P1619.3 Key Management Workgroup Overview

Walt Hubis
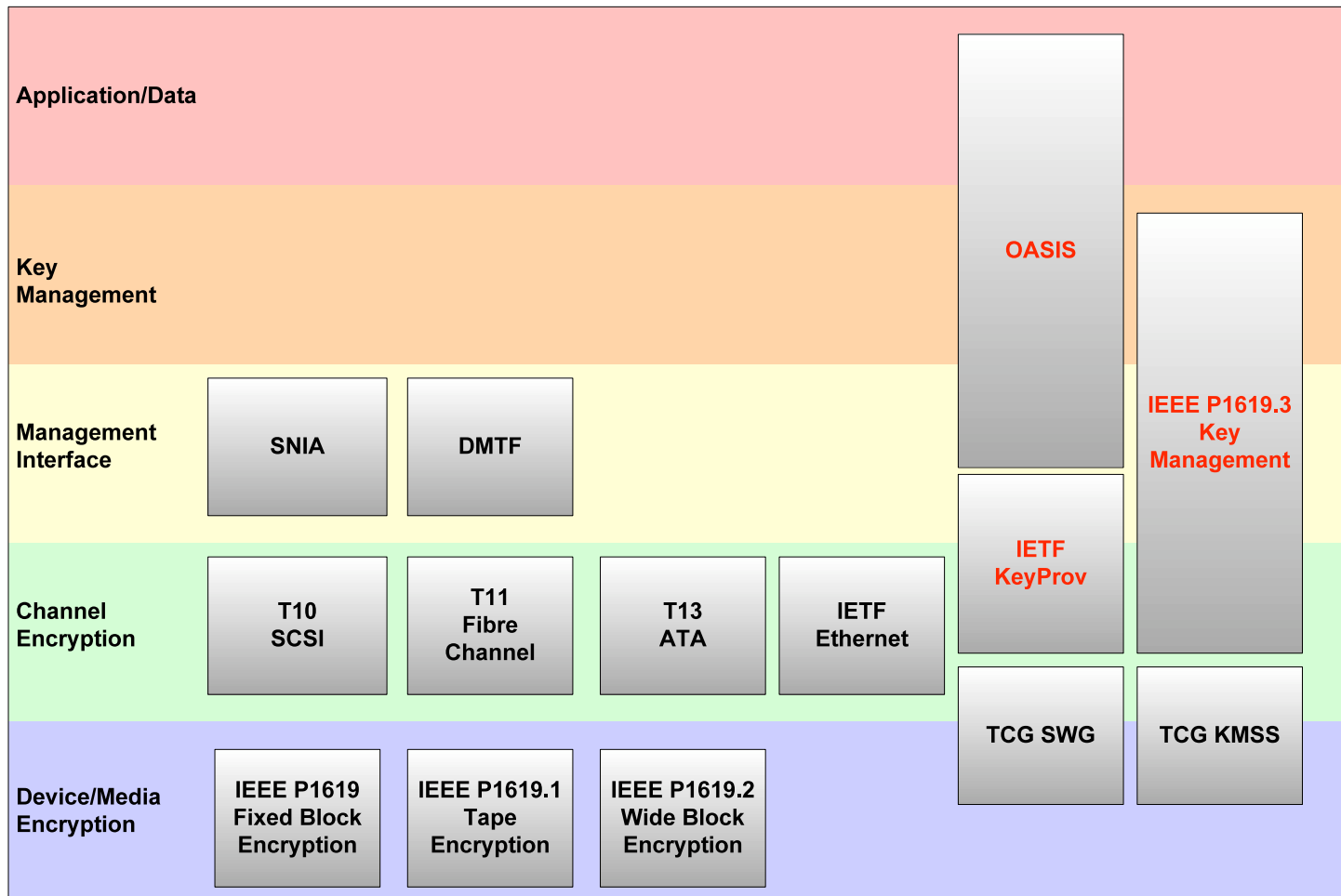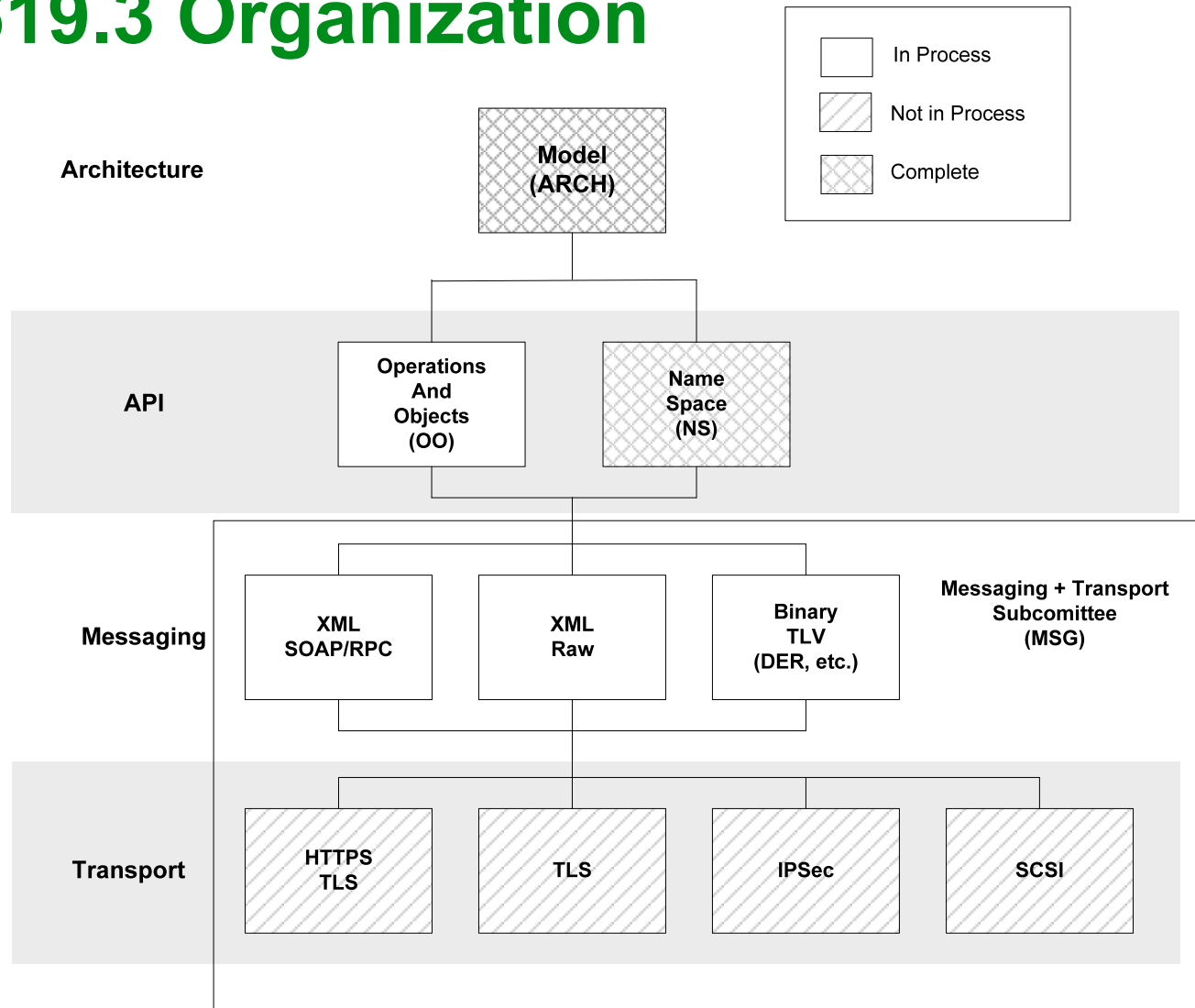
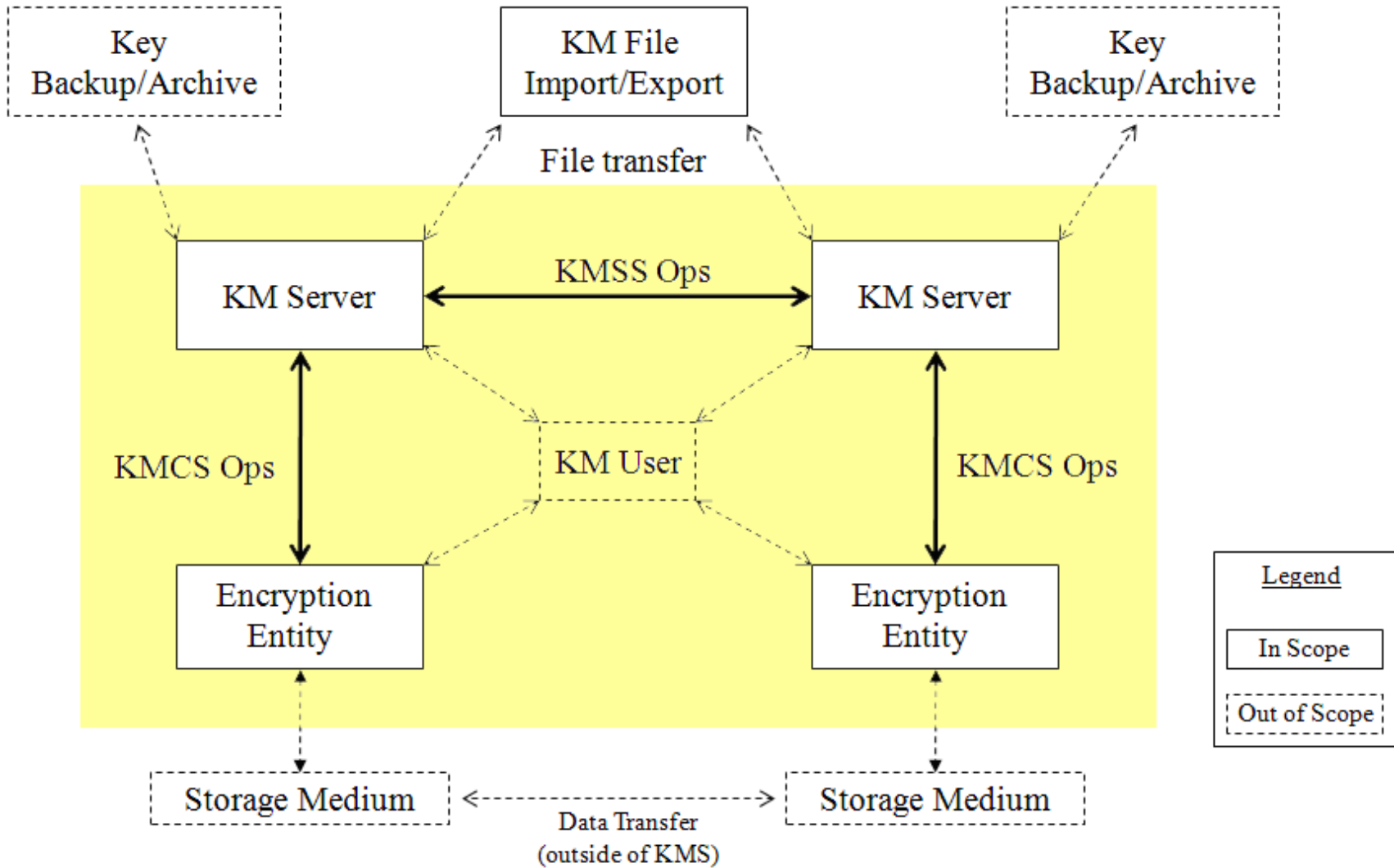# P1619.3 Goals and Priorities

Ÿ Create a standard that allows secure interchange of encryption keys between devices that encrypt stored data and devices that manage keys

Ÿ Understand existing standards and use where possible to expedite the creation this standard

Ÿ Raise public awareness of P1619.3 and encourage adoption

Ÿ Facilitate interchange by providing open source reference implementations

P1619.3 Organization

	In Process
	Not in Process
	Complete

Architecture — Model (ARCH)

API — Operations And Objects (OO) — Name Space (NS)

Messaging — XML SOAP/RPC — XML Raw — Binary TLV (DER, etc.) — Messaging + Transport Subcomittee (MSG)

Transport — HTTPS TLS — TLS — IPSec — SCSI

P1619.3 Architecture

Key Backup/Archive

KM File Import/Export

Key Backup/Archive

File transfer

KM Server — KMSS Ops — KM Server

KMCS Ops

KM User

KMCS Ops

Encryption Entity

Encryption Entity

Legend

In Scope

Out of Scope

Storage Medium ←→ Storage Medium

Data Transfer (outside of KMS)

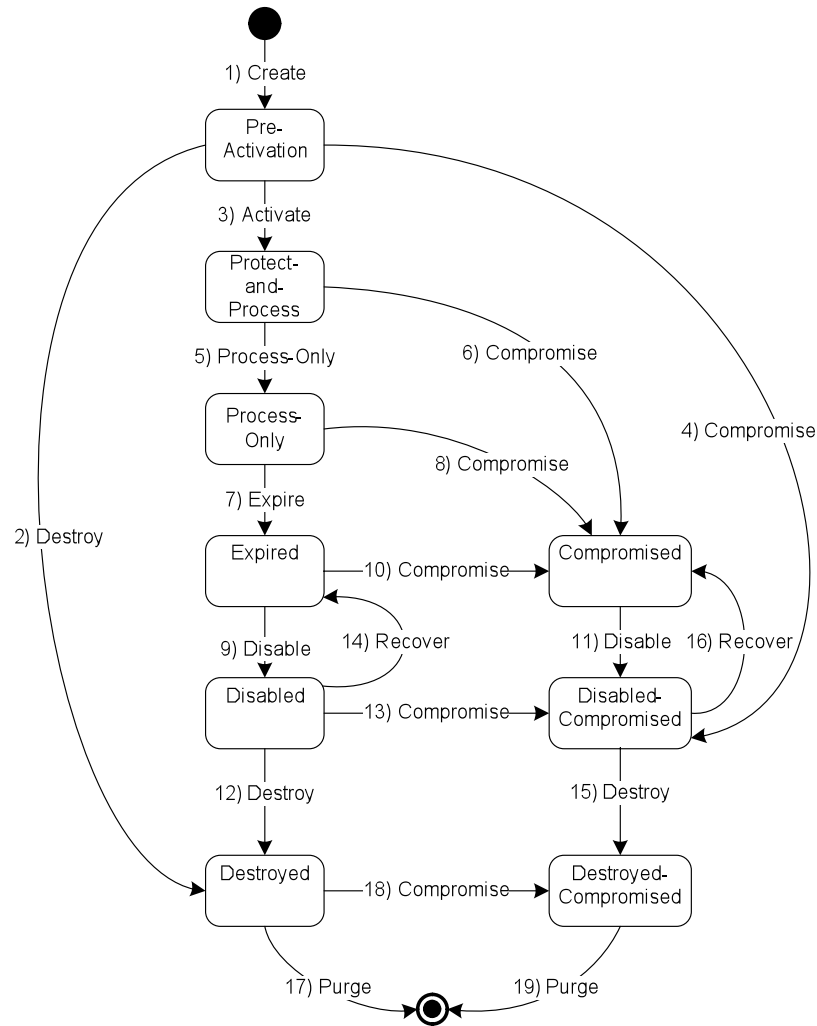# P1619.3 Architecture
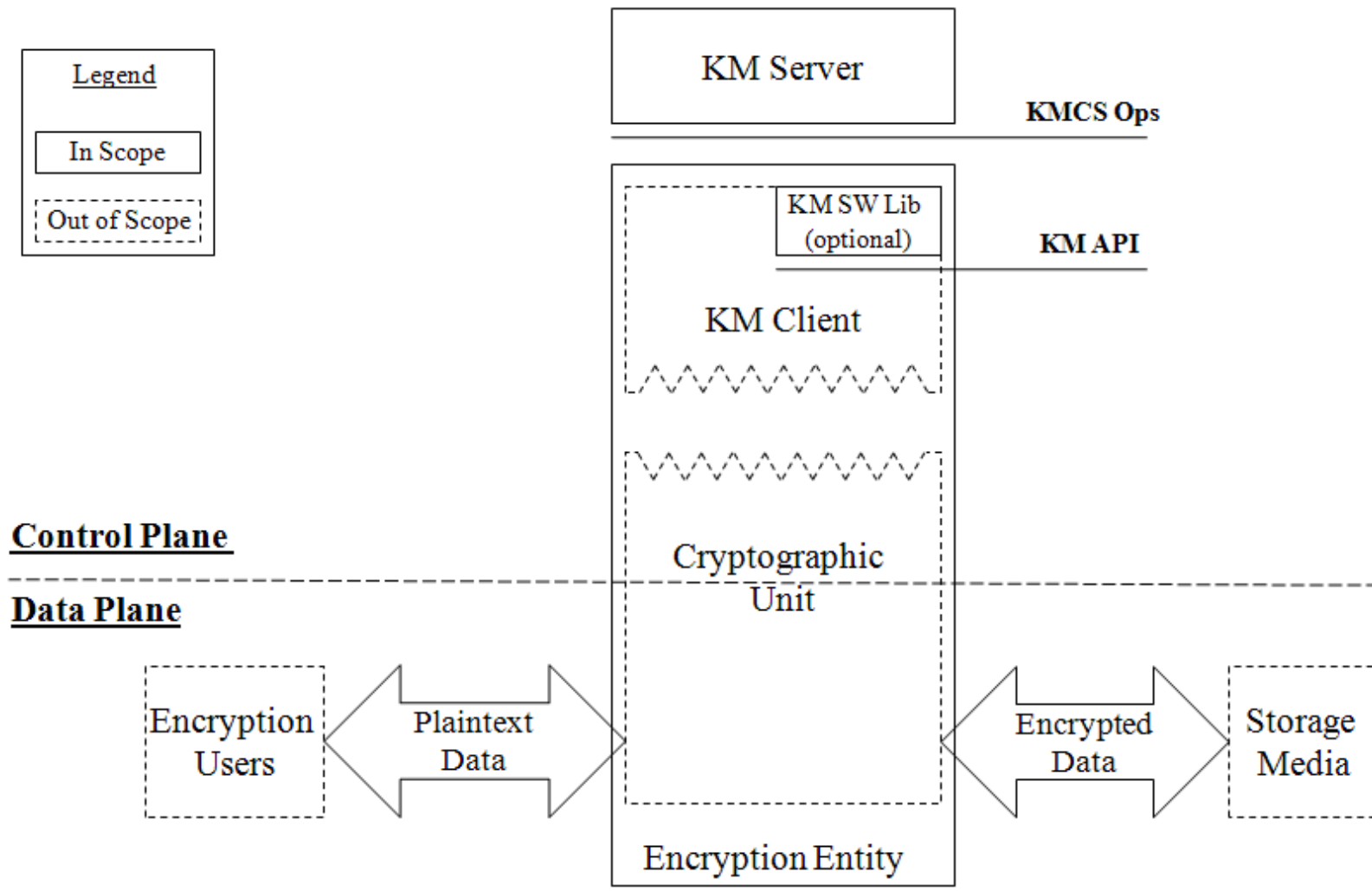
P1619.3 Key Lifecycle

P1619.3 Key Identifiers

Ÿ SO_GUID

  − Security Object Global Unique Identifier

  − Globally unique to the key

Ÿ Uses

  − Integration of different key shares.

  − Sharing keys between companies.

P1619.3 Key Identifier Types

Ÿ Uniform Resource Identifier (URI)

Ÿ Name Address Authority (NAA)

Ÿ Random Number

Ÿ Locally Assigned

Ÿ OASIS EKMI GKID

 – Based on IANA Enterprise number.

P1619.3 Status

Ÿ Multiple Messaging Standards Desired

- XML-Based
    - Raw XML
    - XML SOAP
    - XML SOAP using OASIS SKSML
    - XML SOAP with WS-Management
- Binary-Based
    - Free-form
    - Structured Tag-Length-Value
    - ASN.1 Distinguished Encoding Rules (DER)

P1619.3 Status

Ÿ Moving Forward on the Messaging Layer

1. Decide if one messaging method is mandatory.
   - Vote in progress now.

2. If Vote Passes, decide which protocol to implement.
   - Probably the least common denominator

3. In either case, set deadline for optional messaging methods.
   - Set a deadline (60 days) for proponents to provide proposals.

P1619.3 Status

Committee	Start Date	Current	Comments
ARCH	10/2007	Complete 3/2008	
NS	6/2007	Complete 1/2008	
OO	9/2007	10/2008 (Was 5/2008)	Draft in process now.
MSG	9/2007	In Process	Ÿ Vote in Process for Mandatory Messaging. Ÿ Allow 60 Days for Optional Protocols.

P1619.3 Schedule