Resource PKI: Certificate Policy & Certification Practice Statement

Dr. Stephen Kent
Chief Scientist - Information Security

Terminology

- Certificate: a digitally-signed data structure
  - typically an X.509 public key certificate (PKC), the certificate standard adopted by the IETF and employed in SSL/TLS, IPsec (IKE), S/MIME, and many other IETF security protocol standards
- Certification Authority (CA): an entity that issues (digitally signs) certificates, aka an Issuer
- Subject: an entity to whom a certificate is issued; for a PKC, the subject is the holder of the private key corresponding to the public key in the certificate

More Terminology

- Relying party (RP): an individual or organization that takes actions based on using a public key from a certificate
- Trust anchor (aka root): a public key and associated data used as a reference for validating certificates
  - A trust anchor is often represented as a self-signed certificate, but it need not be
- PKI: a set of procedures, policies, and technical measures employed to manage (issue, renew, revoke, publish) certificates

CP & CPS RFCs

- 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 usually follows the format defined 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 with a specific application
- A CP provides liability protection for a CA, by declaring the intended range of uses for the certificates issued by the CA

Do We Need a CP for this PKI?

- The certificates being defined for the resource PKI are targeted to a specific application context (not generic), so it seems especially important to define a CP consistent with the anticipated range of uses for these certificates
- A CP for this PKI is being developed under the auspices of the SIDR WG in the IETF; it will become an Informational RFC
- 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
- The CP Internet Draft 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 consistent with 3647, to make it easy to compare with other CPs

What Does a CP Describe?

- The purpose of the PKI
- PKI participants (CAs, Subscribers, RPs)
- How certificates and CRLs are published (repository model)
- Allowed and prohibited uses for certificates in the PKI
- Name forms allowed in certificates
- Procedures for certificate issuance, acceptance, revocation, re-key, and modification
- Etc.

An Excerpt from the CP I-D

1.3.4. Relying parties

Entities that need to validate claims of address space and/or AS number current holdings are relying parties. Thus, for example, entities that make use of address and AS number allocation certificates in support of improved routing security are relying parties. This includes ISPs, multi-homed organizations exchanging BGP traffic with ISPs, and subscribers who have received a “portable” allocation of address space from a registry.

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 in the same PKI
- 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 for this PKI?

- 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
  - CRL distribution
- Here the choice of CAs is dictated by the resource allocation hierarchy, so a CPS is not needed to help choose a CA!

Resource Certificate CPS Template

- Unlike the CP, each CPS is a per-CA document, so this I-D has lots of "fill in the blank" text areas; each CA must customize its version of the CPS
- 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 will be produced

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 on track to become Informational RFCs, from the SIDR WG
- A CPS Template for ISPs will be submitted later in the first quarter of 2007
- Comments from registries and ISPs are needed to ensure that these documents are appropriate!

Questions?