# Attestation Nonces

draft-tschofenig-lamps-nonce-cmp-est-00

Hannes Tschofenig, Hendrik Brockhaus

**Hendrik Brockhaus**

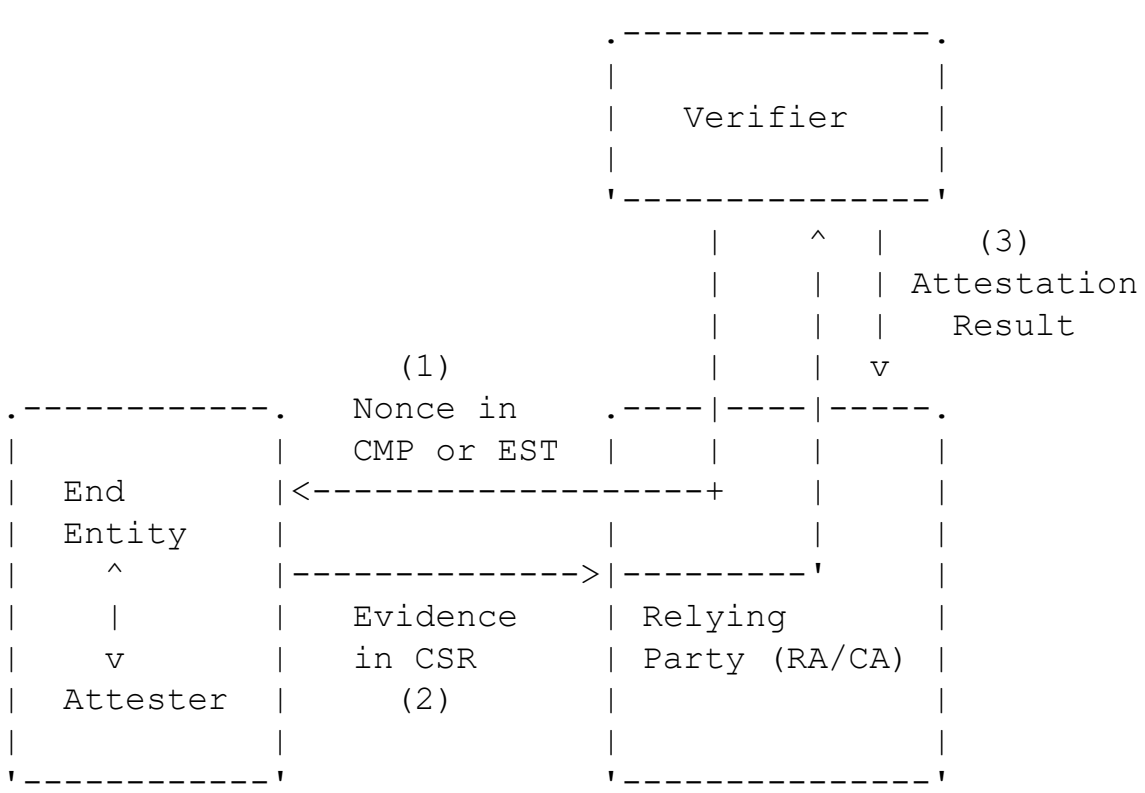
IETF 118 – LAMPS Working Group

# Activities since IETF 117

Changes since IETF 117:

- Added an ASN.1 module
- Added nonce transfer via EST
- Draft on github.com/hannestschofenig/tschofenig-ids

# Providing attestation nonce




(1) The nonce is obtained from the Verifier by the RA/CA and transferred to the EE using an extension to CMP/EST.

(2) The EE uses the CSR extension of [I-D.ietf-lamps-csr-attestation] to convey Evidence provided by the Attester to the RA/CA.

(3) The Verifier processes the Evidence received and returns an Attestation Result to the RA/CA (Relying Party).

# Requesting attestation nonce using CMP/EST

CMP

- The EE requests a Certificate Request Template (see RFC 9480 Section 2.16 and RFC 9483 Section 4.3.3)
- The RA/CA adds an EvidenceNonce extension containing the nonce to the CertReqTemplateContent

EST

- The EE requests CSR Attributes (see RFC 7030 Section 4.5.1)
- The RA/CA adds an EvidenceNonce in the attributes contained in CSR attributes (see RFC 7030 Section 4.5.2, RFC 8295 Appendix B, or draft-ietf-lamps-rfc7030-csrattrs Section 3).