Group D Profile Presentation

Profiles scope

• Definition of profile vs. framework
  – Profile is list of answers (f/w is the questions)
  – Refines the f/w
  – Assist a designer of a CKMS, given the f/w
• Profiles can be created/based on risk situation / sector
  – Implies verticals, and coupled requirements (financials, federal, ...)
• Profiles can also be based on the key usage scenarios (archiving, network security, ...)
  – More natural as it focuses on the purpose of the system rather than it being used by a vertical
  – The vertical may then add specific reqs to this
  – Scope of the CKMS will also influence the profile
  – Regulatory aspects? (may influence e.g. key compromise recovery)
Profile Scope cont.

- **Profile should leverage** (and may be composed of) **existing specifications** (NIST and others)
- **Certain physical components** may be in scope
  - But this is the **keys**, not the **application data** protected by the CKMS (out of scope)

Profile “Depth” and Relationship to Compliance

- CC PPs/TOEs?
  - Costly, time-consuming
- **NIST profile may be seen as a “map” through the f/w**
  - May have multiple “paths” -> levels (loosely analogous to FIPS 140)
  - Concern is that the validation of a CKMS may be vastly more complex than validation of a CM
- **Compliance may be more to the design document level than the implementation level**
Profile Conformance

• Profile is by nature more prescriptive on security requirements but would tend to stay away from general system requirements (e.g. regarding performance)

• Self-certification of CKMS as a whole may suffice since claims can be associated with, e.g., conformance / certification to underlying standards

Examples of existing CKMSs

• Could be used as starting points for profile work

• Include: ATM CKMs, Cell phone CKMs, PKI CAs, Storage (1619...), OASIS, ...

• Architectures may range from hierarchical, peer-peer (implying diversity of authorities)
Profile and Interop

- Again, depends on CKMS purpose
- **May be totally fine to not have interop abilities with other CKMS entities**
- Or may be required (e.g. cell phone roaming)
- Metadata on keys complicates (app-level reqs)
- **For a federal CKMS profile, interop may be a daunting task unless narrowed down substantially** (e.g. to algorithms)

Profile doc as such

- **Given expected multitude of profiles, makes more sense as separate document**
  - More suitable if Framework is more informative / declarative
  - “Build” Requirements could be in profile doc
  - **Could capture additional aspects such as testing facilities**
  - On user satisfaction requirement, group finds this subjective and difficult to capture in measurements