A Profile of PKCS #11 for Mobile Devices

DRAFT

Magnus Nystrom

RSA Security Inc

ABSTRACT

This memo presents a proposal for a profile of PKCS #11 suitable for mobile devices.

$Id: pkcs-11-profile-proposal.m,v 1.1 2002/10/02 14:36:20 mnystrom Exp $

1. Objectives

In an environment, which:

- increasingly is security-aware,
- to a high degree relies on cryptographic tokens for security, and
- has a characteristics of being highly heterogenous,

PKCS #11 [PKCS11] is a good candidate for a well-known, ubiquitous interface to cryptographic tokens. When the environment also is constrained, however, the size and flexibility of PKCS #11 may complicate its use. This discussion paper therefore suggests a profile of PKCS #11 suitable for mobile devices with the above characteristics.

2. Profile

The profile is based on the "Large Application Profile" in [PKCS11Conf]. Some modifications has been done, however, in an attempt to meet the needs of mobile devices.

2.1 SupportedMechanisms

- CKM_RSA_KEY_PAIR_GEN
- CKM_RSA_PKCS
- CKM_RSA_X509 (MUST support at least 1024-bit keys).
- CKM_MD5_RSA_PKCS
- CKM_SHA1_RSA_PKCS
- CKM_SHA_1
- CKM_SHA_1_HMAC
- CKM_CMS_SIG [PKCS11Amd1]
- CKM_SHA1
- CKM_MD5
- A selection of symmetric mechanisms - RC4, 3DES, RC5 (?), AES, and - possibly - TLS/SSL mechanisms (not used frequently by browsers).

2.2 Attributes:

- All attributes needed for the above mechanisms to work must be supported.

  <<Probably need detailing>>

2.3 Functions

Note: This is in addition to the "basic" functions in [PKCS11Conf].

- C_GetFunctionList

  Note: The value of this function has been debated a lot in the cryptoki mailing list. (Rough) consensus seems to be to, for the moment, to keep it.

- C_SetPIN
- C_GetSessionInfo
- C_Login

  Note: Must support for both CKU_USER and CKU_SO.
- C_Logout
- C_CreateObject
- C_DestroyObject
- C_GetAttributeValue
- C_SetAttributeValue
- C_FindObjectsInit
- C_FindObjects
- C_FindObjectsFinal
- C_SignInit
- C_Sign
- C_VerifyInit
- C_Verify
- C_Encrypt
- C_EncryptInit
- C_DecryptInit
- C_Decrypt
- C_GenerateKeyPair
- C_Unwrap
- C_SeedRandom

  Note: This function is not in the Large Application Profile in [PKCS11Conf]. It is believed, however, to have its use in mobile clients.
- C_GenerateRandom

  Note: See note for C_SeedRandom.

2.4 Sessions

A PKCS #11 implementation conformant with this profile must support one R/W and at least ten simultaneous R/O sessions.

2.5 TemplateRequirements

- C_CreateObject: RSA Public Key, RSA Private Key, Certificate (X.509), Data.
- Private key templates: Application must be able to set TOKEN to TRUE.
- Public key templates: PRIVATE must be possible to set to FALSE.
- Certificate templates: The application must set be able to set TOKEN to TRUE.

— Data templates: TOKEN must be supported for both settings. PRIVATE must be supported for both settings.

— C_SetAttributeValue: Applications must be allowed to change the label of an object after creation. Applications must not expect to be able to set attribute values after creation unless explicitly indicated.

3. Discussion

A few of the open issues...

— It can be discussed whether a compound cryptoki call, like a call which finds the slot and token, initiates a session and logs the user in, would make sense, especially on tokens that only can contain one slot, and one token in that slot.

— Whether to include also SSL/TLS/WTLS mechanisms.

— Level of detail regarding supported attributes.

— Thread option?

4. References

[PKCS11] RSA Laboratories, "PKCS #11 v2.11: Cryptographic Token Interface Standard," v2.11 Rev. 1, November 2001.

[PKCS11Amd1] RSA Laboratories, "PKCS #11 v2.11 Amendment 1," August 2002.

[PKCS11Conf] RSA Laboratories, "PKCS #11 Conformance Profile Specification," October 2000.