RSA Client Profile

Scope: Token that supports signing, certificate and basic private key storage.

-Assumptions: Key generation and certification is complete. Unique non-null CKA and ID values exist have proper associations. Key/Certificate pair has appropriate signing permissions.

-Private key is a private object. Private object requires CHV for use. Client Authentication Certificate is a public object.

-Location of intermediate certificates is undefined by the profile.

Mechanisms:

CKA_RSA_PKCS must be supported.

Key Size:

The key sizes that may be supported are: 512, 768, 1024 and 2048.
The application must support each of these.

Additional APIs: (Base API's implied)

C_SignInit, C_Sign (Length is restricted by the mechanism, No OID applied), C_Login (App cannot depend on logging in as SO, User Login must be supported), C_Logout

Sessions:

Single read only serial session is a minimum.

Threading:

Base library locking is negotiable.