P1619.3: Key Management

(Project 1619.3 approved February 28, 2007) Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data

Note: As of December 2010, the Security in Storage Working group has voted to remove this PAR, due largely to the approval of the OASIS KMIP specification. The remainder of this page is for historical purposes.

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.

Patents brought to the attention of the chair

The following patents have been brought to the attention of the SISWG chair and may or may not be essential for a conformant implementation of P1619.3:

- U.S. Patent Application 20090092252 "Method and system for identifying and managing keys description/claims", assigned to Landon Noll and Robert Lockhart

- U.S. Patent 7453593 (No. 11948400 filed on 11/30/2007) assigned to Redhat, covers XMLSOAP used to send UNIX-like commands

- U.S. Patent application #20080219449 "Cryptographic key management for stored data" assigned to Quantum Corporation