Trust Anchor Management (TAM) Specifications

July 29th, 2009

Carl Wallace
cwallace@cygnacom.com
Suggested Way Forward (from San Francisco)

- Hold working group last call for revised TrustAnchorInfo draft
  - draft-ietf-pkix-ta-format-01.txt
- Revise TAMP spec
  - draft-ietf-pkix-tamp-01.txt
  - Hold WG last call as soon as practical
- Submit new individual submission that discusses usage of TA-based constraints
Since San Francisco

• Several revised drafts
  – Two revisions of TAF
  – One version of TAMP
  – New individual draft
    • Using Trust Anchor Constraints During Certification Path Processing

• TAF completed WGLC
  – After brief delay, entered IETF last call
    • A few minor comments will result in a new draft
      – Most significant is addition of optional pathLenConstraint field to CertPathControls structure
Since San Francisco (continued)

• Current PKIX drafts
  – draft-ietf-pkix-ta-format-01
  – draft-ietf-pkix-tamp-03

• Related
  – draft-wallace-using-ta-constraints-00
  – draft-housley-cms-content-constraints-extn-01
Preview of pending TAMP changes

- Next version will include following changes
  - Fixed some tagging issues in ASN.1 module
  - Changed TampStatusResponse to allow apex support to be omitted or phased in (similar change toVerboseUpdateConfirm)

```plaintext
-- old definition
TAMPStatusResponse ::= SEQUENCE {
    version   [0] TAMPVersion DEFAULT v2,
    query     TAMPMsgRef,
    response  StatusResponse }

-- new definition
TAMPStatusResponse ::= SEQUENCE {
    version   [0] TAMPVersion DEFAULT v2,
    query     TAMPMsgRef,
    response  StatusResponse,
    usesApex  BOOLEAN DEFAULT TRUE }
```
Implementation

• Software that uses TAF, TAMP, CCC and UTAC has been developed
  – Intended for release via Source Forge
  – Targets applications enabled using CAPI
    • Allows enforcement of TA-based constraints using a trust anchor store that is managed using TAMP

• Components include
  – PKIFTAM
  – CapiStoreToTampStore
  – CAPI Trust Anchor Guard (CapiTag)
  – StoreManager
  – mod_tam
Component Details

• PKIFTAM
  – Library that augments PKIF to add support for TAF, TAMP, UTAC and CCC
    • Encoder/decoder
    • Path validation using TA-based constraints
    • TAMP-aware trust anchor store
    • PKIF details are here: www.pkiframework.com
      – PKIFTAM not yet released

• CapiStoreToTampStore
  – Utility to copy trust anchors from a CAPI root store to a PKIFTAM trust store
Component Details (continued)

• **CAPI Trust Anchor Guard (CapiTag)**
  - Integrates with Windows as a certificate store provider
  - Intercepts calls to CertGetCertificateChain
    - TA-based constraints enforcement mode
      - Post-processes calls to native CertGetCertificateChain and changes error codes, if necessary
    - CAPI replacement (i.e., could act as an SCVP client – this feature not presently implemented)

• **StoreManager**
  - GUI utility that uses TAMP to view and manage CapiTag local or remote trust anchor stores
    - Remote stores accessed via TAMP over HTTP

• **mod_tam**
  - Apache module that provides HTTP interface to manage CapiTag TA stores
  - Periodically retrieves TAMP messages from remote sources
Suggested Way Forward

• Wrap up IETF last call for TAF
• Hold working group last call for revised TAMP draft
  – draft-ietf-pkix-tamp-03.txt (will be submitted in August)
• Address expiration of requirements draft
  – No change version bump, allow to expire, progress towards informational?