

IEEE P1619.3

Architecture Subcommittee

Model Update and Discussion

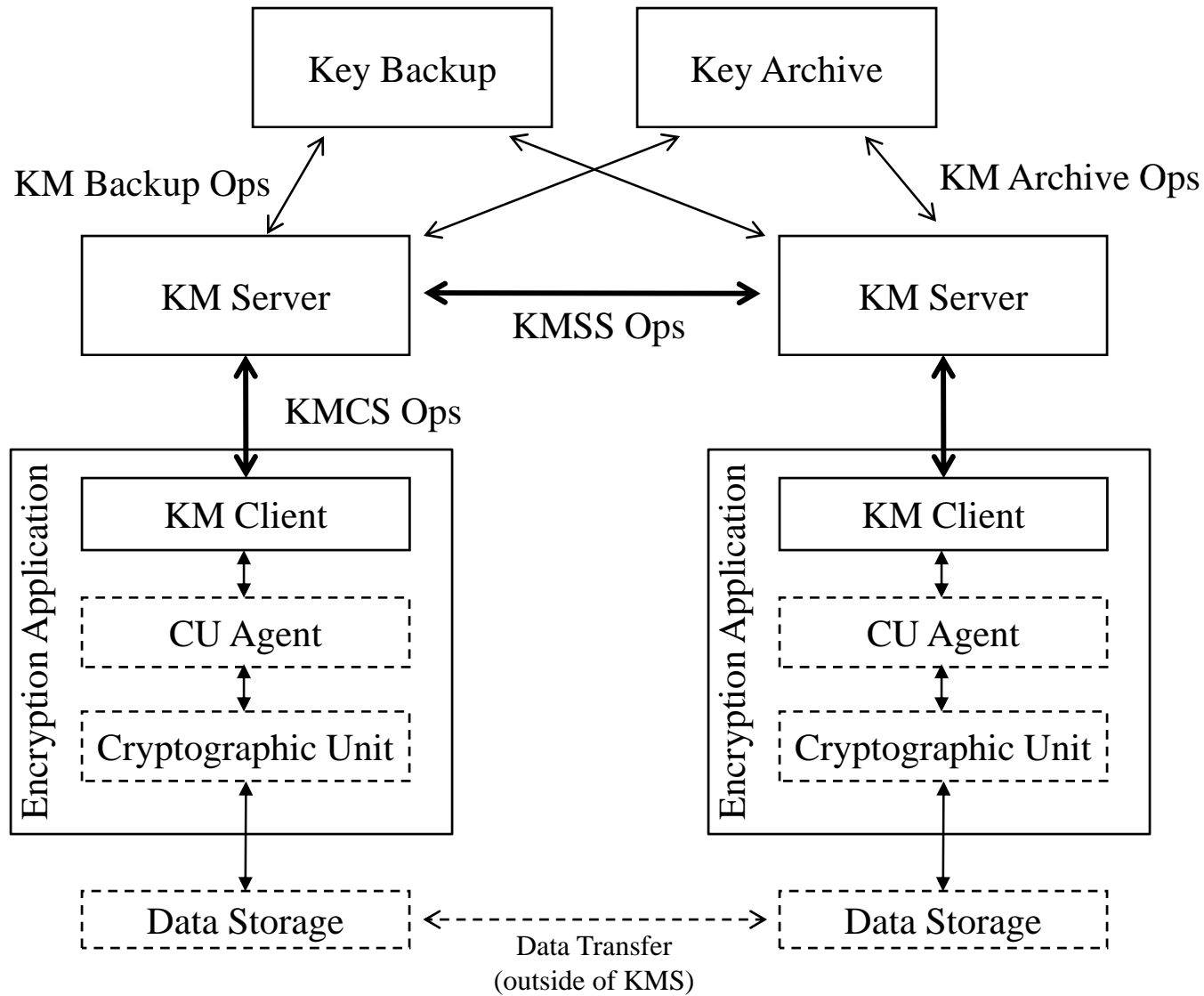
November 1, 2007

Agenda

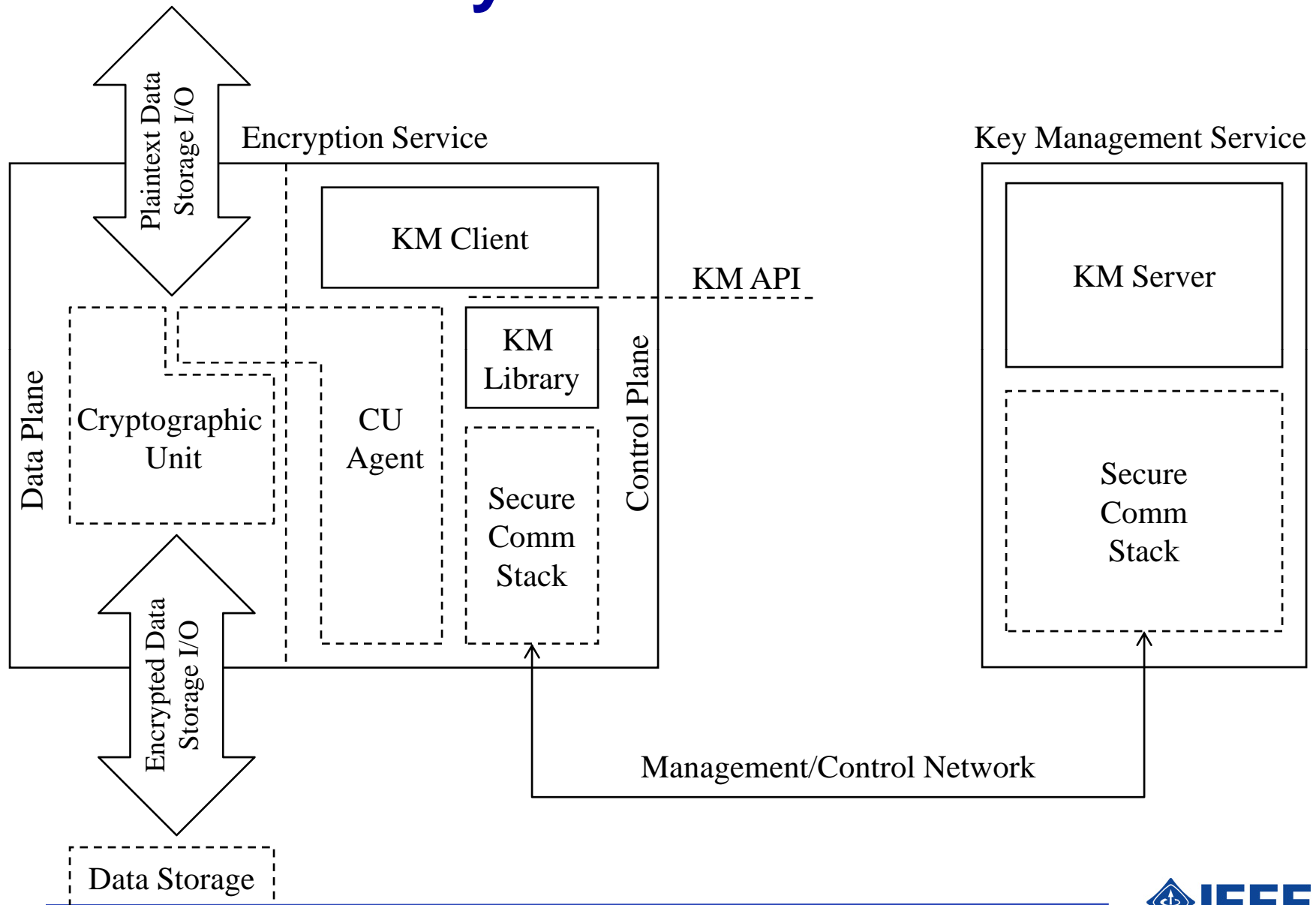
- Discuss updated KM role/layered models
- Discuss John Holdman's key lifecycle model
- Miscellaneous Topics
 - KM Policy Models
 - Data Attribute Models
 - Interaction Models?

Proposed KM Role/Layer Models

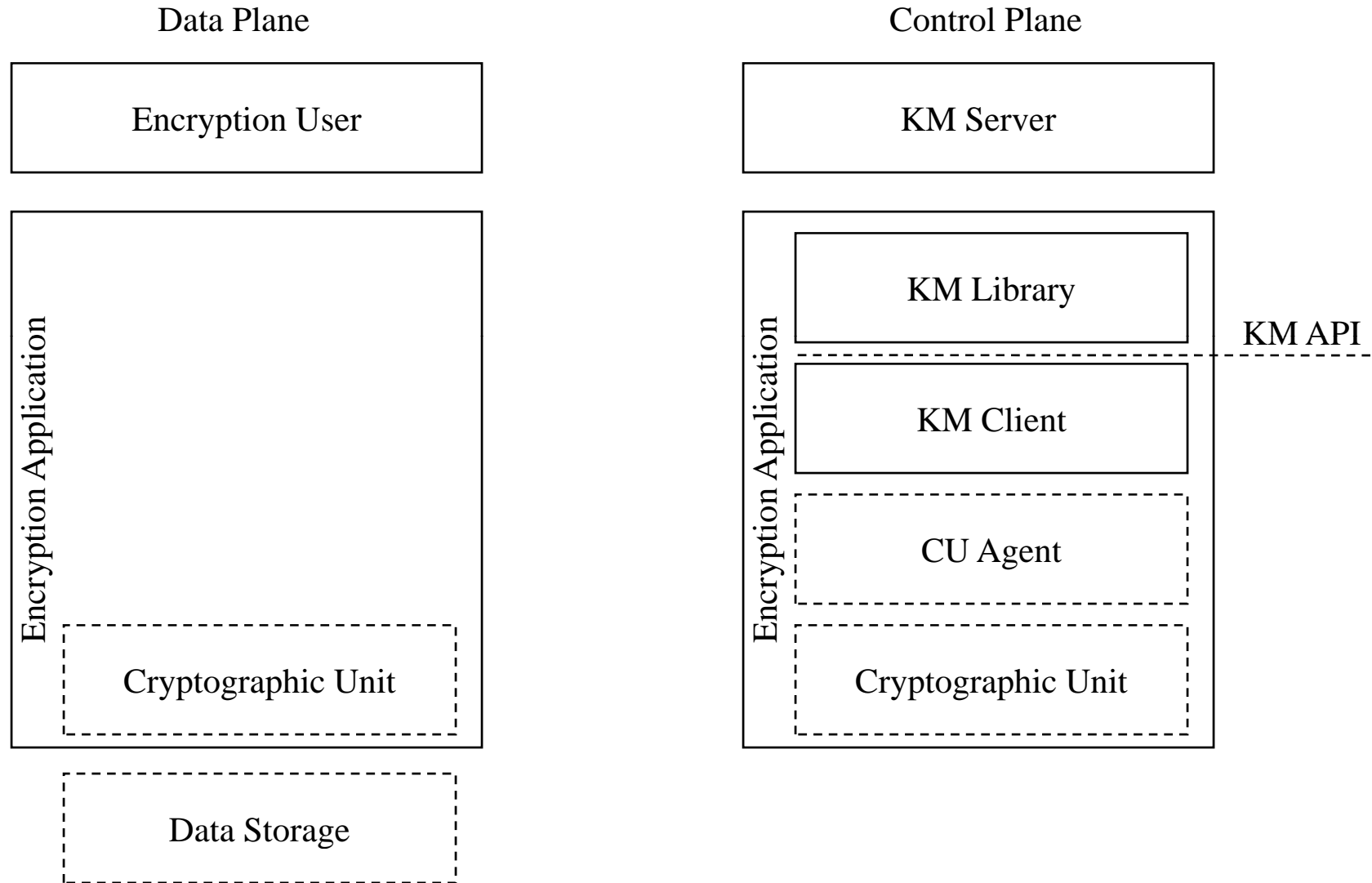
Role/Entity Model



Layered Model #1



Layered Model #2



Updated Definitions

- Data Plane
 - Traditional data communications term that refers to the primary data path through a system. In the case of the P1619.3 standard, it is the path that plaintext user data takes through the cryptographic unit before it is placed on the storage media, and visa versa.
- Control Plane
 - Traditional data communications term that refers to the set of components involved in the configuration, control, and management of the data plane. These components are typically not within the data path used for primary data movement and manipulation.

Updated Definitions

- **KM Server**
 - Implements the key management service that manages the complete key lifecycle for keys and security material used to provide cryptographic protection of stored data
- **Encryption Service**
 - Is the SW and/or HW system that provides encryption services to protect stored data
- **KM Client**
 - Is the component of the Encryption Service that communicates with the KMS and ensure keys and security material are properly loaded into the cryptographic unit

Updated Definitions

- **KM Library**
 - Is the component of the Encryption Service that implements the KM API, KM messaging service, and KM transport protocol client; used by the KM Client to communicate with the KMS
- **KM API**
 - The C\C++ and Java bindings that implement the interface to the KM library
- **Secure Communication Stack**
 - Is the component of the Encryption Service that implements the network communication protocol stack whose services are used to provide secure communication over the internet/intranet; typically, this is the SSL(TLS)/TCP/IP stack

Updated Definitions

- **Cryptographic Unit Agent**
 - Is the component of the Encryption Service that provides the necessary services to allow the KM Client to control the Cryptographic Unit from the control plane
- **Cryptographic Unit**
 - The hardware and/or software component of the Encryption Service that actually encrypts data before it is placed on the media used to store data and decrypts data after it is retrieved from the media used to store data
- **Data Storage**
 - The medium/media used to provide persistent data storage, including disk, tape, etc.

Proposed Key State/Transition Model

See John Holdman's document/email from 10/12/07

Miscellaneous Discussion

Key Policy Model

- Currently defined under key structures
 - Sections 4.3.3.3 thru 4.3.3.6
- Do policies need to be defined in section 4?
 - Or are they more KMS specific (transparent to KM clients)
- Do we need to capture the policy diagram in section 4.3.1

Data Attributes

- Is data attribute model required in section 4?
 - Or can this be confined to the OO section?
 - If we include, what attributes to include?
 - Include a general data object model?
 - Data objects instantiate a unit of data to protect
 - Attributes define the unit of data and how it should be protected
 - Key Policies

Interaction Model?

- Do we need a simplified interaction model to cover KMC/KMS interactions?
 - Coupled with data attribute model?
 - Coupled with policy model?
 - Or is this confined to OO section?