Trust Anchor Management (TAM) Specifications

November 10, 2009

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

• 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?
Since Stockholm

- Several revised drafts
  - One new version of TAF
  - Two new versions of TAMP (in October, not August, as planned)
  - One new version of TAM Requirements (version bump only)
- TAF completed IETF LC
- TAMP entered WG LC
  - Some minor edits resulted in new version
Since Stockholm (continued)

• Current PKIX drafts
  – draft-ietf-pkix-ta-format-04
  – draft-ietf-pkix-tamp-04
  – draft-ietf-pkix-ta-mgmt-reqs-04

• Related
  – draft-wallace-using-ta-constraints-01
  – draft-housley-cms-content-constraints-extn-02
    • -03 version will be posted soon to correct mistake in
      ASN.1 module introduced in -01 draft
TAM Requirements changes

• Version bump only due to I-D expiration
TAF changes

- Added reference to X.680 to introduction
- Clarify some references to TA entities vs. TA information
- Clarification regarding usage of version field
- Added pathLenConstraint to the CertPathControls structure
- Added field to provide language tag for the TA title field
TAMP changes

• -03 includes changes previewed in Stockholm
  – Corrected a tagging issue with VerboseApexUpdateConfirm
  – Added usesApex field to TAMPStatusResponse and VerboseUpdateConfirm
  – MIME type registration information
  – TAMP over HTTP appendix
  – Corrected import statements in ASN.1 module to refer to modules in new ASN.1 document
TAMP WG LC

• Changes made resulting from WG LC
  – Clarify references to TA entity vs. TA information
  – Incorporate trust anchor store definition from TAM requirements draft
  – Assorted editorial changes

• Proceed with IESG submission?
  – Outstanding issues best addressed independent of this draft, if there is interest (i.e., EKU constraints, TA validity)
Suggested Way Forward

• Address any RFC editor issues with TAF
• Submit TAMP to IESG
  – Address any IESG last call issues for TAMP
• Submit TAM requirements draft to IESG as informational