Profile Breakout – Group A

- Most discussion about:
  - Scope of profiles
  - Construction of profiles
  - Conformance
- Still lots of discussion about scoping and what various words mean – profile, design, etc.
- However, this is a very complex area and the consensus was that having a framework and profile is valuable.

What is a profile?

- A profile looks like the framework, just more detailed.
  - Framework, profile, and design all apply to the same system.
  - Profile is system level, not product level. No low-level details.
  - Describe the specific risk management tradeoffs that are relevant in a particular context.
  - Don't become a Common Criteria PP.
  - USG profile: Basic requirements on "what a government agency would do" taking into account all the relevant NIST requirements on cryptography, OS security, physical security, how to perform assessments, etc.

Layers of Profiles

- Is the profile really a requirements profile or a design profile? E.g. customers could generate requirements profiles and vendors could generate design profiles that try to match.
  - Or maybe we say “security requirements” vs. “design requirements”.
  - Or maybe we have profiles for functional units.
  - Or maybe application classes (e.g. web apps).
- Layers of profiles
  - Each profile fleshes out the parent profile for a specific context. Refine until you get to a vendor profile.
  - But too many profiles would get confusing. More than two layers is probably overkill.
- How do “company policy and standards” interact with this? Are they outside the profile or part of it?

Creating a Profile

- Profiles are very difficult to do because of the number of things that must be captured. E.g. some CKM systems have very short cryptoperiods.
  - Concern about NIST resourcing.
  - Can we get a standards body to volunteer? E.g. X9.24 Part 2 could be a profile. But this is also a resourcing issue.
  - Valuable for NIST to maintain a list of examples.
  - Don’t go to CC-land.
- How much detail?
  - Right now it is valuable simply to identify needs and gaps in existing interfaces and technologies, e.g. archiving and how is archiving keys different from archiving other data.
  - Not clear what level of detail goes in framework vs. profile vs. elsewhere.
- Maybe a profile construction kit with examples? E.g. FISMA tool.

One Profile or Many?

- Aren't CKM best practices the same for everyone?
  - Different compliance requirements and industry standards. (see diagram in framework draft)
- The first profiles defined will serve as examples to the community.
  - Toy examples or real-world?
  - Having examples that are too few or too narrow will cause people to view the applicability of the framework narrowly.
  - Possibilities: first responders, control towers, health care, FOIA declassification
- For USG, could NIST do different profiles based on high / medium / low security level?
  - Maybe sub-profiles for particular agencies or application classes?

Related Work

- If we think of layers of profiles – requirements profiles and functional profiles – existing frameworks are at the lower (functional) layer. Examples:
  - KMIP
  - PKI (X.509, PKIX)
  - PCI
  - ZigBee
  - TCG Storage (e.g. Opal)
  - IEEE P1619.3
  - OASIS EKMI
  - NSA Trusted Computing
  - Various proprietary products
- Pacific Northwest Labs is doing a KM whitepaper.

Assessments

- Who is responsible?
  - Customer does the assessment for the as-deployed system.
  - Profile needs to specify assurance procedure and product responsibilities
  - Vendor tries to meet profile in their design
- What do we measure conformance of?
  - Profile: Body that writes the profile has a review process.
  - Design document: Product should be well documented and enable safe implementation choices. Profile should specify what needs to be documented.
  - Specific deployment: Too hard
- What is NIST's role?
  - These are complex systems, and the only artifact is documentation.
  - NIST could do validation for the USG profile. Maybe just an RFI-style process would be enough.
  - Don't want to end up with another expensive CC-style process.
  - Maybe we need to wait until we have a profile so we can understand this further. Not clear how much value is added by complex validation.

Other Topics

- Interoperability
  - Not mature yet
- User satisfaction
  - Hard to measure.
  - CKM should be invisible, it should just happen in the flow of other things that users understand.
  - Maybe usability of CKM is just administrator usability?