

Framework Group D Report

- What is the primary use of the Framework?
 - Use by a product designer to design a CKMS?
 - Use by potential CKMS product customers to compare competing CKMS designs/products?
 - Use by NIST Profile Team to create a Profile?
 - Use as a Template to describe CKMS?
 - Use as a Homogeneous Thinking Model on CKMS?
 - Use by CKMS Evaluators as a checklist?

Framework VS Profile

- Is a Framework needed once a Profile is done?
- Is a Profile a tailored version of a Framework?
- Should the Framework be a Taxonomy?
- How can one Profile cover so many CKMS alternatives?

Framework Suggestions

- More diagrams are needed for design and engineering processes for CKMS.
- A Chain of Trust model is needed to evaluate different alternatives for CKMS design.
- A comprehensive taxonomy of the broad spectrum of CKMS alternatives is needed.
- A comprehensive document is needed for design and implementation of CKMS alternatives

Framework Suggestions

- Core functionality (e.g., security) should have priority over lesser goals (e.g., performance, ease of use); Note that there was not consensus on this suggestion.
- Framework and Profile should not restrict technology, innovation, new applications.
- Requirements should be reviewed for balance, easement of verification, utility

Security Policy

- Diagram in Framework was useful
- Policy should start with organizational goals
- Requirements should be specified and used that implement, enforce, and that are derived from policy.
- Policies should be encoded so that Security Domains can use, negotiate, and enforce them
- A CKMS should be a magnification of policy

Roles and Responsibilities

- List of Roles in Framework was too long.
- Should be restricted to people; Note, some felt devices should be personified to perform these.
- Roles must be defined in a context of trust.
- There should be multiple models of trust.
- Should be clear that not all roles are needed for all CKMS.

Terminology

- Framework could be called “Considerations” or “Fundamental Components”; Note, there was not consensus on this.
- CKMS Profile may not be consistent with common use of Profile in standards usage.
- Framework should have precise definitions to establish basis of discussion, design, use.
- Some definitions are inaccurate or incomplete.

Suggestions

- More diagrams, flow charts, models, charts, etc. are needed for clarity and understanding.
- A taxonomy is desirable to understand how a CKMS is designed for some {security domain : application set : communication topology}.
- Consistency of requirements and treatment of alternatives is needed.

Observations

- Creating a good CKMS Framework is a difficult task.
- Creating a good CKMS Profile is a VERY difficult task.
- Both documents could be useful if written for a specific audience (e.g., CKMS designers); Note, some felt should be written to be useful to multiple audiences.