To: IEEE P1619.3 Task Group
From: P1619.3 [subgroup or ad hoc committee], Members:
[Subhash Sankuratripati, NetApp]
[Ravi Kavuri, NetApp]
[Gaurav Agarwal, NetApp]
[Scott Kipp, Brocade]
[Landon Noll, Cisco]
[Kevin Marks, Dell]
[Jon Hass, Dell]
[Larry Hofer, Emulex]
[Glen Jaquette, IBM]
[Walt Hubis, LSI]
[Matthew Ball, MV Ball Consulting]
[Robert A. (Bob) Lockhart, nCipher]
[Jon Holdman, Sun]
[Luther Martin, Voltage Security]
[Michael Marcil, Vormetric]

Date: September 8, 2008
Purpose: Proposed changes against P1619.3/D3 to incorporate [Add Sections 4, 5 & 6 into the draft._]
[NOTE: Draft number proposed against should replace red x]

Introduction

The P1619.3 [subgroup or ad hoc committee] has been working on a proposal to create [Fill in an overview of what the committee is proposing].

[Please delete anything between brackets (including the brackets) and replace with the appropriate proposals]

[Rules and Guidance

a) *Diagrams can be submitted in color or grayscale. You may be asked to convert it if time is not on the editor's side at the moment.*

b) *All* [black bracketed] *text should be replaced with the appropriate information.*

i) *Note please delete this bullet completely. The format of the text is there for example purposes.*

c) *All text in dark red italics should be cut out of a document prior to submission (includes this entire section with numbering).*

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

d) *If you have verbiage or information that belongs in a section that Bob L. did not include you as creating, ignore Bob L.(this once only) and create away!*

e) *All dates that must be updated are automatically updated as you open & save the document. You should replace them with fixed dates for proposal and tracking purposes.*

f) *If you are not running a PC with Windows using Word, do not enable the macros. You should also avoid deleting them. Any documents that have to be cut and pasted back into a good macro document will cost you $25 to be put towards the WTSS subgroup (see P1619.3 meeting minutes dated September 17 2007).*

g) *Bob Lockhart will be participating off and on in all subgroups to monitor progress and assist with the documents as needed.]*

Changes to P1619.3/D3

[Change the red x to the appropriate draft number]

[Note any sections that are to be completely removed from the existing document.]
[Note sections that contain changes if the section is not to be fully deleted.]

1.Normative References

[Include any normative references in this section]

2.Definitions, acronyms, and abbreviations

For the purposes of this proposal, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards, Seventh Edition,* should be referenced for terms not defined in this clause.

[Ensure that definitions, acronyms and abbreviations do not already exist in the above reference]

2.1Definitions

***[2.1.term1:** select the 'definitions' and select 'format terms and definitions' in the IEEEStdsTemplate tool bar. If you do not have macro enabled please enter the number manually.]*

2.2Acronyms and abbreviations

[LAH List Acronyms (and/or abbreviations) Here]

[I have to manually edit the numbers here so just use standard body text formatting.]

3.General Overview

[Place any overview information as it pertains to the proposal in this section. Use section numbers appropriately. The editor reserves the right to move information from any section to a more appropriate section based on workgroup feedback]
[Architecture and Name Space belong in this section]
[We may need to move some or all of Name Space to section 5 or give it a separate section]

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

4.General Concepts and Models

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

5.Key Management Namespace

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

6.Key Management Objects

This section describes KM objects as they are transmitted across the wire to a KM client. Attributes that are 'persistent' across clients are listed in '**bold font'**. Attributes that are 'optional' are listed in '*italicized font*'.

6.1Key

Scope: Client & Server.

The Key object consists of the key blob (potentially wrapped) along its meta-data.

6.1.1Attributes

A key object distributed by a KMS contains the following attributes:

- **KEY_ID** (Type: SO_GUID)
- **FRIENDLY_NAME (**Optional: Type:String) Not necessarily unique within a KMS as additional attributes may be used to make a unique reference.

  Note: It should be possible to request a key by its Friendly_name (plus additional reference attributes if needed), and this may be used to hold prior key names for legacy key applications.

- **STATE** (Type:String) EDITORIAL: Reference back to the relevant section.
- T_EXPIRED (Type: UTC - time beyond which the key should not be used to encrypt new data)
- T_DISABLED (Type: UTC - time beyond which the key should be used)
- T_CACHED (Type: 64-bits – seconds that the key may be cached for. This may be differentiated by endpoint)
- **CIPHER_TYPE** (Type:String OID – **TODO:** Insert)
- KEY_BLOB (Object as defined in the next section) (This may be differentiated by endpoint, and is constructed from an immutable key value, the storage and representationof which is outside of this standard)
- *VENDOR_SPECIFIC_EXTENSIONS*
- *APPLICATION_EXTENSIONS*
- *CACHING_POLICY*
- (*VERSIONING_INFORMATION*:)

  Narrative: A KMS shall represent versioning of Key objects using two values: Version, which is an incrementally increasing value, representing changes to Key attributes, including changes to policies referenced by the key, and a GMT dateTime value representing the time of the last change. KM Clients may treat the combination as an opaque token, or use the values to protect against updates of stale copies. KMS servers may construct these values customized to the requestor, or maintain them globally independent of the endpoints. (for example, if a policy for a key changes, but that change is not relevant for an endpoint, the KMS may or may not represent update the versioning_Information. Versioning information will not change due to auditing activity, reference, inclusive Realm_Associations or backup.

  - *VERSION* (Type: unsigned Numeric)

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

(NOTE: It must be possible for an endpoint to request key object if altered since a reference version)

— *EDIT_DATETIME* (TYPE: DATETIME)

(NOTE: It must be possible for an endpoint to request a list of key objects altered since a reference time)

In addition, a KMS must be capable of representing the following attributes and references:

— REALM_ASSOCIATIONS (SERVER ONLY)

(Note: keys will not be delivered to endpoints without compatable Realm rights)

— *WRAPPING_POLICY*

— *DESCRIPTION* (Type:String)

— *ATTRIBUTE_ASSOCIATIONS*

(A list of named value pairs useable as an alternate mechanism to define or reference a key . Keys can be retrieved by their key_ID or alternatively by an ANDED match on these NVPs)

In addition, a KMS must be capable of representing the following associations:

— *USE_BY_CLIENTS*

(Note: does not alterVersioning_Information for a key itself. Note since any given key may be used by multiple clients or CUs, this tracking must be maintained, so the KMS is capable of initiating unsolicited updates to a KM Client when a key's attributes or policies change)

— *USE_BY_CUS (see above note)*

6.1.2States

As defined in the key state diagram (Editorial: as defined by the architecture sub-committee)

6.1.3Operations

— Create

— Get

— Store

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

6.2Key Blob

6.2.1Attributes

- ProtocolVersion (Type:int and defined as 1 for this version of the standard – This attribute will be remain constant for all clients for this version of the standard.).
- WRAPPING_TYPE (Type:String) – and can take any of the values as listed in the key wrapping section.
- Length (Type:int)
- Data (Type: Character Array)

  Editorial: CMS will be used to wrap keys. The updates necessary to add key wrapping will be done at a later point.

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

6.3Key_Template

Scope: Server.

Narrative Text: This object is not transmitted over the wire between the client and the server. The only attribute that a client needs to understand is the notion of 'key_template_id' which can be passed in as a DataSet attribute.

The Key_Template object consists of attributes and policies which may be inherited when creating a key (either by the KMS Admin, or by a key request). It does not represent any actual key.

It should be possible to make a key creation request "byTemplate", with or without additional dataset bindings. It is not possible to make a key retrieval request "byTemplate" without distinguishing dataset bindings.

Discussion: I suppose one could think of "template" as an additional "dataset binding" and use the same service as previously envisioned. The important notion here is the ability to predefine all the policy and attributes into some template to avoid having to manage all this separately.

6.3.1Attributes

A Key_Template object defined within a KMS contains the following attributes:

- **KEY_TEMPLATE_ID** (Type: SO_GUID)
- **FRIENDLY_NAME (**Optional: Type:String) Unique within a KMS

  Note: It should be possible to request a key creation by template using its Friendly_name
- **CIPHER_TYPE** (Type:String OID – **TODO:** Insert)
- *VENDOR_SPECIFIC_EXTENSIONS*
- *APPLICATION_EXTENSIONS*
- *CACHING_POLICY*
- (VERSIONING_INFORMATION:)
  - *VERSION* (Type: unsigned Numeric)
  - *EDIT_DATETIME* (TYPE: DATETIME)
- *REALM_ASSOCIATIONS*
- *WRAPPING_POLICY*
- *DESCRIPTION* (Type:String)

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

6.4ENDPOINT_TYPE

Endpoint_Type is an object to simplify the need to exchange capabilities between a KM Client or CU and a KM Server, as well as managing a collection of capabilities at the Server. (Discussion point: It would be desirable if these values were standardized in some registry.) An Endpoint_Type will always equate to a deterministic set of capabilities, though the converse need not be true. During registration, KM Clients or CUs will present identifying information that will allow a KM Server to map it to an Endpoint_Type.

6.4.1Attributes

- ENDPOINT_TYPE_ID (Type:TBD)
- CAPABILITIES (Note: common registry should allow retrieval of such characteristics as has-certificate, understands-time, min and max keyID lengths, never-exposes-key, hasHSM, etc.)

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

6.5REALM (optional)

Realms are used to segment objects into separate administrative domains.

Administrative users and endpoints requesting key services will have “RealmAssociations” which will allow many to many representations specifying differing rights. For example, a policy may be deleted by an administrator belonging to a realm which also has delete capabilities on the policy, while an administrator in a realm with only read rights may use the policy, but can not delete or edit it. While a KMS may implement administrative “Roles”, Realms allow segmentation based on data characteristics rather than functional capabilities.

When a KMS provides Realm support, the KMS must insure no object is assessable unless the requesting endpoint or administrator has been properly associated with an incorporating realm that allows the access. Realms must allow the following distinctions: create, edit, delete, read, reference (use but not view). The most privileged right from any associated realm may be use to determine an access.

6.5.1Attributes

- REALM_ID (Type *TBD*; where domain is a string that is in compliance with DNS name as defined by RFC 1034.
- DESCRIPTION

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

6.6CU Cryptographic Unit

Scope: Client & Server

Narrative: While there is no direct communication with a CU, there will be certain end points which may want to present an identity to the KM Server, so key information can be conveyed in a secure and predictable manner to the CU.

6.6.1Attributes

- CU_ID (Type:SO_GUID)
- Array of Name/Value pairs.

  NOTE: The name of the attributes that are part of the CU object shall follow the following convention:

  CU://domain/context/attribute-name where domain is a string that is in compliance with DNS name as defined by RFC 1034.

  In addition – the following domin/context combination – ieee.org/siswg/ is reserved for use by this standard.
- REALM_ASSOCIATIONS (Server Only)
- ENDPOINT_TYPE_ID (TYPE:TBD Server Only.)

  DiscussionPoint: ~~Prefer this to be some IEEE registry.~~ note: KMS Clients shall provide a CIM_PhysicalElement or CIM_SoftwareIdentity object upon registration of a CU, which will allow a KMS to map an entity to a TYPE_ID. Or perhaps we define a new CIM object derived from common ones to include capabilities we want that may not be determined by attributes in the mentioned CIM objects.
- CLIENT_ASSOCIATIONS (Server Only)

  Note this might be done with a Client_Group. A CU will initially be associated with full rights granted to its registering Client. Other behaviors to manage associations is outside the scope of this spec., but a KMS must be capable of conforming to a policy or configuration that prevents a CU from receiving its key from an "unauthorized" client. This can easily be accomplished by restricting access to keys both to authorized KMS clients and authorized CUs.)
- *AUTHENTICATION_POLICY*
- *AUTHENTICATION_VALUES (It must be possible for a CU to authenticate to the KMS through an untrusted KM Client)*
- *List of {CREDENTIAL_LENGTH,CREDENTIAL_VALUE} tuples.*
- *WRAPPING_POLICY. (Note: this may typically be inherited via endpoint_type_id)*
- *WRAPPING_VALUES (Since CUs can uniquely protect some wrapping values, such as private keys, data can pass through a KM Client without exposure)*

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

6.7Client

Scope: Client & Server.

The client object consists of its credentials and capabilities.

6.7.1Attributes

- CREDENTIAL_TYPE (Session, Username/Password, Symmetric / Asymmetric key, SSO, CHAP)
- List of {CREDENTIAL_LENGTH,CREDENTIAL_VALUE} tuples.
- REALM_ASSOCIATIONS
- **ENDPOINT_TYPE_ID**
- WRAPPING_POLICY

6.7.2States

- Active
- Disabled/Locked
- Authenticated

6.7.3Operations

- Create
- Delete
- Authenticate
- Disable

NOTE: All of these operations with the exception of authenticate are performed by way of KM Console operations and are outside the scope of the standard.

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

6.8Capability

6.8.1Attributes

- Name (Type: String)
- Supports AES 128
- Supports AES 256
- Supports 3DES
- Understands Relative time (elapsed time)
- Understands Universal time
- Includes HSM
- Includes TPM-
- Has Cert
- Has PKI key pair
- min and max keyID lengths
- never-exposes-key
- is client-cu Hardware combo
- is_Kernel Software
- is User Space Software
- is Hardware
- Utilizes Host for Crypto
- can Persistently Cache keys
- Offers api to provide key in clear
- .. and more tbd

6.8.2States

None.

6.8.3Operations

No direct operations. The capability object is sent as part of the capability negotiation operation, or constructible by reference to an endpoint type

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

6.9Data Sets

Scope: Client, CU & Server.

Data sets represent manageable units of encrypted data. Data sets are expressed as selection rules that can be applied to data set attributes such as file path, tape volume id, server IP, or a range of disk blocks. There should be flexibility in defining what a data set is, depending on the position of the encryption agent "in the stack" of the storage infrastructure.

Once the data sets are identified, keys may be associated to data sets via a key assignment policy.

6.9.1Attributes

- NAME
- VALUE
- SIZEOF_VALUE

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

6.10Client Groups

Scope: Server only.

Clients may be grouped together for ease of management. This grouping may be static – i.e. clients are explicitly added into a group or dynamic i.e. based on a regular expression match on client attributes.

6.10.1Attributes

- TYPE (STATIC or DYNAMIC)
- List of CLIENT_SO_GUIDs (only in case of static binding)
- List of {PATTERN, ATTRIBUTE} tuple.
- REALM_ASSOCIATIONS

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

6.11Key Groups

Scope: Server only.

Keys may be grouped together for ease of management. This grouping may be static – i.e. explicitly added into a group or dynamic i.e. based on a regular expression match on dataset attributes.

6.11.1Attributes

- TYPE (STATIC or DYNAMIC)
- List of CLIENT_SO_GUIDs (only in case of static binding)
- List of {PATTERN, DATASET} tuple.
- REALM_ASSOCIATIONS

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

7.Key Management Policies (KM Server only)

This clause only applies to the KM server and does not represent objects sent between the KM server and the KM client. These objects may be represented in KM Server to KM Server operations.

A policy is a deliberate plan of action to guide decisions and achieve rational outcome(s).. In the same vein, Key Management Policies are used to guide assignment, retention, wrapping, replication & access control decisions on keys.

The scope of some policy objects will extend to an endpoint.

7.1Key Assignment Policy

Key Assignment Policies contain logic that is able to determine which data set should be encrypted with which key using which algorithm (e.g. encrypt and sign all emails sent outside of the company. Sign all tapes with a unique key per tape, etc.)

A key assignment policy determines

- the type of unencrypted data that is determined to be encrypted with a specific key.
- how often to generate new keys

Therefore, the key assignment policy encapsulates both key generation and key scope policies. This is done to fit regular usage patterns. For example, when a tape is loaded into a drive, the drive will request a key by data, and will receive both a key that may be used on that drive, as well as a policy notifying the drive whether all tapes should be encrypted with this key, or only the current tape.

The key assignment policy is determined by the set of supported data set attributes, and is encoded as a set of name, value pairs.

The policy is interpreted to mean that the key may be used whenever all the named parameters have values equal to the values of the data presented to the client. So, for example, in the following encryption policy:

container attribute name = ”storage_server_name” value=”Ireland.com”

data attribute name = ”financial”

The provided key may be used to encrypt all of the data tagged as “financial” on the storage server named “Ireland.com” with the key listed in the KeyExchangeStructure.

Note that there is a difference between a data set binding and an assignment policy, and the KMS must track both. An organization may set a policy to encrypt a pool with a specific key, but due to key rotation policies, not all tapes within the pool will have been encrypted with that key. Therefore, assignment policies specify the current desired behavior, whereas the KMS will store all data set bindings that are reported to it, for future audit and key query commands. State logic within the KMS may allow for the automatic creation of key assignment policies based on the “most recent” data set binding.

7.1.1Attributes

- KEY_ASSIGNMENT_POLICY_ID
- DESCRIPTION

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

— REALM_ASSOCIATIONS

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

7.2Retention Policy

7.2.1Overview

The retention policy dictates the duration for which protected data, hence the key with which it is encrypted, is accessible to a given client. It also dictates when new data should no longer be encrypted with a given key.

This policy should be superseded by the key life cycle.

7.2.2Attributes

- RETENTION _POLICY_ID
- DESCRIPTION
- REALM_ASSOCIATIONS
- T_EXPIRATION
- T_DISABLE

7.2.3States

- Created
- Assigned
- Enforcing
- Disabled

7.2.4Operations

- Add
- Associate
- Disassociate
- Delete

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

7.3Wrapping Policy

The wrapping policy indicates whether a key should be wrapped prior to being dispatched to a client. This policy may be referenced from the key object, ?a key_group?, a client object, ?a ClientGroup?, a CU object, or a Endpoint_type. If multiple policies are defined then the order of precedence shall be per the following:

1. Key shall prevail over KeyGroup
2. Key or KeyGroup shall prevail over CU
3. CU shall prevail over CU's Endpoint_Type
4. Client shall prevail over Client's Endpoint_Type
5. If both a CU and Client specify (or inherit) a Wrapping Policy, the key will be double wrapped, first by policy prevailing for the CU, then by prevailing ClientPolicy. The KM Client will unwrap the key and pass the wrapped Client_Key for subsequent unwrapping.

7.3.1Attributes

- WRAPPING_TYPE (asymmetric / symmetric / signature)
- WRAPPING_MODE (as listed in the key blob section)

7.3.2States

- Created
- Assigned
- Enforcing
- Disabled

7.3.3Operations

- Add
- Associate
- Disassociate
- Delete

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

7.4Audit Policy

Audit policies state the auditing requirements that need to be enforced on keys and clients.

TODO: Bob Lockhart to provide new content.

7.4.1Attributes

- Operation type
- Event type (to trigger, Log, SNMP trap, etc.) Mandatory: Log
- Event Dispatch Destination (Local, SNMP, syslog) Mandatory: Local, syslog.

NOTE: The only mandatory type that should be supported is ‘log’ and the mandatory dispatch destinations are local and syslog.

7.4.2States

- Created
- Assigned
- Enforcing
- Disabled

7.4.3Operations

- Add
- Associate
- Disassociate
- Delete

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

7.5 Access/Distribution Policy

Key access policies encode which clients and key management servers may access which keys. This may be controlled by the clients or CUs, as a key creation request may set the data set bindings of a key, but it is enforced by the KMS, which lookup tables storing keys to data assignments, and clients to data permissions, always enforcing any realm restrictions.

In addition, the KMS administrator for a key's realm may alter a key's access and distribution policy.

This policy is referenced by a key or key group.

Note: this policy governs what endpoints MAY receive a key, but can not be used to determine which endpoints in fact received any given key.

7.5.1Attributes

- SO_GUID
- Client or clientGroup list
- CU list
- KM server list.
- REALM_ASSOCIATIONS

7.5.2States

- Created
- Assigned
- Enforcing
- Disabled

7.5.3Operations

- Add
- Associate
- Disassociate
- Delete

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

7.6Caching Policy

The key caching policy dictates whether a key shall be cached by a KM client and if so, the duration for which it it is cached.

Attributes

- CACHING_TYPE, T_CACHE_INTERVAL tuples (list)

  Note: It should be possible to allow different time intervals for caching depending on the security of the caching along different attributes such as HSM, TPM, neverExposedHardware,

  - HARDWARE TYPE – (e.g., HSM, TPM, FIPS 140-2 Approved, software)
  - DESTINATION (particular clients, where it is stored in a file, is it unwrapped in memory)
  - STANDARDS CONFORMANCE (FIPS 140-2, VISA PCI,...)
  - CACHE_TIME – Number of seconds the CU is allowed to cache a particular key
  - USAGE_COUNT – How many times can the CU use the key before purging from cache (do we need this – general feeling was that it's not generally applicable, but could be used with credit cards)

Applicable objects

- Key Object
- Key Group Object
-

7.6.1States

- Created
- Assigned
- Enforcing
- Disabled

7.6.2Operations

- Add
- Associate
- Disassociate
- Delete

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

8.Key Management Operations

8.1Register KM Client

Scope: KMCS Ops, including registration for KM Client or CU

8.1.1Overview

This operation allows clients to register themselves with a KM server. These clients by default, should be placed in an administrative realm where they are not allowed to perform any operations unless an administrator approves their transition from an ‘unapproved’ state to an ‘approved’ state by verifying the authentication credentials that have been provided to by the client.

This behavior may be modified based on the trust that a KM server has on the credentials that are being presented to it. Examples of such trust might include CA signed certificates, trusted Kerberos realm, etc.

Though support for this operation is mandatory, a KM server might require an administrative action to enable this operation. Based on the threat model in which the server is deployed, a KM server shall provide an administrator the ability to disable this operation.

8.1.2Input / Output / Error

- (I): Client
- (I): Credentials
- (O): Boolean (SUCCESS OR FAILURE)
- (E): E_SELFREGISTRATION_UNSUPPORTED.

8.2Authenticate

Scope: KMCS

8.2.1Overview

A client needs to authenticate with the KM server to perform any sensitive operations. Authentication is accomplished either at the transport level (SSL/TLS) or at the object/messaging level. Every request shall contain the “credential” object so that the KM server can validate the client.

8.2.2Input / Output / Error

- (I): Client
- (O): Credentials (If the request type is login and not validation)
- (E): E_INVALID_CREDENTIALS
- (E): E_UNSUPPORTED_AUTHENTICATION_MODE

8.3Capability Negotiation

Scope: KMCS

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

8.3.1Overview

The client sends its capabilities to the server and the server returns back a list of capabilities it supports. If none of the capabilities are supported, then it returns back an empty list.

8.3.2Input / Output / Error

- (I): Client
- (I): List of Capability Objects
- (O): List of Capability Objects that are supported by the KM server

8.4Get Server Capabilities

- (I): Client
- (O): List of Capability Objects.

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

8.5Create/Generate Key

Scope: KMCS, KM Console

8.5.1Overview

A client upon authentication invokes the Generate key operation to generate a new key by passing in the KeyTemplateID and/or DataSet context in which this key would be used so that the KM can apply the appropriate policies.

8.5.2Input / Output / Error

- (I): Client
- (I) *CU_ID* or EndPoint's CIM Object - Identifier of final destination for the key.
- (I): List of Dataset objects.
- (O): Key (including unique So_Guid)
- (E): …

8.6Store Key

Scope: KMCS, KM Console

8.6.1Overview

Keys that are generated at the client can be stored in the KM server by invoking its store functionality.

8.6.2Input / Output / Error

(I): Client

(I): List of Dataset objects.

(I) *CU_ID* or EndPoint's CIM Object - Identifier of final destination for the key.

(O): Key_SO_GUID

(I) *Friendly_Name*

(E)…

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

8.7Get Key

8.7.1Overview

Clients invoke the get key operation to fetch keys from the KM server. They may invoke the query based on either a Key ID or FriendlyName, and/or based on the Dataset attributes. When querying based on dataset attributes, the KM returns a key based on the application template and the policies that govern the key and the client.

8.7.2Input / Output / Error

(I): Client

(I) CU

(I): List of Dataset objects.

(O): Key

(E): …

8.8Push Audit Message

8.8.1Overview

This operation is intended to be used by 'super' clients that maintain local caches of keys and ship them out to cryptographic units on demand. This will ensure that the KM Server can be a central audit repository for any/all accesses to keys.

Discussion: Marcil: I think this should be broader than presented, which only covers one type of message. For example, an encrypting drive may be configured locally to unlock the drive and therefore no longer need a key. Or an existing key may be used for another device. It would be good to have an audit message that reflects these. Audit messages should also be batchable and uploaded in a file.

8.8.2Input / Output / Error

(I): Client or CU

(I): Key_SO_GUID

(I): Message (Optional)

(O): Boolean – SUCCESS/FAILURE.

(E): …

8.9Get Random Bytes

8.9.1Input / Output / Error

— (I): Client (question: why?)

— (I): numbers of bytes desired

— (O) Base64 Encoded bytes

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

8.10GetStatus --KM Client Service (optional) -- [Server initiated]

Server asking client for status.

Discussion: To aid KMS Administrators to provide key management for endpoints, we will need some mechanism to gather status on endpoints, including operating mode, Keys in use, status of any rekeying, We could try and define some predetermined status types or just allow these to come back with what the KMS Client and CU can provide.

Discussion: This probably matches the concepts of some existing WSMAN service.

- (I): Target of Interest Type: filter expression
- (I) *Locale* – requested language for any NVPs
- (O) *Locale – language used for NVPs*
- (O) Endpoint + NVPs

8.11UpdatePending --KM Client Service (optional) [Server initiated]

Server notifying client of relevant updates.

KM Clients expose this service. KMS Servers will repeat this service until the client acknowledges currency by virtue of matching UpdateVersioningTokens. Note, these tokens are used for sequencing between this service and GetChangeList. A simple implementation of this would be for the KMS Server to maintain a VersioningToken to represent the latest version of "Everything" for a KM Client or CU and a response to a GetUpdateList that returns everything.

- (I): Type (Keys, AllKeys and custom types)
- (I) Scope: (KM Client or CU identifier)
- (I) UpdateVersioningTokens - KMS server sends its tokens representing the state to which the client (or CU) needs to update.
- (O) UpdateVersioningTokens - KMS client sends its tokens representing the state it has received

8.12GetUpdateList --KM Server Service [Client initiated]

Discussion: can this be done with a WS-ENUMERATE service?

- (I): Type: (Keys, AllKeys and custom types)
- (I) Scope: (KM Client or CU identifier)
- (I) UpdateVersioning Tokens (zero values will result in all requested instances of requested type)
- (O) requested objects
- (O) New UpdateVersioningTokens

9.Key Management Transport

[Supported transport protocols go here]

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

10.Key Management Messaging

[This is an additional section that I am proposing we add to help complete the standard. It does not currently exist in Draft 1.]
[This section would contain normative information for the XML and/or TLV formats we decide to support]

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Annex A

(informative)

Bibliography

[List all bibliographic material here]

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Annex B(informative)

Example Use Cases

[Objects & operations or use cases should add the appropriate use cases here]

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Annex C(informative)

XML and TLV Schema Definitions

C.1XML Schema

[Additional messaging group information for selected XML syntax goes here]

C.2TLV Schema

[Additional messaging group information for selected TLV schema goes here]

Copyright © <year> IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.