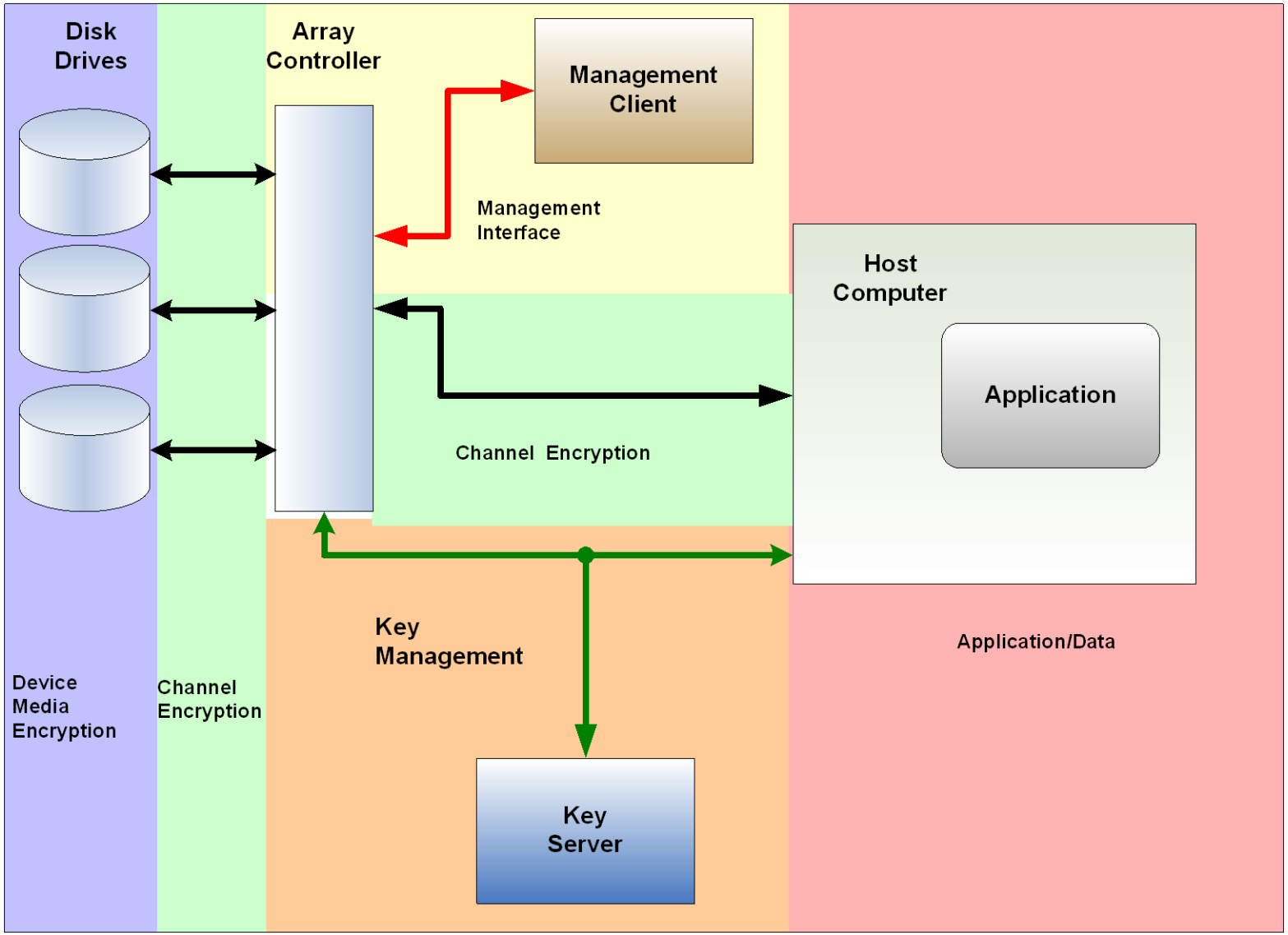
# IEEE SISWG P1916.3
# Key Management Workgroup

**Walt Hubis**

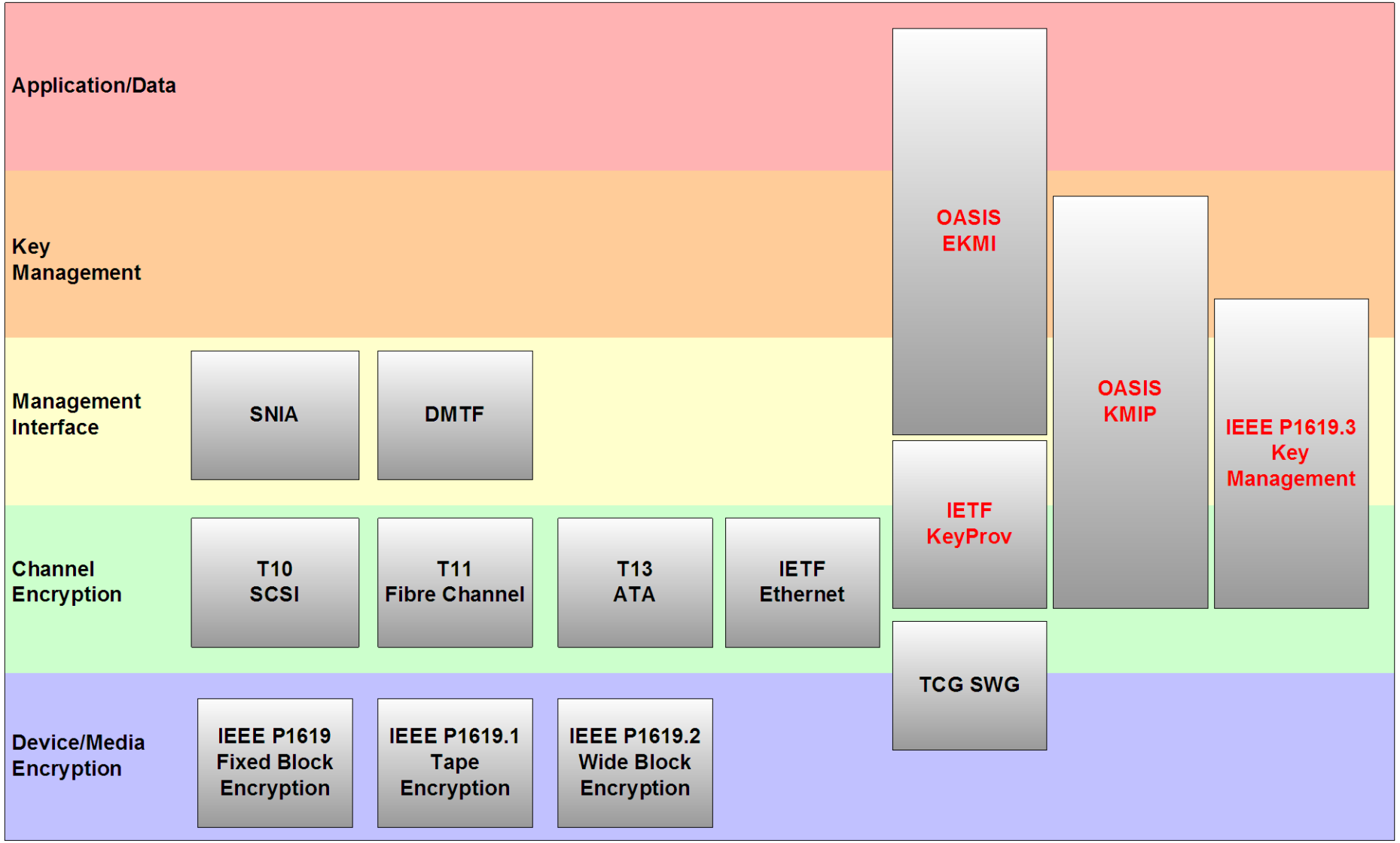
**Key Management Summit**

**May 4, 2010**

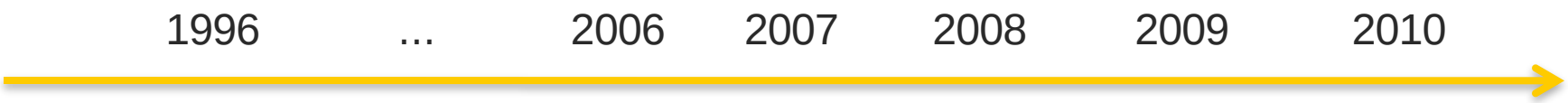
# Key Management Overview



# Security Standards Organizations



# Standards Timeline History




Frameworks:

ISO 11770-1:1996
1996 (rev 2009)

NIST SP 800-57
Part 1, 2 (Mar 07)

NIST SP 800-57
Part 3

Protocols:

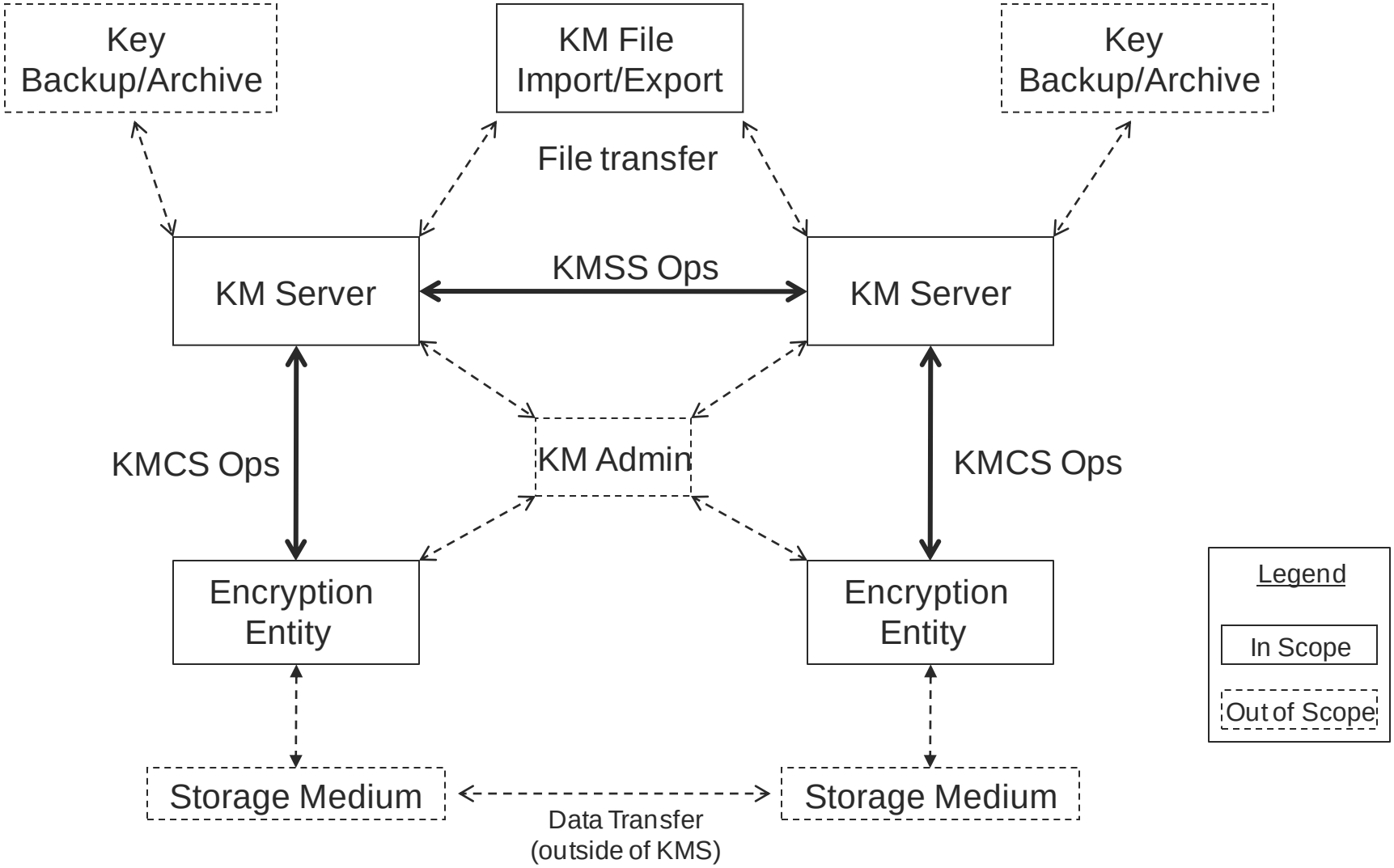
OASIS EKMI

IETF KEYPROV

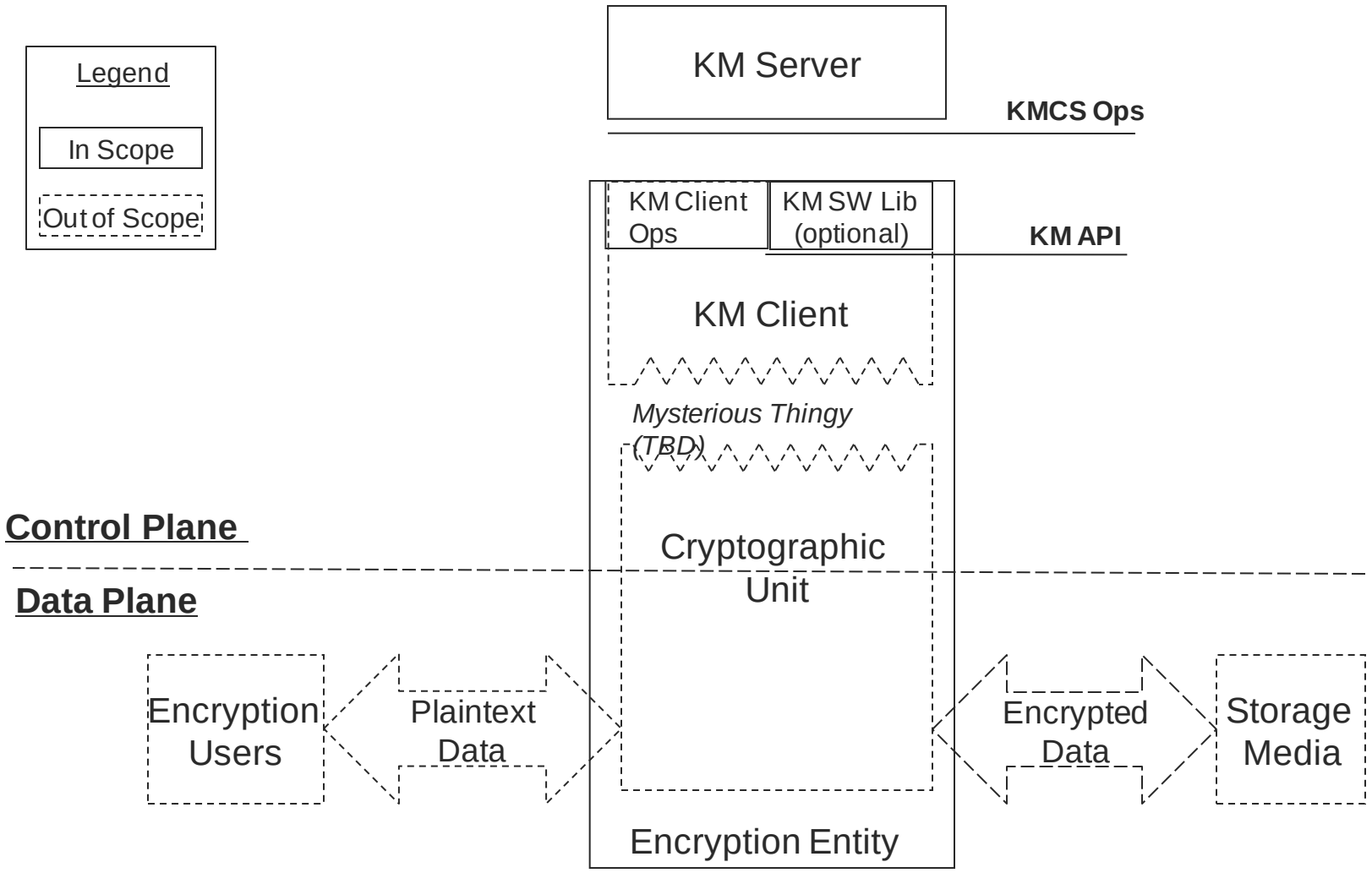
IEEE P1619.3

OASIS KMIP

# P1619.3 Architecture



# Conceptual Key Management Model



# Using P1619.3 extensions to KMIP

- Standard in progress, so details may change!
- Defines a RESTful and SOAP-based web service using WSDL 2.0.
  - RESTful interface is based on resources (objects)
  - SOAP is based on procedure calls (actions)
- Map KMIP binary types to XML types
- Many tools exist to help with XML processing
- Keep the same object model as KMIP so that the back-end database can be the same.

# REST Summary

- Stands for REpresentational State Transfer
- Introduced by Roy Fielding in 2000 thesis
- A web service that follows the REST guidelines is said to be "RESTful"
- Uses HTTP/1.1 commands:
  - GET – Retrieve a resource without side-effects
    - Allows for caching
  - PUT – Update or create a resource or collection
  - POST – Issue command with potential side-effects, or create a new resource or collection
  - DELETE – Remove a resource or collection

# Web Services Description Language

- A WSDL (pronounced Wiz-Dull) is an XML-based schema for describing the objects and operations of a web service
- WSDL 1.1 was originally for describing SOAP
- WSDL version 2.0 was published in June 2007
- New features include support for RESTful bindings
- Some tools support WSDL 2.0, including Apache AXIS2 (for both Java and C)

# Comparison of Primitive Types

| KMIP Primitive Type | P1619.3 XML Type | Typical C++ Encoding |
|---|---|---|
| Integer | xsd:int | int (32-bit) |
| Long Integer | xsd:long | long long (64-bit) |
| Big Integer | xsd:base64Binary | struct { } |
| Enumeration | xsd:string | enum { ... } |
| Boolean | xsd:boolean | bool |
| Text String | xsd:string | wchar_t * |
| Byte String | xsd:base64Binary | struct { } |
| Date-Time | xsd:dateTime | time_t (64-bit) |
| Interval | xsd:duration | char * (or long long) |

# P1619.3 Cluster Discovery

- P1619.3 Discovery service allows client to discover other available servers in the cluster
- Provides way for client to perform automatic failover if primary server is unavailable
- Details are still being worked out by the P1619.3 task group.
- Many of these changes will likely be integrated into future KMIP specifications or profiles

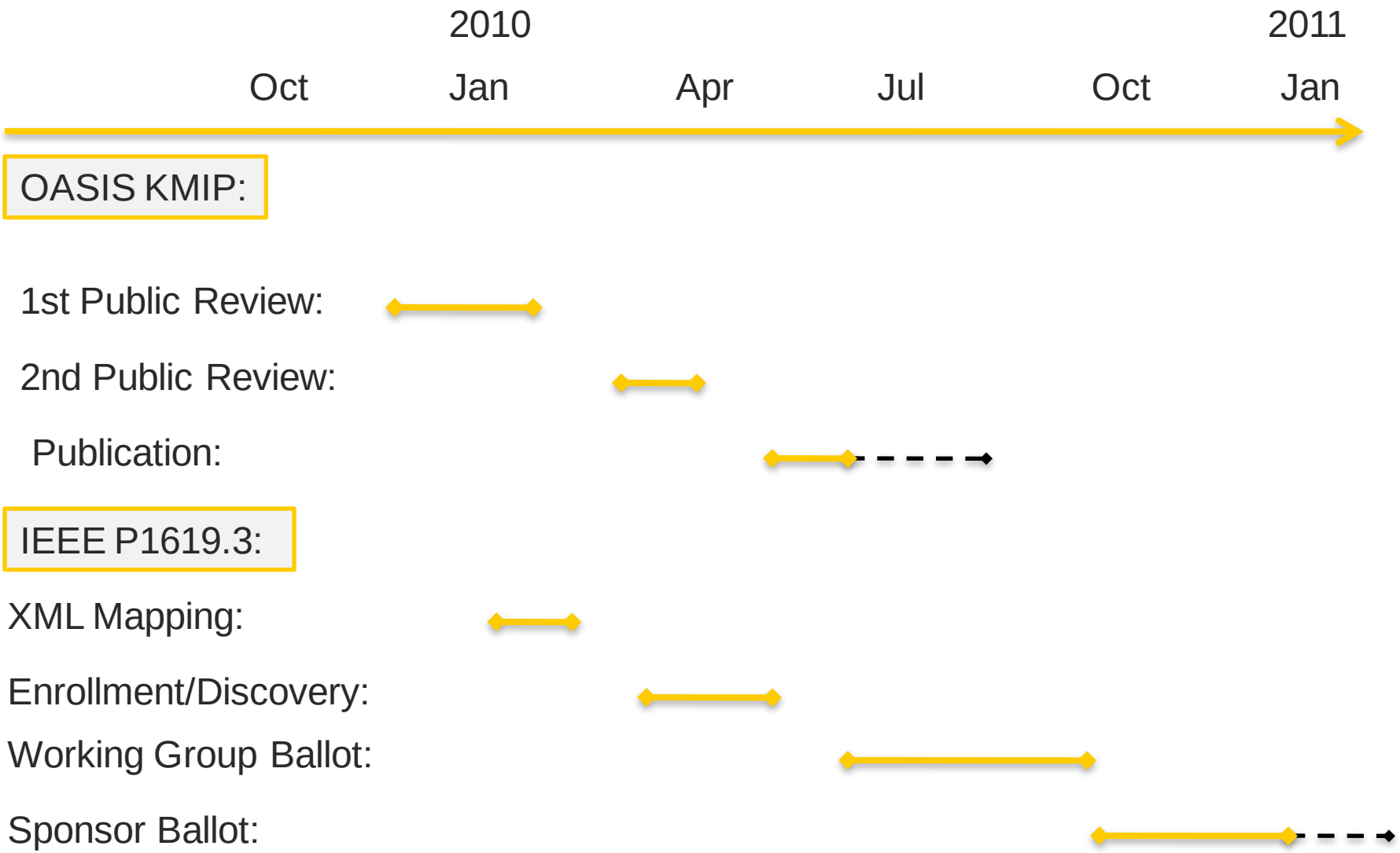
# P1619.3 Enrollment

- P1619.3 will also provide a way to perform a client enrollment operation, using some form of credentials (like username/password, token, etc)
- Details are being worked on within the P1619.3 task group
- Similar changes are under consideration for KMIP v1.1

# Encoding: KMIP vs. P1619.3

| Attribute | OASIS KMIP | IEEE P1619.3 |
|---|---|---|
| Overall Format | TTLV Binary | RESTful XML |
| Message Version | Version field in header | HTTP header version |
| Error Reporting | Error field in header | HTTP Error codes |
| Tool Support | No tool support | Many XML libraries |
| Grammar Validation | Manual | WSDL validation |
| Code size | Small | Medium |
| Processing Overhead | Low | Medium |
| Security | HTTPS with TLS | HTTPS with TLS |
| HTTP Command | POST | GET, POST, DELETE |
| Asynchronous Msg | Async flag in header | POST to startCmd |
| Command Batching | Count in header | Keep session alive |

# Projected Timeline



# The Future ?

Special Thanks to

**Matt Ball**


LSI
TM