IEEE P1619.3 Plan for 2010

Matt Ball, IEEE Security in Storage Working Group Chair

Walt Hubis, IEEE P1619.3 Task Group Chair

Version 1 – January 19, 2010

Overview

This document describes the plans for the IEEE P1619.3 Task Group for the 2010 calendar year.

Background

The IEEE P1619.3 Task Group was formed in February 2007, with the following Title, Scope, and Purpose:

Title:

Draft Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data

Scope:

This standard specifies an architecture for the key management infrastructure for cryptographic protection of stored data, describing interfaces, methods and algorithms.

Purpose:

This standard defines methods for the storage, management, and distribution of cryptographic keys used for the protection of stored data. This standard augments existing key management methodologies to address issues specific to cryptographic protection of stored data. This includes stored data protected by compliant implementations of other standards in the IEEE 1619 family.

In early 2009, a consortium brought forward the “Key Management Interoperability Protocol” (KMIP) into the OASIS standards organization. This new standard has much in common with the scope and purpose of P1619.3. Many people have asked whether P1619.3 is still relevant with the presence of OASIS KMIP. We believe the answer is “yes”.

2010 Plan for P1619.3

Overall, the existing of KMIP has benefitted the P1619.3 effort because it is now possible to leverage the KMIP standard – which (as of January 2010) is in public review and nearly complete – as the basis for the low-level key management functions, and position P1619.3 as a KMIP profile that adds on enterprise-class additions to make it suitable for key management in a storage encryption environment.

In reviewing KMIP, the P1619.3 task group plans to enhance KMIP with the following extensions:

1. Start with the KMIP binary format and the ‘Symmetric Key Foundry’ and ‘Symmetric Key Store’ profiles
2. Create an XML WSDL that is a mechanical translation of a subset of the KMIP binary protocol. The KMIP binary primitives have a clean mapping into standard XML-Schema objects, and this work has already been completed by at least two members of the KMIP consortium, for a proof-of-concept.
3. Add in the P1619.3 Namespace work into the XML and the binary represenatation. KMIP does not appear to define any namespaces, but relies on the users to hopefully create identifiers that are unique (actually, the only requirement is that they are unique in the local server context). This can also be achieved by implementing the XML representation in 1619.3 and take the binary representation into KMIP.
4. Define concrete default port bindings for the XML P1619. 3 services, through IANA. KMIP is currently planning to reserve a port through IANA for both the client and server implementation of the binary KMIP format. Proposal includes another, separate port for the XML representation. These are fixed TCP ports for default. Questions over why this is needed and not the default port 443 that is defined for HTTPS. Using 80 and 443 provide a convenient way to get through firewalls and/or proxies. Possibly a better approach is a content type (via IETF).
5. Define an enrollment protocol. KMIP doesn't do this, but assumes that you've already white-listed the certificates used for the SSL/TLS channel. Define a discovery protocol: a way to get servers, ports, and capabilities.
6. Define an XML-based key backup format for interchangeable archiving keys from a key management server. Consider using CMS for storing keys.
7. Define the use of WS-Security for further authenticating messages within a TLS channel (i.e., the TLS channel itself could have one level of authentication – based on the client certificate – but could be a proxy for other clients that use WS-Security for their authentication). Are there use cases available for this functionality? Unclear why this is needed. Consider removing this section for 2010.

Strawman schedule for completing P1619.3

Currently, the P1619.3 PAR (Project Authorization Request) is set to expire on December 31, 2011, so we have almost 2 years left to complete the project and deliver the draft to IEEE. This should be enough time to complete the remaining work, and if not, it is possible to get a 1-2 year extension, if needed.

Many members of P1619.3 are also members of OASIS KMIP, and the previous push was to get the KMIP 1.0 specification out to public review. Now that KMIP 1.0 is in public review, P1619.3 members have more time to focus on completing P1619.3.

Here is a strawman schedule for completing P1619.3 by the end of 2010:

- January 2010: Decide as a group what will go in to P1619.3 (this document)
- February 2010: Complete high priority action items for KMIP and Specification integration.
  - Base Objects
  - Managed Objects
  - Client and Server Operations
- March 2010: Complete XML mapping of KMIP binary protocol

- March 2010: Namespace
- May 2010: Complete Enrollment and Discovery protocol
- June 2010: Complete specification initial draft
- June 2010: Start working group ballot
- July-August: Call for participation in sponsor ballot.
- October 2010: Working group ballot complete
- October2010: Start Sponsor Ballot:
- January 2011: Complete Sponsor Ballot and submit to IEEE
- March 2011: IEEE approves standard
- June - August 2011: IEEE publishes standard (typical 3-6 month delay between approval and publication)

Notes:

1. Optimistic schedule. What can be dropped?
2. Concerns about patent and copyright between OASIS/KMIP and IEEE. Most issues are believed covered but a memorandum of understanding between IEEE and OASIS is outstanding. This is an area that needs to be watched.
3. Some discussion around the core value added functions that P1619.3 is addressing.
4. June 2010 Date is important – this is a deadline for completing the work since the PAR for 1619.3 ends October 2011. A go/no-go decision should be considered at this point. Also for consideration is the relevancy of this work given the current status of KMIP.
5. This is a working draft of the plan, not a statement of position.