Certificate Policy & Certification Practices Statement Internet Drafts

Steve Kent

BBN Technologies

Context

- RFC 3647 (Informational) provides an outline and explanatory text for defining
  - A certificate policy (CP)
  - A certification practice statement (CPS)
- This RFC is very widely cited
  - Essentially every large scale PKI publishes a CPS and uses the outline from 3647 as its model
  - When a certificate issuer publishes a certificate policy (CP), it also tends to follow the format defines in this RFC
- There is one outline in 3647; it nominally applies to both CP and CPS documents

What is a CP?

- X.509 defines a certificate policy as

  > "a named set of rules that indicates the applicability of certificate to a particular community and/or class applications with common security requirements"

- A CP provides guidance to replying parties, to help them know whether a certificate is appropriate for use in conjunction a specific application
- A CP provides liability protection for a CA, by declaring the intended range of uses for the certificates it issues

Do We Need a CP?

- Because the resource certificates being defined in SIDR are targeted to a specific application context (not generic), it seems especially important to define a CP consistent with the anticipated range to uses for these certificates
- Even if multiple resource certificate PKIs arise, e.g., for use in the public Internet vs. private nets, the same CP is probably applicable
- A CP is "named" by an object identifier (OID) and we already have an OID for this policy:

```
 id-cp-ipAddr-asNumber OBJECT IDENTIFIER ::= { iso(1)
identified-organization(3) dod(6) internet(1) security(5)
mechanisms(5) pkix(7) cp(14) 2 }
```

Resource Certificate PKI CP

- RFC 3647 assumes that a PKI will not use ALL of the outline elements in the RFC
- Apropos, the CP I-D is a profiled subset of 3647, reflecting the authors’ perception of what is relevant to the resource certificate PKI
- The result is a document a bit under 45 pages, as opposed to RFC 3647, which is a bit under 100 pages!
  - The document maintains section level numbering consistency with 3647, to make it easy to compare with other CPs

A CP Outline Snippet

```
4.0 Certificate Life-Cycle Operational Requirements
      Certificate Application
      Certificate application processing
      Certificate issuance
      Certificate acceptance
      Key pair and certificate usage
      Certificate renewal
      Certificate re-key
      Certificate modification
      Certificate revocation and suspension
```

What is a CPS?

- A CPS is defined by RFC 3647 as

  "a more detailed description of the practices followed by a CA in issuing and otherwise managing certificates […] published by or referenced by the CA"

- A CPS is CA-specific document, whereas a CP may be common across many CAs
- A CPS also documents the means by which subjects and relying parties interact with a CA
- A CPS may used by relying parties to select a CA
  - For certificate issuance, from among multiple candidates
  - As trust anchor, from among multiple suitable candidates

Do We Need a CPS?

- Yes!
- We need a standard way to document the means by which subjects and relying parties interact with the CA for
  - Certificate requests
  - Certificate revocation requests
  - Certificate distribution
  - Revocation status data distribution
  - Etc.

Resource Certificate CPS Template

- Unlike the CP, a CPS is per-CA, so this I-D has lots of “fill in the blank” text areas, to allow each CA to customize it
- This document is 45 pages, but when a CA fills in the text that it must to complete the document, it will be much bigger
- As with the CP, the document maintains section level numbering consistency with 3647, to make it easy to compare with other CPSs
- This template is intended for RIRs & NIRs; another template for ISPs may be needed

A CPS Outline Snippet

6.0 Technical Security Controls

- Key pair generation and installation
- Private Key Protection and Cryptographic Module Engineering Controls
- Other aspects of key pair management
- Activation data
- Computer security controls
- Life cycle technical controls
- Network security controls

Summary

- These two I-Ds are intended to become informational RFCs in support of the SIDR work
- Additional CPS Templates for CAs at other points in the resource allocation hierarchy may be needed
- Comments are welcome!