

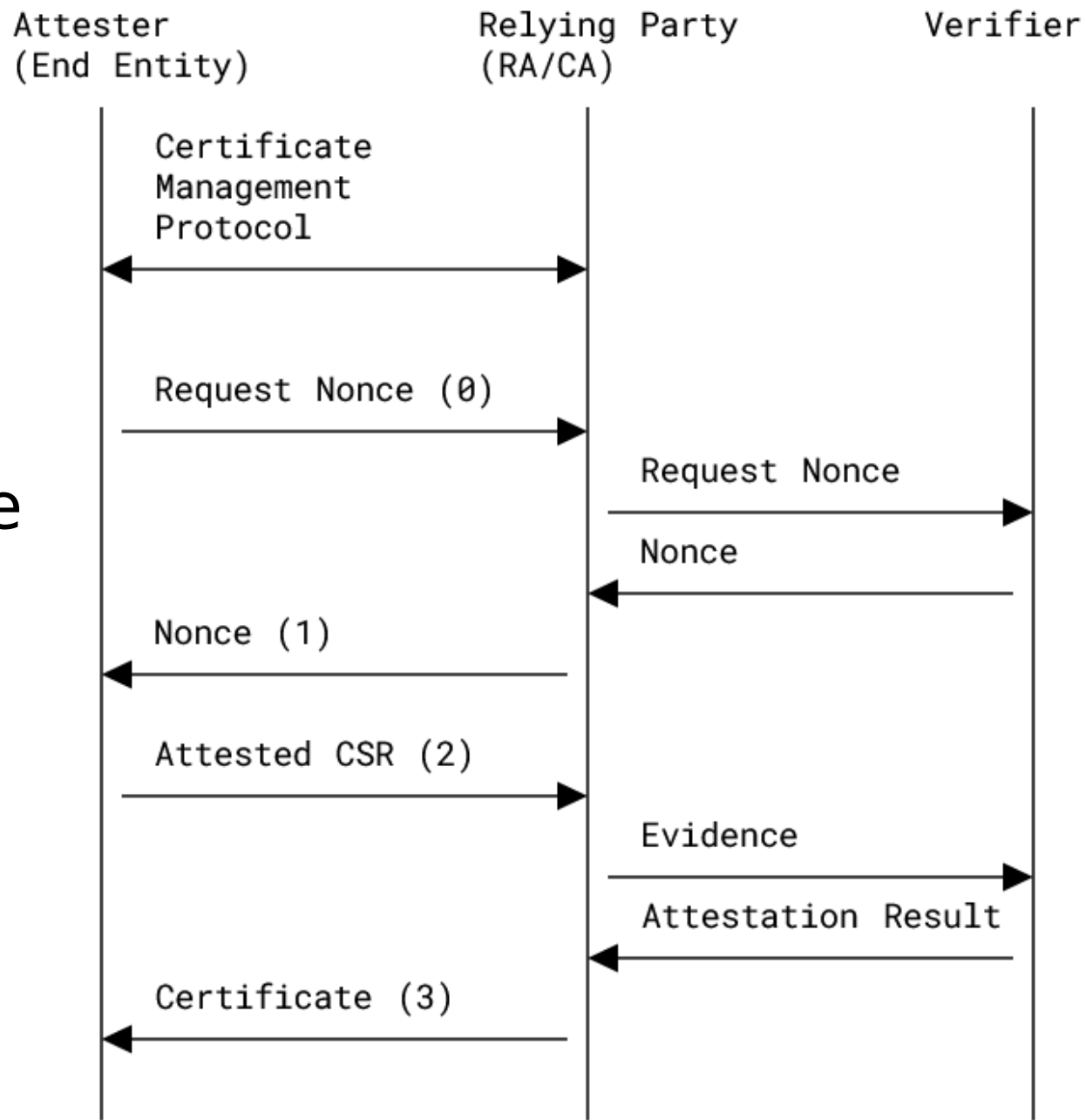
Nonce-based Freshness for Remote Attestation in Certificate Signing Requests (CSRs) for the Certification Management Protocol (CMP) and for Enrollment over Secure Transport (EST)

draft-ietf-lamps-attestation-freshness

Hannes Tschofenig, Hendrik Brockhaus

Architecture

- Updated ASN.1
- Editorial update
- Support for multiple nonce structures.



Next Steps

- Alignment with CSR attestation draft
- Better understanding of anticipated remote attestation deployment model