(text for inclusion in Usage Guide or in Authentication Suite profiles)

KMIP Client Registration Models

The KMIP V1.2 Use Cases document describes several common approaches to registering KMIP clients with KMIP servers:

* Manual client registration within a single trust boundary
* Automatic client registration across multiple trust boundaries
* Configuring a KMIP Server for use with Automatic Client Registration

As described in that document, the goal of these three use cases is to establish the KMIP-interoperable secure channel or channels between KMIP servers and clients, such as a mutually-authenticated TLS channel.

The use cases establish high-level process flows for these three approaches to establishing the mutually-authenticated TLS channel described in the KMIP authentication suite profiles. In order to support the goal of establishing an interoperable approach to establishing this channel, this section provides more detailed information about these approaches to client registration.

Reflecting common usage for KMIP, all three of the scenarios described below discuss the use of X.509 certificates for trust establishment; other mechanisms, such as quantum key distribution, may be used instead but are not described here. Similarly, all three scenarios describe the establishment of a mutually-authenticated TLS connection as the basis trusted exchange of KMIP messages, corresponding to the published KMIP authentication suite profiles; other authentication mechanisms can be used with KMIP, but are not described here.

* 1. Manual Client Registration

The use case process flow in section 7.1 of the KMIP Use Cases document describes the interaction between human actors responsible for the client and server systems, resulting in the client administrator receiving a registration packet that can be used to authenticate the client to the server and to confirm the authentication of the server by the client.

In this approach, there is no assumption of pre-population of authentication credentials in the client, such as by installing an X.509 certificate into a tape library or drive during the manufacturing process. Rather, a credential is propagated out-of-band to the client administrator, who installs it into the client environment. The credential is then used on initial and subsequent contact between the client and server systems.

The most common registration model that takes this approach entails the server administrator creating a package that contains 1) X.509 certificate that the client will use to identify itself to the server when creating a TLS mutually-authenticated session; 2) information about the X.509 certificate that will be presented by the server to the client during negotiation of the mutual authentication, enabling the client to verify the server identity; and 3) possibly additional information that can be included in the credential of the KMIP message sent across the established channel, such as to provide finer granularity for particular drives within a tape library. As indicated, the use of this package of materials takes place during two phases: first during the establishment of the TLS secure channel; second during the transmission of KMIP messages. The server administrator must have configured the server to recognize the X.509 certificate presented by the client, to present the correct X.509 certificate of its own to the client in return and to recognize the additional information provided in the credential object in the KMIP message, if any.

In this model, KMIP is not used to transmit the X.509 certificate and server information used in establishing the secure channel. There is nothing to prevent KMIP being used to send this information; but commonly this is done using mechanisms other than KMIP, nor is there any expectation that KMIP is a required or default mechanism for propagating the credential and the information. The distribution mechanism, therefore, may well vary across vendors.

The use of additional information as the credential in the KMIP message is also neither required nor a default. Inclusion of such a credential in the package distributed to the client administrator and in one or more KMIP messages is also, therefore, likely to vary across vendors.

* 1. Automated Client Registration

The use case in section 7.2 of the KMIP Use Cases document that the credential used to establish a mutually-authenticated TLS connection is not provided in the package provided by the server administrator. Instead, the establishment of trust between the client and server is accomplished by some other mechanism.In one common version of this approach, an X.509 certificate that has been installed in a client device during the manufacturing process. This certificate is then used as a bootstrap mechanism for the subsequent exchange of the kind of information exchanged between client administrator and server administrator in section 1.1.

As described in this use case (see KMIP Use Case section 7.2), there will be typically be configuration activity for the client device based on information, such as a Service ID, received from the server administrator. Once the client administrator initiates auto-registration, the client device sends the X.509 certificate to the server, for example in order to use it to establish an initial TLS session. The server then sends the equivalent of the registration packet in section 1.1 above to the client and the client returns the certificate to be used for establishing the secure TLS channel with the server.

In this model, one common variant is to require administrator intervention to determine whether the initial client certificate should be accepted. The scenario above assumes that the return of the server’s packet of registration is immediate and automatic; alternatively, the return of the packet of information may be done manually by the server administrator, as in section 1.1 above; or the return of the packet of server information may be done by the server, but only after that action has been approved by an administrator.

As discussed in section 1.1, KMIP can be used by the client in sending the X.509 certificates to the server. However, this is not required and is currently not typical. If it is sent to the server using a KMIP register operation, the server must be able to distinguish that this operation is intended not only to register the cryptographic object, but also to initiate the registration of the client as a legitimate participant in KMIP message exchange.

* 1. Registering Sub-Clients Based on a Trusted Primary Client

The third use case described in the KMIP Use Cases document contains additional information about setting up the KMIP server to participate in automatic client registration described in section 1.2, particularly in terms of the distribution of the service ID for the server.

Although not described in this use case, it does point to a third common model for registering sub-clients of a trusted client. In this model, the establishment of trust between the client and server can be accomplished using either of the approaches in section 1.1 or 1.2. However, the server may also send additional information to the client, such as a “tenant identifier”, which it will have to provide to sub-clients for them to use they attempt to register individually. The individual sub-clients would follow a registration model such as that described in section 1.2, but would also provide the tenant identifier along with the X.509 certificate so that the server can decide whether to accept the client, based on such criteria as the TCP/IP address of the sub-client relative to that of the primary client.

This approach is common for tiered clients such as virtual machines that need to be grouped based on their association with a larger trusted entity, but that also need individual identities and trust relationships established based on those identities.

KMIP can be used for sending both the client certificate and the tenant identifier to the server. But again this is no currently common practice.