draft-ietf-lamps-csr-attestation

Mike Ounsworth, Hannes Tschofenig, Henk Birkholz, Monty Wiseman, Ned Smith

LAMPS 120
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
Since we last met our heroes…

● Russ started a WGLC on May 20 (ended June 3)
  ○ Thread received 46 replies. Special thanks to Carl Wallace and Michael StJohns for deep review.
  ○ Generated 13 new github issues [1]. 7 have since been closed; 6 still open.
  ○ We’ll clean up the remaining, then ask for another WGLC.
  ○ In the meantime, we would like to start early Sec AD, SecDir, and expert review (if we can find any experts who are not already involved – Ira McDonald maybe).

● We had a super successful time implementing the draft over the hackathon weekend in Brisbane (which produced the sample data in Appendix A.2).

[1]: https://github.com/lamps-wg/csr-attestation/issues?q=is%3Aissue+created%3A%3E%3D2024-05-20
Resolved Since Last Time (-08 – -10)

Since we last met our heroes…

- Lots of editorial and readability changes.
- Switched from our custom `CertificateAlternatives` to RFC6268 CertificateChoices with the restriction:

```
EvidenceBundle ::= SEQUENCE {
    evidence EvidenceStatements,
    certs SEQUENCE SIZE (1..MAX) OF CertificateChoices OPTIONAL
    -- CertificateChoices MUST only contain certificate or other
}
```

- The intended way to include multiple evidence statements is through multiple EvidenceBundles or multiple EvidenceStatements. So:

```
attr-evidence ATTRIBUTE ::= {
    TYPE EvidenceBundles
    COUNTS MAX 1
    IDENTIFIED BY id-aa-evidence
}
```
Resolved Since Last Time (-08 – -10)

Since we last met our heroes…

- Received IANA early allocation of OID id-aa-evidence so that we could generate samples.

EvidenceBundle ::= SEQUENCE {
  evidence EvidenceStatements,
  certs SEQUENCE SIZE (1..MAX) OF CertificateChoices OPTIONAL
  -- CertificateChoices MUST only contain certificate or other
}
Still open

- **Issue #131: EvidenceStatement.hint**
  - `<HANNES TO FILL IN>`
  - Currently:

```
EvidenceStatement ::= SEQUENCE {
  type   EVIDENCE-STATEMENT.&id({EvidenceStatementSet}),
  stmt   EVIDENCE-STATEMENT.&Type({EvidenceStatementSet}{@type}),
  hint   UTF8String OPTIONAL
}
```

“The hint SHOULD contain a value that is unique to this Verifier, for example, a fully qualified domain name (FQDN), a uniform resource name (URN) [RFC8141], or a registered value corresponding to this Evidence format.”

Still open

- **Issue #139**: the RATS Architecture does not actually define “attestation” or “key attestation”.
  - Clearly a LAMPS CSR spec is not the right place to bury an authoritative definition of those terms.
  - But if anyone knows of an existing definition that we could cite, please let us know.

- **Issue #144**: the DICE CMW example appendix has a stub ASN.1 module which should probably do its imports properly so that it compiles.
  - @NedSmith – this one’s on you to address.

- **Issue #150**: TPM CSR sample has an extraneous empty extensionRequest
  - Mike & Monty need to fix our hackathon sample code.

- **Issue #151**: More feedback on TPM appdx from MSJ
  - This feedback came in July 8; we haven’t looked at it in detail yet.

#139: https://github.com/lamps-wg/csr-attestation/issues/139
#144: https://github.com/lamps-wg/csr-attestation/issues/144
#150: https://github.com/lamps-wg/csr-attestation/issues/150
#151: https://github.com/lamps-wg/csr-attestation/issues/151
Still open

● **Issue #152**: Provide test vectors that exercise all functionality of the draft
  ○ The TPM example nicely exercises the “single evidence statement with cert chain” case.
  ○ For completeness, we should also provide samples of:
    ■ Case 3 - Multiple Evidence Bundles each with Complete Certificate Chains
    ■ Case 4 - Multiple Evidence Bundles with Certificate Transmission Optimization
      even if the actual evidence payload is a stub, like a JWS over the string “evidence”.