The name of the TC:

OASIS Key Management Interoperability Protocol (KMIP) Technical Committee

Statement of Purpose:

The KMIP Technical Committee will develop specification(s) for the interoperability of key management services with key management clients. The specifications will address anticipated customer requirements for key lifecycle management (generation, refresh, distribution, tracking of use, life-cycle policies including states, archive, and destruction), key sharing, and long-term availability of cryptographic objects of all types (public/private keys and certificates, symmetric keys, and other forms of "shared secrets") and related areas.

Scope:

The initial goal is to define an interoperable protocol for standard communication between key management servers, and clients and other actors which can utilize these keys. Secure key management for TPMs (Trusted Platform Modules) and Storage Devices will be addressed. The scope of the keys addressed is enterprise-wide, including a wide range of actors: that is, machine, software, or human participants exercising the protocol within the framework. Actors for KMIP may include:

- Storage Devices
- Networking Devices
- Personal devices with embedded storage (e.g. Personal Computers, Handheld Computers, Cell Phones)
- Users
- Applications
- Databases
- Operating Systems
- Input/Output Subsystems
- Management Frameworks
- Key Management Systems
- Agents

Out of scope areas include:

- Implementation specific internals of prototypes and products
- Multi-vendor Key Management facility mirrors or clusters
- Definition of an architectural design for a central enterprise key management or certificate management system other than any necessary models, interfaces and protocols strictly required to support interoperability between Actors in the multi-vendor certificate and key management framework.
- ~~Framework interfaces not dedicated to secure key and certificate management~~
- ~~Certain areas of functionality related to key management are also outside the scope of this technical committee, in particular registration of clients, server-to-server communication and key migration.~~

- ~~Bindings other than tag-length-value wire protocol and XSD-based encodings.~~

List of deliverables:

The deliverables for the KMIP Technical Committee are anticipated to include the following:

- Revised KMIP Specification~~ v0.98~~. This provides the normative expression of the protocol, including objects, attributes, operations and other elements. A Committee Specification is scheduled for completion within 12 months of the first TC meeting.
- Revised KMIP Profiles. This provides the normative expression of conformant implementations of the protocol. A Committee Specification is scheduled for completion within 12 months of the first TC meeting.
- Revised KMIP Usage Guide~~ v0.98~~. This provides illustrative and explanatory information on implementing the protocol, including authentication profiles, implementation recommendations, conformance guidelines and security considerations. A Committee Note is scheduled for completion within 12 months of the first TC meeting.
- Revised KMIP Use Cases. This provides illustrative use cases for KMIP. A Committee Note is scheduled for completion within 12 months of the first TC meeting.
- Revised KMIP Test Cases~~ v0.98~~. This provides illustrative test cases for KMIP~~,~~ and examples of the protocol implementing those test cases. A Committee Note is scheduled for completion within 12 months of the first TC meeting.
- Revised KMIP Frequently Asked Questions. This illustrative document provides guidance on what KMIP is, the problems it is intended to address and other frequently asked questions.

KMIP, as defined in the above deliverables, will be scoped to include the following:

1. Comprehensive Key and Certificate Lifecycle Management Framework

    A. Lifecycle Management Framework to Include:

        a. Provisioning of Keys and Certificates

            i. Creation
            ii. Distribution
            iii. Exchange/Interchange
            iv. Auditing

        b. Reporting
        c. Logging (Usage tracking)
        d. Backup
        e. Restore
        f. Archive
        g. Update/Refresh

h. Management of trust mechanisms between EKCLM (Enterprise Key and Certificate Lifecycle Management) actors only as necessary to support EKCLM

B. Comprehensive Key and Certificate Policy Framework to include:

a. Creation
b. Distribution
c. Exchange/Interchange
d. Auditing
e. Reporting
f. Logging (Usage tracking)
g. Backup
h. Restore
i. Archive
j. Update/Refresh
k. Expectation of Policy Enforcement

i. At endpoints
ii. At Key Manager
iii. At intermediaries between endpoints and Key Manager facility

C. Interoperability between Machine Actors in performing all aspects of A) and B), and addressing:

a. pre-provisioning and late binding of keys and certificates
b. support for hierarchical or delegation or direct models
c. actor discovery and enrollment as necessary to support ECKLM
d. key, certificate and policy migration
e. audit and logging facilities

D. General Capabilities may include:

a. Secure and Robust Mechanisms, Techniques, Protocols and Algorithms
b. Recovery capabilities, only as needed by interoperable interfaces, anticipating power failure, or other common failures of automated Actors
c. Forward compatibility considerations
d. Interface to Identity Management facilities as necessary for A) and B)
e. Interface to Enterprise Directory facilities as necessary for A) and B)

KMIP TC will also support activities to encourage adoption of KMIP. This would likely include:

- Interoperability sessions to test effectiveness of the specification
- Reference implementations of KMIP functionality

IPR Mode under which the TC will operate:

The KMIP TC is anticipated to operate under RF on RAND.

Anticipated audience or users:

KMIP is intended for the following audiences:

- Architects, designers and implementers of providers and consumers of enterprise key management services.

Language:

Work group business and proceedings will be conducted in English.