One Statement Certificate Policies

Milan Sova

The problem

- “Was this certificate issued to a host or to a person?”
- “Is the private key stored on a hardware token or in a software?”
- “Is the private key encrypted?”
- “Was the private key generated by the subscriber or by the issuing CA?”
- …

Proposed solution

- Define a “One Statement” Certificate Policy for every property, e. g.:
  - certificate issued for a physical person
  - certificate issued for a network entity
  - keypair generated on a hardware token
  - keypair generated by the subscriber
  - …

1SCP example – host certs

- RFC 3647
- 1.1 Overview
  “This CP describes requirements certificates issued for internet hosts...”
- 1.1.2 Subscribers
  “Certificates issued under this CP MUST be issued only for internet hosts...”
- (Almost) all other sections
  “No stipulation.”

1SCP example – host certs

- Assign an OID for the policy

  ```
  id-1scp-internet-host
      { igtf id-certificatePolicies 1 }
  ```

- Publish the CP
- CAs then include the OID into the **`certificatePolicies`** extension of host certs (together with other relevant policy OIDs)

1SCP processing

- RPs keep a list of required/forbidden certificate properties (OIDs)
- Compare the OIDs from the cert with the requirement list => cert suitability

Side-effects

- Policies standardization
- Motivation for RP to deal with certificate extension and `certificatePolicies`