PKCS #11 v2.11 Changes

Included in Draft 1

Functional

- ✓ Deprecate secondary authentication
  - ✓ Add appendix to use the iD2 multiple slot method as informative [Magnus; included]
- ✓ Add note about write-protect flag changing with login to allow public objects to be read-only without login
- ✓ PIN expiration
  - ✓ If PIN expires, CKF_USER_PIN_TO_BE_CHANGED is set, allow login and all functions that require login return CKR_PIN_EXPIRED until C_SetPIN is called. C_Login will *never* return CKR_PIN_EXPIRED.
  - ✓ Allow C_SetPIN to work without login (always changes user PIN)
- ✓ Trusted objects (keys, certs) CKA_TRUSTED; never settable by caller, must be set by initialization; ***settable by SO during C_CreateObject (open for discussion)?***
- ✓ Misc. typo fixes.

Algorithms

- ✓ AES mechanisms, RIJNDAEL, CKM_AES w/modes (variable block size 16, 24, 32; variable key length 128, 192, 256)
- ✓ X9.31 RSA w/related combos

Included in Draft 2

Functional

- ✓ Updated references
- ✓ Many misc. typo fixes.

Algorithms

- ✓ X9.31 RSA key pair generation
- ✓ ECC X9.62-3 mechanisms [Francois]
- ✓ X9.42 mechanisms [Francois]
- ✓ Parameter generation and validation. New explicit objects and mechanisms. [Simon]
- ✓ AES mechanism; updated w/o variable block size

Not Included in Draft 2

Algorithms

- SHA-256, -384, -512 and related combos
  - Deferred: Draft specification not scheduled until ‘Q2 FY01
- RSA PKCS #1 PSS & multi-prime [Burt]

- TLS mechanisms
- IPSEC transforms