THALES

Proposals for P1619.3

Bob Lockhart, Sr. Solutions Architect
Thales Information Systems Security
May 6, 2009

Caveats, Generalities and other Minutia

General Minutia

- Requirements are only shown for objects, policies or operations
  - Attribute requirements need to be revisited across the entire standard so I have left them out for now
- This is only a proposal and I am really looking for feedback!
  - Revised state model is still a work in progress so I would like lots o feedback there
- Everyone should allow others to complete their comments prior to responding
  - If you can't get a word in edgewise raise your hand on WebEx and Walt will own who gets to speak
- Detailed proposal for insertion into Draft 7 to follow for accepted additions, changes and/or deletions
- These changes if accepted should not be considered final so if you don't get your comments in now feel free to use draft comment process.

Additions

- Key Set Object
- Key Granularity Policy
- Replication Policy

Changes

- Key Object (Draft 6 Clause 6.1)
- Key Blob to Key Block (Draft 6 Clause 6.2)
- NIST Key State to P1619.3 Key State Mappings and Back (Draft 6 Clause 4.4)
- New Key State Model

ADDITIONS

Key Set Object

Key Set

- A set of keys used to encrypt a common set of data over time
  - Keys change or are updated as a result of re-key or replication operations
- Keys can be retrieved by Key Set SO_GUID
  - Older keys retrieved by Key Set SO_GUID and Key Creation Time
  - Older keys retrieved by Key Set SO_GUID and Key Count
- Single key in active state
  - All other keys in expired or later state
  - Other considerations for more keys in active state (think files)

Requirements

- KM Server Optional
- KM Client not applicable
- Require Attributes
  - Key Set SO_GUID
  - Key Set Creation Time
  - Current key SO_GUID
  - Key Number
  - Key Count
  - Key Set List
- Optional Attributes
  - Key Set Name
  - Key Count
  - Key Set State

Key Set

Attribute	Type	Description
Key Set SO_GUID	String	Common SO_GUID for a set of keys
Creation Time	Date Time	
Key Number	Integer	Incremental number starting with 1 assigned to keys in list
Key Count	Integer	Number of keys that have been in key set (avoids the key purge issue)
Current Key SO_GUID	String	Current key SO_GUID
Key Set List	Structure	List of all SO_GUIDS associated with a Key Set including current Key

Key Granularity Policy

Key Granularity

- Defines the minimum number of keys based on a KMS hierarchy
  - Key per KMS
  - Key per Realm
  - Key per Group
  - Key per Device
  - Key per Media
  - Key per Data Set
  - Key per Object

Requirements

- KM Server Required
- KM Client Optional
- Required attributes
  - Policy SO_GUID
  - Granularity Value
  - Date Created
- Optional attributes
  - Policy Name
  - Date Modified

Key Granularity Policy Attributes

Attribute	Type	Description
Policy SO_GUID	String	Globally unique policy identifier
Granularity	Integer	See next slide for details
Date Created	Date Time	Date and time policy created
Policy Name	String	User readable policy name
Date Modified	Date Time	Date and time policy last modified

Granularity Values

Granularity	Value	Examples
KMS	0x00	A single key for all entities within a KMS (no granularity requirements – default) NOTE: Not practical or recommended but needs to be defined for devices that want a policy to be set
Realm	0x01	A single key for all groups within a realm NOTE: Attempts to ensure keys do not cross realms without specific policies allowing so (encrypt in one realm, decrypt in the other)
Group	0x02	A single key for all devices associated with a group
Device	0x03	An array, a library, a file server, laptop, a database, an application
Media	0x04	A database table, a tape cartridge, a disk, a file system, Flash storage device
Data Set	0x05	a database table column, a backup set on a tape, a slice of a disk, a directory in a file system
Object	0x06	A database record, a tape block, a range of sectors on a disk, a file, each version of a file
Extensions	0x80	Vendor or end user defined extensions

Replication Policy

Replication Policy

- Defines requirements for replication of keys, policies and other security objects
- Synchronous or Asynchronous replication
- Number of replications required
- Security requirements of replication

Requirements

- KM Server Required
- KM Client Optional
- Required Attributes
  - Policy SO_GUID
  - Date Created
  - Replication Type
- Optional Attributes
  - Policy Name
  - Date Modified
  - Number of Replications
  - Security Requirements

Replication Policy Attributes

Attribute	Type	Description
Policy SO_GUID	String	Globally unique identifier for the policy
Date Created	Date Time	Date and time policy created
Replication Type	Binary	0 = Synchronous, 1 = Asynchronous
Policy Name	String	User readable name of policy
Date Modified	Date Time	Date and time policy last modified
# of replications	Integer	Number of times a key must be replicated for protection purposes
Security Requirements	Octet	Minimum security level of devices where key is to be replicated
None	0x00	No security requirements defined
FIPS Level	0x01-0x04	Correlates with FIPS 140-2 Levels 0x01 = Level 1, 0x04 = Level 4
CC Level	0x05-0x0B	Correlates with CC Earned Assurance Levels 0x05 = EAL 1, 0x0B = EAL 7
Extensions	0x80+	Custom attributes defined by vendors or end users

CHANGES

Additions

- Add State Change Time Stamp attributes
  - Implement new state model
  - Creation time required
  - All state change time stamps optional
    - Add time stamp attributes for all states not just a few
- Creator ID attribute
- Key Set Member attribute

Changes

- Specify all time stamps must be in GMT
- Change Friendly Name to Key Name
- Convert Cipher Type to Integer versus OID
- Consolidate vendor and application attributes into extended attributes

Deletions

- Description (consolidate into extended attributes)
- Attribute Associations (vendor specific implementation)

Key Object Attributes

Attribute	Type	Description
Key ID SO_GUID	String	Globally Unique Key Identifier
Key Name	String	Human readable non-unique Key Identifier
Key Block	Structure	Keying material stored as block of data
Key State	Value	Current state of key as defined in Clause 4.4
Creation Time	Date Time	Date/Time using GMT
Activation Time	Date Time	Date/Time using GMT
Disable Time	Date Time	Date/Time using GMT
Expiration Time	Date Time	Date/Time using GMT
Destroy Time	Date Time	Date/Time using GMT
Compromise Time	Date Time	Date/Time using GMT

Key Object Attributes (continued)

Attribute	Type	Description
Cipher Type	String	OID String of Algorithm and/or Algorithm/Mode Pair defined by various standards (see http://grouper.ieee.org/groups/1619/SISWG_OID_registry.txt for example)
Extended Attributes	Structure	Name/Value Pairs of vendor or application specific attributes
Wrap Type	Integer	Key Wrapping
Policy List	Structure	Name/Value Pairs of applicable policies for given key Name = Policy Name Value = Policy SO_GUID } Flip?
Version	Integer	Incremental value based on changes to key attributes or other metadata

Key Object Attributes (continued)

Attribute	Type	Description
Edit Time	Date Time	Time attributes last modified by administrator. Does not include state changes.
Source ID	String	SO_GUID Identifier of RNG (KM Server where key was generated)
Creator ID	String	SO_GUID of where creation request was generated (KM Server or KM Client)
Key Set Member	Boolean	Denotes if key is member of one or more key sets

Additions

- None (at this time)

Changes

- Change Name to Key Block

Deletions

- None (at this time)

NIST SP800-57 Part 1 to P1619.3 Key State Mappings

NIST Key State	P1619.3 Key State
Pre-Activation	Pre-Activation
Active	Active
Deactivated	Disabled
Compromised	Disabled - Compromised
Destroyed	Destroyed
Destroyed - Compromised	Destroyed - Compromised

P1619.3 to NIST SP800-57 Part 1 Key State Mappings

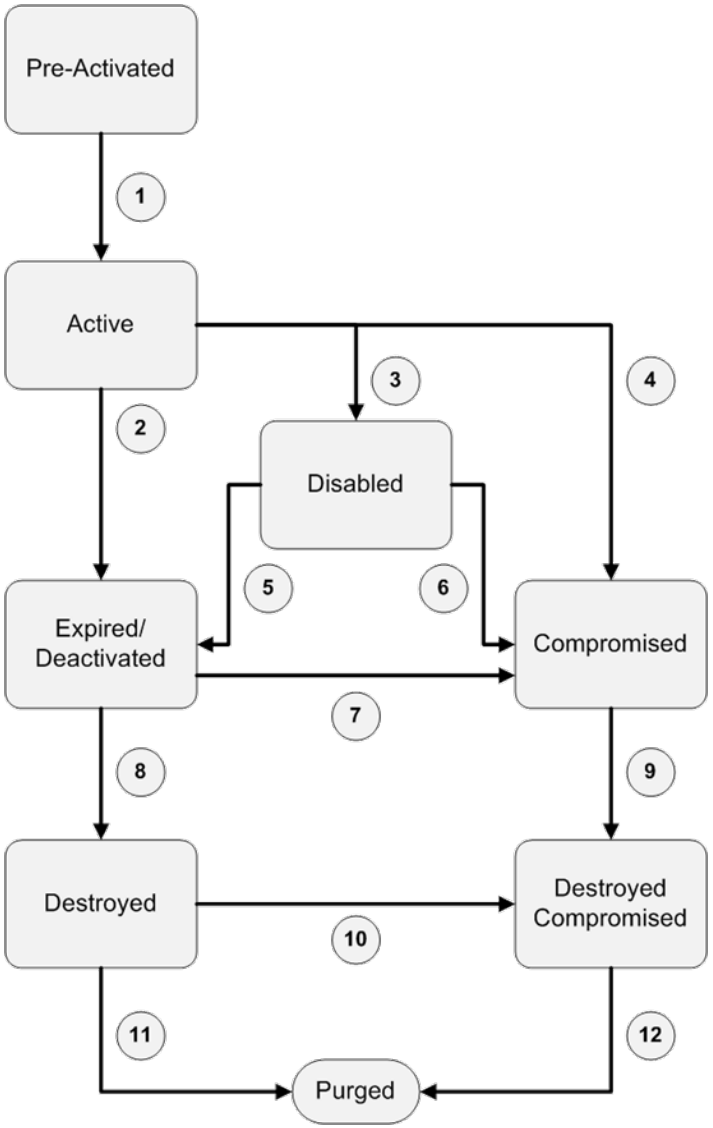
P1619.3 Key State	NIST Key State
Pre-Activation	Pre-Activation
Active	Active
Process Only	Active
Expired	Deactivated
Compromised	Compromised
Disabled	Deactivated
Disabled Compromised	Compromised
Destroyed	Destroyed
Destroyed Compromised	Destroyed-Compromised

Revising the Key State Model

Modify Key State Model to be more inline with NIST

- Move “Process Only” to Policy for usage (Protect Only, Process Only, Protect & Process)
- Place Disable above expired in the chain
  - Disabled key is a temporary state to determine if data has been lost or key is compromised in order to move it to Expired state
  - Removes the need to create policies and provides a state that can be set by Business Applications or KM Clients
- Remove Disabled-Compromised state
- All other states remain same
  - Consider lining up names with NIST states (Expired becomes Deactivated)

New State Model



All states have same description as before

- Modifications are removal of states that are policies and association of state transitions and moving disabled to appropriate place
- Modifications and renumbering “fairly” straight forward
- Reduces state model complexity
  - Fewer states and transitions