Trust Anchor Management (TAM) Specifications

November 20th, 2008

Carl Wallace
cwallace@cygnacom.com

Suggested Way Forward (from Dublin)

- Update requirements draft and progress as Informational
- Adopt modified TAMP draft as a Standards track working group draft
  - Move TrustAnchorInfo specification from TAMP to separate draft
  - Provide capability to manage alternative TA formats
    - Minimally, Certificate and TBSCertificate
    - Extensible to support TrustAnchorInfo (and others?)
  - TAMPUpdate would be the primary structure
    - Suitable for directory-based distribution
- Submit new TrustAnchorInfo and CMS Content Constraints drafts compatible with PKIX TAMP

Since Dublin

- Performed each of the suggested items
- Current drafts
  - draft-ietf-pkix-ta-mgmt-reqs-02
    - Two revisions since Dublin
  - draft-ietf-pkix-ta-format-00
    - New draft split out from TAMP
  - draft-ietf-pkix-tamp-00
  - draft-ietf-pkix-cms-content-constraints-00
    - Mostly minor changes vs. -00 individuals submissions

TAM requirements changes

- Initiated WG LC for -01 draft
  - Addressed comments and submitted -02 draft
- Changes
  - Adopted 2119 language throughout
  - Collapsed old requirements 3.8 and 3.9 into one section
  - Added additional security considerations
  - Various clarifications/edits

TAMP changes

- TrustAnchorInfo format moved to standalone specification
- TAMP messages extended to support managing trust anchors other than TrustAnchorInfo
- Certificate option added per WG comments.
- tbsCert added as alternative to TrustAnchorInfo for associating constraints with a certificate.

```
TrustAnchorChoice ::= CHOICE {
  certificate     [0] EXPLICIT Certificate,
  tbsCert         [1] EXPLICIT TBSCertificate,
  taInfo          [2] EXPLICIT TrustAnchorInfo }
```

TA Format changes

- Separates format from protocol spec
  - Text is essentially same as what was removed from TAMP
  - Added an extensions field
  - Made contingency key field optional in ApexTrustAnchorInfo

CCC changes

- No significant changes vs. -00 individual submission

Document Reorganization

- Remove CCC from working group
  - Re-submit as personal draft (as before)
- Remove CCC and clearance constraints fields from TrustAnchorInfo structure
  - Remainder will be compact representation of TA information that allows binding constraints to a certificate
  - Add new content type for sequence of trust anchors
  - CCC and clearance constraints can be carried as extensions by those who want to use them

Document Reorganization (continued)

- Remove CCC fields from TAMP
  - Relocate sequence number conveyance to signed attribute (possible)
- Clarify requirements draft as addressing TA management for push environments only

Suggested Way Forward

- New working group last call for new requirements draft after IETF
  - draft-ietf-pkix-ta-mgmt-reqs-03.txt
- Hold working group last call for revised TrustAnchorInfo draft as soon as practical
  - draft-ietf-pkix-ta-format-01.txt
- Revise TAMP spec
  - draft-ietf-pkix-tamp-01.txt
  - Aim for last call shortly after San Francisco