The profile of PKCS #11 v2.11 for mobile devices

Magnus Nyström

PKCS Workshop April 2003

Objectives

- Motivation, relation to earlier work, etc. was done at the October 2002 workshop in Paris, France
  - Presentation available from http://www.rsasecurity.com/rsalabs/pkcs/workshop/02workshop.html
- This segment to focus on the current draft
  - Intent is to highlight any issues before submitting a final version

Draft 3 – Highlights

- Contains two profiles
  - Signature device profile
  - Communication device profile
- Contains some common requirements
  - Session support (one r/w, ten r/o simultaneously)
  - Thread handling (option 4) from PKCS #11 v2.11)

Signature device profile

- Object classes
  - (X.509) Certificate, (RSA) private key, (RSA) public key
- Attributes
  - Matrix listing objects and associated supported attributes
  - In principle, all attributes for the given objects need to be supported (not CKA_DERIVE, CKA_START_DATE, CKA_END_DATE, CKA_WRAP, CKA_UNWRAP, CKA_ENCRYPT, CKA_VERIFY_RECOVER, CKA_DECRYPT, CKA_SIGN_RECOVER)
- Mechanisms
  - CKM_RSA_KEY_PAIR_GEN
  - CKM_RSA_PKCS
  - CKM_MD5_RSA_PKCS
  - CKM_SHA1_RSA_PKCS
  - CKM_SHA_1
  - CKM_MD5

Signature device profile, continued

- Functions
  - All functions in the “Base API” in existing conformance document
  - In addition, `C_SetPIN`, `C_GetSessionInfo`,`C_Login`,`C_Logout`,`C_CreateObject`, `C_DestroyObject`,`C_SetAttributeValue`, `C_DigestInit`, `C_Digest`, `C_SignInit`, `C_Sign`, `C_VerifyInit`, `C_Verify`, `C_GenerateKeyPair`, `C_SeedRandom`, `C_GenerateRandom`

Communication device profile

- Object classes
  - (X.509) Certificate, (RSA) private key, (RSA) public key, (RC4 or 3DES) secret key
- Attributes
  - Matrix listing objects and associated supported attributes
  - In principle, all attributes for the given objects need to be supported (not CKA_START_DATE, CKA_END_DATE, CKA_VERIFY_RECOVER, CKA_SIGN_RECOVER)
- Mechanisms
  - `CKM_RSA_KEY_PAIR_GEN`,`CKM_RSA_PKCS`,`CKM_MD5_RSA_PKCS`, `CKM_SHA1_RSA_PKCS`,`CKM_SHA_1`,`CKM_MD5`,`CKM_SHA_1_HMAC`, `CKM_RC4` *or* `CKM_3DES_CBC`, and all `CKM_SSL3_*` and `CKM_TLS_*` mechanisms

Communication device profile, continued

- Functions
  - Same as for signature device profile + encrypt/decrypt and wrap/unwrap

Open issues

- None, to my knowledge
- Remaining to be done
  - Editorial corrections (Laszlo has pointed out some errors)
  - Publish final draft (next week)
    - Two week review period
- Others?