Nonce-based Freshness for Remote Attestation in CSRs for CMP and EST

draft-tschofenig-lamps-nonce-cmp-est-01

Hannes Tschofenig, Hendrik Brockhaus
Motivation

- **draft-ietf-lamps-csr-attestation** defines the ability to carry attestation evidence in a CSR
- CSR is a one-shot message and the draft discusses freshness of evidence:

  “Evidence generated by an Attester generally needs to be fresh to provide value to the Verifier since the configuration on the device may change over time.

  ...

  Developers, operators, and designers of protocols, which embed Evidence-carrying-CSRs, MUST consider what notion of freshness is appropriate and an available in-context; thus the issue of freshness is left up to the discretion of protocol designers and implementers."

"
Design Approach

- New messages for CMP/EST defined based on IETF#118 hackathon experience.
- Section 10 of RFC 9334 discusses different approaches for providing freshness:
  - a nonce-based approach,
  - the use of timestamps, and
  - an epoch-based technique.
- draft-tschofenig-lamps-nonce-cmp-est-01 defines how to exchange nonces in CMP and EST.
A little more details

• CMP

GenMsg: {id-it TBD1}, NonceRequestValue
GenRep: {id-it TBD2}, NonceResponseValue | < absent >

id-it-NonceRequest OBJECT IDENTIFIER ::= { id-it TBD1 }
NonceRequestValue ::= SEQUENCE {
    len INTEGER OPTIONAL, 
    -- indicates the required length of the requested nonce
    hint EvidenceHint OPTIONAL 
    -- indicates which Verifier to request a nonce from
}

id-it-NonceResponse OBJECT IDENTIFIER ::= { id-it TBD2 }
NonceResponseValue ::= SEQUENCE {
    nonce OCTET STRING 
    -- contains the nonce of length len
    -- provided by the Verifier indicated with hint
    expiry Time OPTIONAL 
    -- indicates how long the Verifier considers the 
    -- nonce valid
}

• EST

<table>
<thead>
<tr>
<th>Message type</th>
<th>Media type(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(per operation)</td>
<td>N/A (for GET) or application/json (for POST)</td>
</tr>
<tr>
<td>Nonce Request</td>
<td>application/json</td>
</tr>
<tr>
<td>Nonce Response</td>
<td>application/json</td>
</tr>
</tbody>
</table>
Next Steps

• Missing component in the key attestation architecture.

• Relatively simple but DDoS mitigation technique may need to be addressed using stateless ticket approach.

• Call for adoption?