KMIP client registration

Options for discussion

Assumptions in the KMIP 1.0

- Client registration and the establishment of security is based upon out of band methods for SSL/TLS certificates
  - When you set up clients you configure SSL/TLS mutual authentication
  - Decision was to keep establishment of trust outside of the protocol

Beyond 1.0

- Problems with manual client registration
  - Certificate management challenges for some adopters
  - Automated client registration is desirable for some customers
    - Administrator monitoring and intervention may help mitigate risks

Security for KMIP

- Can the client connect to the server
- How is the client identified
- Why should these be not linked
  - Certificate management complexity
  - Proxy deployments
  - Device mobility and the amount of storage available for possibly storing a certificate
- Why they should be linked
  - Simplicity of definition, certificate security
  - Strong linking may provide security benefits

Right to connect

- SSL/TLS authentication – different levels of rigor
  - Server only – not supported or recommended
  - Client
    - Could be used by all clients
    - A group of clients
    - Unique per client
- Implementations could decide what certificates to trust
- Implementation dependent methods for establishment of trust

Client identification – userid and password

- Client identifier
  - Hardware serial number
  - Volume name
  - Application instance name
  - Some unique identifier
- In addition to the client identifier we should define a shared secret like a password which can be used in the authentication of the client
  - Optional because some implementations may not have the ability to store a shared secret
  - Could be used for encryption of client identifier but focus is only for authentication

Client identification

- Why use a shared secret for client authentication?
  - Model that users understand – for instance wireless setup
  - Sneaker net provides the trust
- When a client connects collect the context of the connection
  - WWN
  - Environment identification
- Could the context of a request be a substitute for shared secret or other client authentication?
  - This is probably less secure

Association of certificate to client

- Could have strong association
  - Extend x.509 attributes to include client identity
- We could support this mode of operation if desired

Questions for discussion

- How do we have unique client identifications?
  - Vendor qualifier
  - Registration authority
  - Namespace registration
- Should we be standardizing how the clients are grouped?
  - Named instances of groups
  - Owners of the clients/groups

Recommendations for 1.1

- Optionally separate right to connect from identification
- Methods of establishing trust for SSL/TLS authentication implementation dependent
- Support flexible client identification
  - With or without shared secret
- Defer standardizing capturing other client information and grouping of clients