KMIP Entity Object and Client Registration

Alan Frindell -- with input from Robert Haas
SafeNet, Inc
11/17/2010

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, including other entities
- Register Attributes that can be searched and retrieved
  - Possible policy relevant attributes like FIPS Level, hardware capabilities, server to client operation support
- Register extended data that can be logged by the server
- Ask server to notify entity when one or more objects change

Credential Redefinition

Object	Encoding	REQUIRED
Credential	Structure	
Credential Type	Enumeration	Yes
Authentication Information Type	Enumeration	No
Credential Value	Structure	Yes

Object	Encoding	REQUIRED
Credential Value	Structure	
Subject Value	Varies according to Credential Type	Yes
Subject Authentication Information	Varies according to Authentication Information Type	No

- Username and Password Credential Value still supported for backwards compatibility

Credential/Subject Types

Credential/Subject Type	Value
Username and Password (KMIP v1)	00000001
Username	00000002
Device	00000003
World Wide Name	00000004
Distinguished Name	00000005
SAML Subject	00000006
WS Security Token	00000007
Open ID	00000008

Authentication Information Type	Value
Password	00000001
Extensions	8XXXXXXX

Entity Definition

Object	Encoding	REQUIRED
Entity	Structure	
Credential	Structure	Yes, May be repeated

Entity Attributes:

- UUID, Name, Object Type, Operation Policy, Initial Date, Destroy Date, App Specific Info, Contact Info, Last Change Date, Custom Attributes

Entity Operations:

- Register, Locate, Get, Get Attributes, Get Attributes List, Add Attribute, Modify Attribute, Delete Attribute Destroy

Default Operation Policy for Entity Objects

Operation	Object Type	Policy
Create	Symmetric Key	Allowed to all
Create Key Pair	Public Key, Private Key	Allowed to all
Register	All	Allowed to all
Certify	Public Key	Allowed to all
Re-certify	Certificate	Allowed to all
Validate	Certificate	Allowed to all
Query	N/A	Allowed to all
Cancel	N/A	Allowed to all
Poll	N/A	Allowed to all

How are entities created?

Manually entered by server administrator

Imported from a third-party directory by a server administrator

Explicitly registered by a KMIP client with appropriate permissions

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

Implicitly registered by a KMIP client by sending a new Credential object in a request