



CKM Framework

Miles Smid
with input from
Elaine Barker
Dennis Branstad
Santosh Chokhani

For those viewing via webcast, please submit questions to kmwquestions@nist.gov

NIST CKM Workshop June 9, 2009

1

Goals



- A cryptographic key management framework that:
 - Provides organization and consistency to CKM solutions
 - Provides a structure for the organization of current and future key management standards
 - Supports the use of cryptographic mechanisms providing security to current and future information management applications
 - Can be used by both the U.S. Government and private sector.

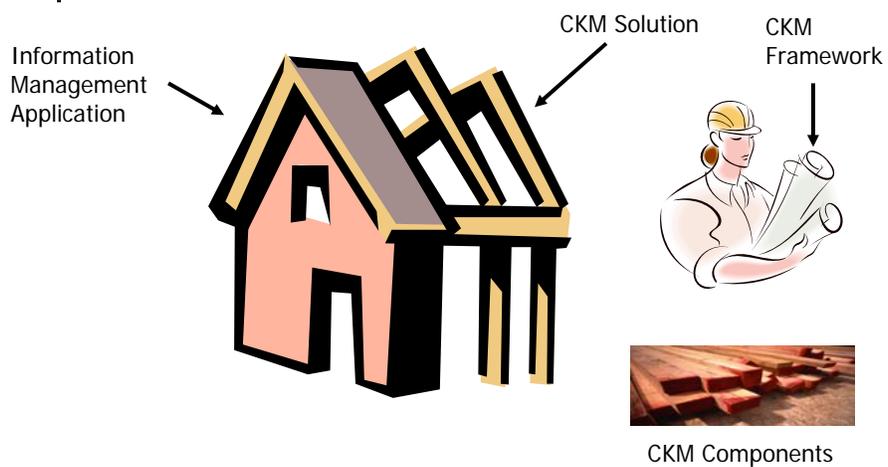
2

What constitutes a CKM Framework?

- A comprehensive list of the essential policies, components, and assurances that compose a CKM solution.

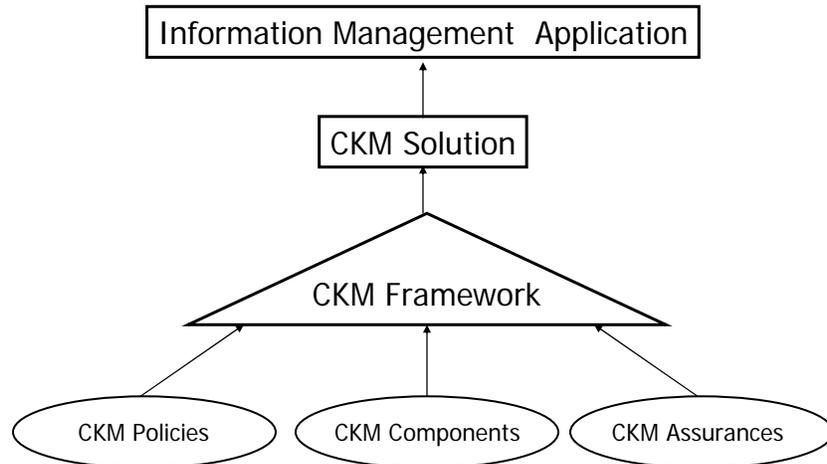
3

Framework to Support Information Management



4

Mapping CKM Solutions into the Framework



5

Required Policies



- Data Availability
- Data Confidentiality
- Data Integrity
- Data Access
- Lifetimes
 - Key lifetimes
 - Algorithm lifetimes
 - Data lifetimes
- Key Management Policies for all key types and related keying material over the entire key management lifecycle

6



Unique Application Requirements and Constraints

- Unique requirements/constraints imposed by the application should be specified in CKM solution so as to ensure the framework provides adequate support.

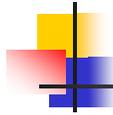
7



Assurances

- What is the target security strength required for the managed information?
- What assurance do we have that the CKM solution meets the target security strength?
- How is conformance of the CKM solution verified?

8

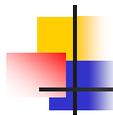


Components



- Components of the framework must be selected to support the selected policies, requirements and constraints.

9

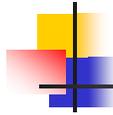


Usual Components



- Keys
 - Public, private, and symmetric
- Algorithms
 - Encryption, data integrity, identity authentication, non-repudiation, key generation
- Primitives
 - Key derivation, key transport, key agreement, certificate path validation
- Protocols
 - IPsec, TLS, S/MIME, Kerberos, DNSSEC, EFS, SSH, etc.

10

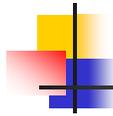


Additional Components



- Cryptographic Modules
 - FIPS 140-2/3
- Products
 - Software, hardware
 - Communications, storage, access control
- Composition
 - Putting all the components together to provide a secure CKM solution

11



Interfaces

- Possible interfaces
 - Cryptographic Algorithm Interface
 - Key Management Interface
 - Cryptographic Module Interface
 - Product/Application Interface
- Which interfaces need to be addressed?

12

Planning for Transitions

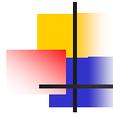
- When will the CKM solution need maintenance?
- When will the CKM solution need replacement?
- How should it be phased out?

13

Frameworks can make beautiful structures



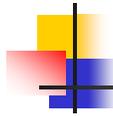
14



But can a single CKM Framework accommodate all CKM solutions and information management applications and still be useful?

For those viewing via webcast, please submit questions to kmwquestions@nist.gov

15



Submit your thoughts

- Now, or on the
- NIST Key Management Workshop BLOG.

<http://keymanagement.wordpress.com/>

16