CSR Attestation

M. Ounsworth, H. Tschofenig, H. Birkholz, M. Wiseman, N. Smith

Design Team formed and dissolved since 124

- The authors and Mike StJohns had reached a stalemate over design opinions for this draft.
- The authors want to thank **Carl Wallace**, **Steve Hanna**, and **Tim Polk** for hearing out both design options and taking a deep editorial pass over the document.
- The authors merged almost all of the changes recommended by the DT – very helpful.

Status

- Version -22 largely reflects the changes made by the design team. Additional changes includes:
  - editorial updates,
  - author info updates,
  - Minor ASN.1 updates regarding
  - Minor terminology adjustments.
- Following discussions on the mailing list we removed the Attestation OID Registry in version -23
- We are down two two open PRs on https://github.com/lamps-wg/csr-attestation/pulls

PR 232

Changes in the PR are accepted except for this:

> Certification Authorities (CAs) issuing certificates to PKI end entities MAY require a certificate signing request (CSR) to include verifiable attestations that contain claims regarding the platform used by the end entity to generate the key pair for which a certificate is sought and also contains claims of attributes of the key pair with respect to its protection, use and extractability. At the time of writing, the most pressing

MSJ believes that this MAY is required for interoperability issues. HT disagrees.

"Attribute"

```
ATTESTATION-STATEMENT ::= TYPE-IDENTIFIER

AttestAttrSet ATTRIBUTE ::= { ... }

AttestationStatement ::= SEQUENCE {
   type   ATTESTATION-STATEMENT.&id({AttestationStatementSet}),
   bindsPublicKey [0] BOOLEAN DEFAULT TRUE,
   stmt   ATTESTATION-STATEMENT.&Type({AttestationStatementSet}{@type}),
   attrs  [1] Attributes {{AttestAttrSet}} OPTIONAL
}
```

- The authors are not convinced that promoting the “Hint” to a full-blown CMS Attribute is the correct resolution
- This seems to be introducing more complexity than is really warranted.
- At this point perhaps we should just drop the Hint / Attributes entirely?
- If an attester needs to carry aux data, then they need to define an attestation stmt encoding that includes it.
    - As you would expect, this has spawned a new round of design discussion and debate.

PR 236

PR 236 attempts to change ASN.1 back to the pre-DT days:

```
- AttestAttrSet ATTRIBUTE ::= { ... }
-
  AttestationStatement ::= SEQUENCE {
     type   ATTESTATION-STATEMENT.&id({AttestationStatementSet}),
-    bindsPublicKey [0] BOOLEAN DEFAULT TRUE,
     stmt   ATTESTATION-STATEMENT.&Type(
-                {AttestationStatementSet}{@type}),
-    attrs  [1] Attributes {{AttestAttrSet}} OPTIONAL
+                {AttestationStatementSet}{@type})
  }
```

Requires more discussion

Next Steps

… design work continues, stay tuned 😉