): Does this need a recharter?

Roman Danyliw: No, he doesn't think so.