draft-ietf-lamps-csr-attestation

Mike Ounsworth, Hannes Tschofenig, Henk Birkholz

LAMPS 119
General Refresher

- This is the “Whatever kind of attestation evidence you have, here’s how you put it in a CSR” Internet-Draft
- New CSR extension `attr-evidence` (or `ext-evidence` for CRMF)
- Carries EvidenceBundles which carries EvidenceStatements and a bag of Certificates
- An EvidenceStatement is an OID and generic value – so just assign yourself an OID and stick in your remote attestation related data.

- This Internet-Draft IS NOT covering how you publish remote attestation data in an X.509 certificate – there are privacy implications here that we don’t want to touch.
New Since Last Time (-02 – -08)

Normative changes

- Hint
  - "The EvidenceStatement includes both a type OID and a free form hint field with which the Attester can provide information to the Relying Party about which Verifier to invoke to parse a given piece of Evidence."
  - See the new Security Consideration 7.3.

```plaintext
EvidenceStatement ::= SEQUENCE {
  type   EVIDENCE-STATEMENT.&id({EvidenceStatementSet}),
  stmt   EVIDENCE-STATEMENT.&Type({EvidenceStatementSet}{@type}),
  hint   EvidenceHint OPTIONAL
}
```

```plaintext
EvidenceHint ::= CHOICE {
  rfc822Name  [0] IA5String,
  dNSName     [1] IA5String,
  uri         [2] IA5String,
  text        [3] UTF8String
}
```

It’s GeneralName with the non-relevant stuff removed. (thanks Russ)
New Since Last Time (-02 – -08)

Non-normative changes

● Greatly expanded the explanation and context text.
● Long discussions on freshness
  ○ Basically, yes freshness / nonces are good, but not always possible in CSR flows, and regardless, how to establish a nonce between Attester and Verifier requires some sort of carrier protocol (ex.: CMP, EST, etc), and a nonce slot in the Evidence format, so is out-of-scope for a CSR draft.
● “Appendix A: Examples” now contains:
  ○ An almost-complete TPM 2.0 example (pending hackathon).
  ○ A complete PSA Token example.
● Creates two IANA Registries:
  ○ "SMI Security for PKIX Evidence Statement Formats"
  ○ “Attestation Evidence OID Registry”
  ○ (see next slide)
New Since Last Time (-02 – -08)

New IANA Registries

● "SMI Security for PKIX Evidence Statement Formats"
  ○ Straightforward – the IETF will undoubtedly need to register OIDs for various Evidence formats, so we need a registry for the mapping of OIDs to Evidence formats.
  ○ Creates this under "SMI Security for PKIX".

● “Attestation Evidence OID Registry”
  ○ Less straightforward.
  ○ Intended for being the one-stop-shop for answering the question: “I’m writing an RP to parse these CSRs, what is the list of EvidenceStatement OIDs that my implementation should be aware of?”
  ○ It’s basically asking IANA to create a table to track OIDs created by other SDOs – inclusion by Designated Expert.

<table>
<thead>
<tr>
<th>OID</th>
<th>Description</th>
<th>Reference(s)</th>
<th>Change Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 23 133</td>
<td>Conceptual</td>
<td>[TCGDICE1.1]</td>
<td>TCG</td>
</tr>
<tr>
<td>5 4 9</td>
<td>Message Wrapper</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Next Steps

- Finish the TPM 2.0 sample (Hackathon)
- WGLC
  - There is great eagerness to implement, so let's get this one closed off.