Summary of Second Round Public Comments on SP 800-130

September 10, 2012

Elaine Barker

Dennis Branstad

Miles Smid (Presenter)

What is the CKMS Framework?

- The Framework provides design documentation requirements.
- A Framework is an organized list of Framework topics and individual CKMS design documentation requirements.
- The Framework asks for a complete specification of the CKMS

What is a CKMS Profile?

- A CKMS Profile provides the requirements that a qualifying CKMS, its implementation and its operation must meet.
- A CKMS Profile specifies how the CKMS must be designed, implemented, tested, and operated.
- A CKMS Profile is limited to a particular group or area of interest (e.g. US Government and government contractors)

Framework/Profile Differences

- Framework
  - – Asks for a description of the CKMS.
  - – The CKMS Framework is not judgmental. Any CKMS could comply.
  - – E.g., Specify all cryptographic algorithms used.
- Profile
  - – States what makes a satisfactory CKMS.
  - – The CKMS Profile makes judgments as to what is necessary and what is not necessary. All CKMS may not comply.
  - – E.g., Only NIST Approved cryptographic algorithms **shall** be used

Comments Received

- Chii-Ren Tsai, Citigroup
- Ben Nick, Microsoft

Summary of Comments

- The requirements described in this Framework are quite comprehensive.
- It may not be straightforward to figure out which requirements are needed.
- The framework could start with a reference architecture to highlight core components, protocols and interfaces, and then associate KM requirements with architectural components and interfaces.

Summary of Comments (2)

- It is difficult to support existing or legacy applications. Such applications may deviate from certain Framework requirements.
- It would be beneficial if standard interfaces/API and implementation guidelines were developed.

Summary of Comments (3)

- Dual control is required for certain key management functions (e.g., key recovery, permanent destruction of keys, key export in plaintext, etc.) in a CKMS.
- We are happy to participate in this standardization process.
- It is not clear from the document which requirements are necessary for which use cases.

Summary of Comments (4)

- It would be helpful if requirements were organized by use case so that vendors and CKMS designers could determine which requirements applied to which product design.
- SP 800-130 requirements target the CKMS designer, not the component vendors directly.

Summary of Comments (5)

- It might be helpful to have a section or companion document that targets the vendor and defines requirements specifically for conforming products
- Requirements should contain objective criteria for determining conformance.
- Some requirements are likely common to all CKMS (e.g., FIPS Cryptomodule or anti-malware software)

Summary of Comments (6)

- We are not recommending a heavy weight certification process such as the Common Criteria Target of Evaluation with a Protection Profile. We would favor a lighter weight process based on vendor affirmation

Final Thoughts

- It is important to differentiate between what constitutes the CKMS Framework and what constitutes a Profile.
- The Framework says “Specify what you did”. A Profile says “This is what you must do to comply”.

Discussion?