KMIP Client Registration Ideas for Discussion

Alan Frindell
SafeNet, Inc
9/29/2010

Entity Definition

Object	Encoding	REQUIRED
Entity	Structure	
Unique ID	Text String	Yes
Subject	Structure	Yes
Operation Policy Name	Text String	No, if not present default entity operation policy is used
Attribute	Structure	Yes, MAY be repeated

- Entity Unique ID may be passed in Credential object
- Subject comes from Access Control proposal.
- Named Operation Policy specifies if this entity can issue operations that create objects like Create, Register, Create Key Pair. May also control registration of Entities.
- The default entity operation policy is All Operations allowed (same as v1.0)
- Attributes including custom attributes can be associated with the Entity and can be searched via Locate or retrieved using Get or GetAttributes

How are entities created?

Manually entered by server administrator

Imported from a third-party directory by a server administrator

Registered by a KMIP client with appropriate permissions

- Some server implementations may require administrator approval before the entity is registered

What can you do with an entity?

- Require subjects passed in TLS and/or Credential to be registered entities
- Register or generate data that can be used during authentication, possibly to a third party system
- Restrict operations that create objects
- Register Attributes that can be searched and retrieved
  - Possible policy relevant attributes like FIPS Level, hardware capabilities
- Register extended data that can be logged by the server

Automated TLS certificate creation
(from Sun KMP)

Assumption: Client and server share an authentication passphrase

Part I – Plaintext

1. Client sends subject information to server
2. Server replies with CA Certificate and client authentication challenge

Part II – TLS with server-only authentication

1. Client sends client authentication response and server authentication challenge to server
2. Server verifies client authentication response
3. Server generates key pair and certificate, signs certificate
4. Server replies with server authentication response, private key, certificate
5. Client verifies server authentication response, stores private key and certificate