Hash Of Root Key Certificate Extension

draft-ietf-lamps-hash-of-root-key-cert-extn-00

Russ Housley
LAMPS WG at IETF 103
July 2018

Hash Of Root Key Cert Extension

- A certificate extension carried in the self-signed certificate for a trust anchor to identify the next public key that will be used by the trust anchor
  - Publish the hash value of the next generation public key in the current self-signed certificate
  - Allows a relying party to unambiguously recognize the next generation public key when it becomes available

Overview

Initial deployment of the Root CA

R1 = The initial Root key pair

C1 = Self-signed certificate for R1, which also contains H2

R2 = The second generation Root key pair

H2 = Thumbprint (hash) of the public key of R2

When the time comes to replace the initial Root CA certificate

R3 = The third generation Root key pair

H3 = Thumbprint (hash) the public key of R3

C2 = Self-signed certificate for R2, which contains H3

And so on …

Cert Extension Syntax

```
 ext-HashOfRootKey EXTENSION ::= {    -- Only in Root CA certificates
     SYNTAX         HashedRootKey
     IDENTIFIED BY  id-ce-hashOfRootKey
     CRITICALITY    {FALSE} }

HashedRootKey  ::=  SEQUENCE {
     hashAlg        HashAlgorithmId,     -- Hash algorithm used
     hashValue        OCTET STRING }     -- Hash of DER-encoded
                                       --   SubjectPublicKeyInfo

HashAlgorithmId  ::=  AlgorithmIdentifier

id-ce-hashOfRootKey OBJECT IDENTIFIER  ::=  { 1 3 6 1 4 1 51483 2 1 }
```

WG Last Call

- Security Considerations were expanded based on the discussion at IETF 102

- The document is in LAMPS WG Last Call
- Please review and comment

- Tim will make all LAMPS WG consensus calls related to this *informational* document