Overview of NIST Cryptographic Key Management Profile for Federal Government Applications

Presentation Overview

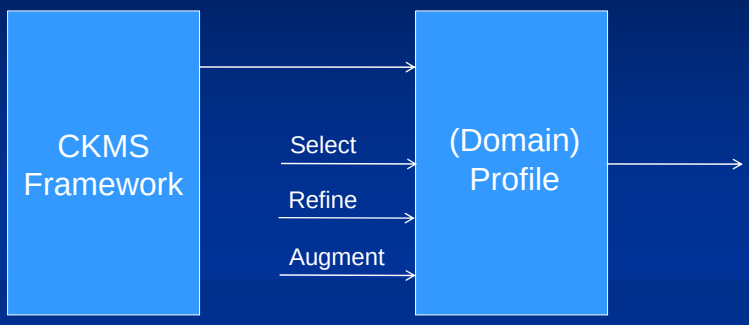
- What is a Profile?
- Framework to CKMS product relationships
- Framework and Profile development plan
- Generic Profile considerations
- Vendor action examples
- Federal secure CKMS Profile topics

What is a CKMS Profile?

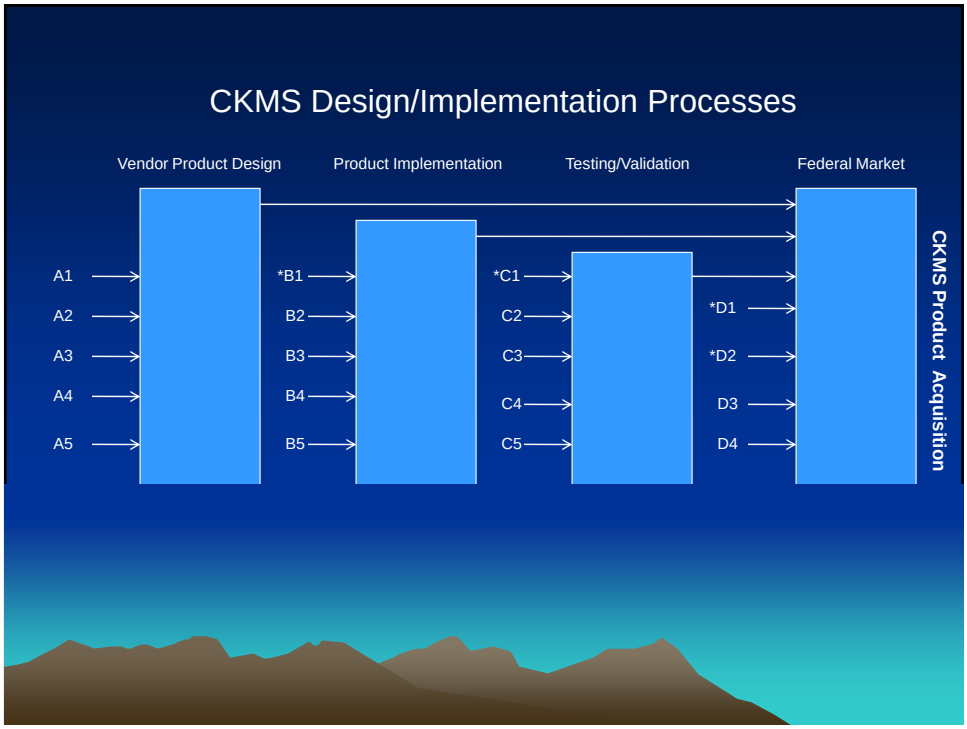
- A selection, refinement, and augmentation of component specifications to achieve specific objectives (e.g., security, compatibility, interoperability) among a group of organizations (e.g., Federal agencies) having similar goals and applications.

3

CKMS Framework and Profile



4



Framework → Profile(s) → CKMS Products

- Profile customizes the Framework
- Profile specifies CKMS Components
- Profile specifies Design Requirements
- Framework is a foundation for Profiles
- Federal Profile is being drafted
- CKMS Designs and Products may be developed

CKMS Federal Profile Development Plan

- Publish CKMS Framework Draft
- Hold CKMS Workshop
- Include Comments & Workshop Results in Revised Framework Draft
- Include Workshop Profile Results in first Federal Profile Draft

CKMS Considerations

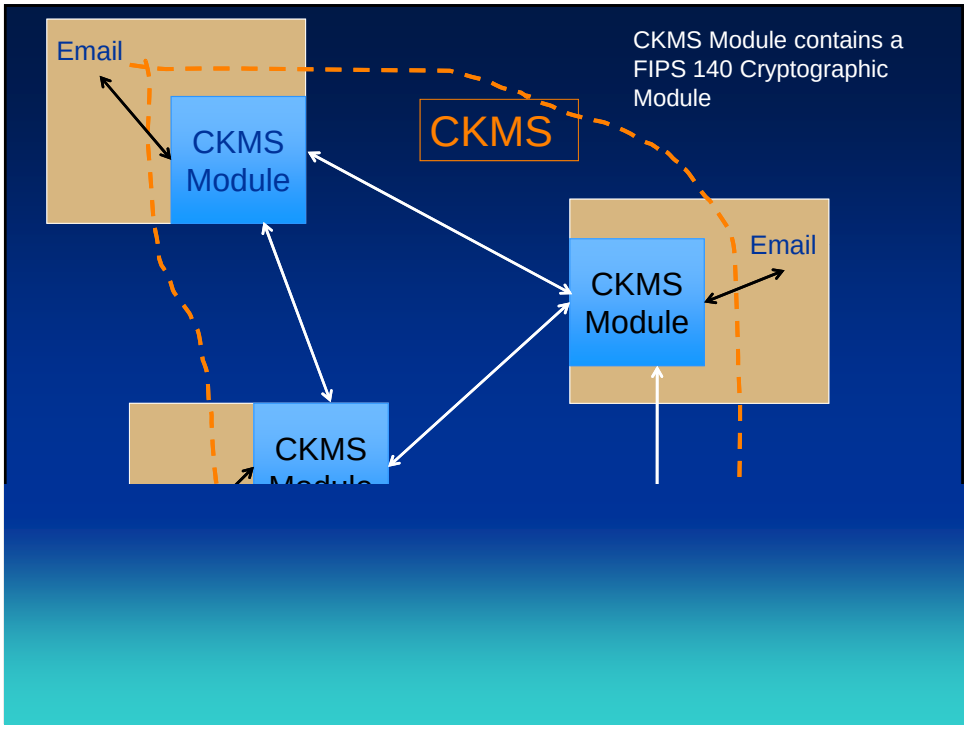
- Customer Security Requirements
- Roles and Responsibilities
- CKMS Services, Constraints, Objectives
- CKMS Testing and System Assurances
- CKMS Security and Disaster Recovery

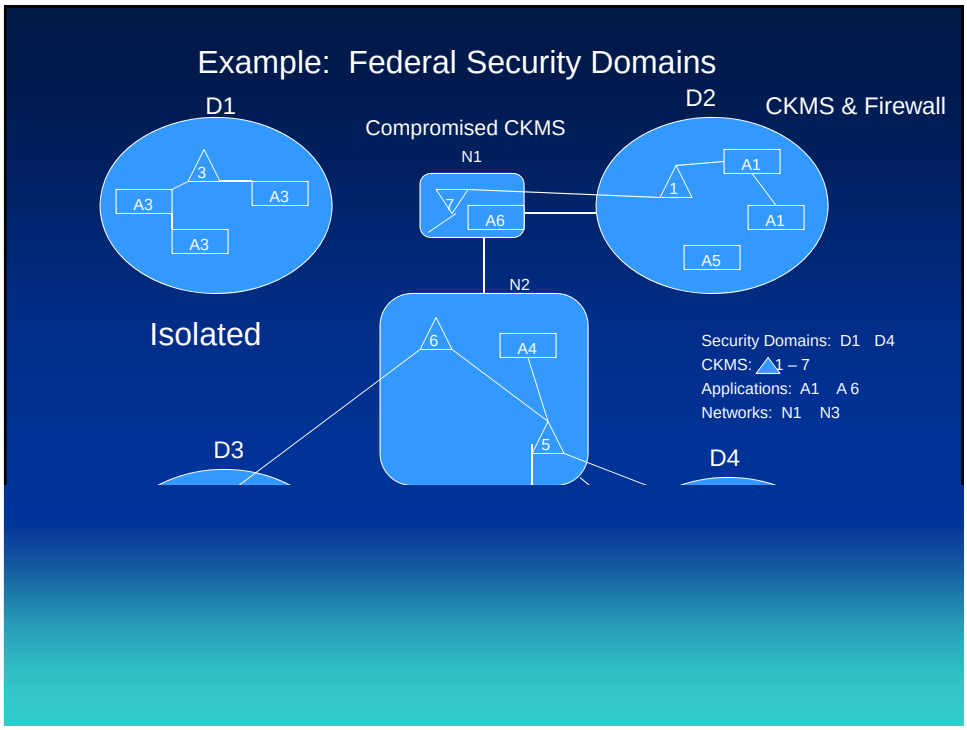
CKMS Generic Profile Considerations

- CKMS Security Domains and Service Providers
- CKMS interactions within and across organizations and Security Domains
- CKMS Implementations?
- CKMS Validation?

Profile Requirements

- The Profile will require that the design must conform to the profile.
- The Profile will require consistency between the design and the implementation.
- The Profile will address how the


Email
CKMS Module contains a FIPS 140 Cryptographic Module
CKMS
CKMS Module
Email
CKMS Module
CKMS


Example: Federal Security Domains
D1
Compromised CKMS
N1
D2
CKMS & Firewall
3
A3
A3
A3
7
A6
1
A1
A1
A5
N2
Isolated
6
A4
5
Security Domains: D1 D4
CKMS: 1 – 7
Applications: A1 A 6
Networks: N1 N3
D3
D4

CKMS Vendor Actions: Examples

- Specify CKMS Goals & Target Markets
- Use Framework and Profile requirements to design and implement for a selected Market (ex: high level)
- Vendor's Design Group verifies design against Framework & Profile

CKMS Vendor Actions (Cont'd.)

- Vendor submits Design and Implementation to Accredited Validation Service Providers (if Purchaser Requires)
- Use validation results as part of vendor's CKMS marketing strategy

Federal Secure CKMS Profile

- Federal/Agency/User Security Policies
- National/International Laws and Federal Regulations
- Service Provider Alternatives
- Compatibility and Interoperability Needs
- Cryptographic Algorithms Supported

Federal Security Policies Supported

- Sensitive but Unclassified Applications
- Organizational and User Policies
- Integrity, Confidentiality, Availability
- User Identification/Authentication
- User Accountability
- Controlled Access to Sensitive Data