Resolved V2.40 items

First drafts of V2.40 docs posted to repository (Base/Current/Historical spec; Usage Guide; Profile; Conformance Clause; header files)

ulPasswordLength datatype. Resolved via straw poll ballot 10-May.

V2.40 items under discussion

Secure key import (Doron). Updated proposal posted 27-May)

AES modes (Valerie/BobR). Discussion on reflector; need proposal (2-May)

CKA_GLOBAL, CKM_CERTIFY_KEY and CKM_SEAL_KEY (MikeS): on reflector, updated 15-May

CKD_SHA*_KDF (MikeS): Raised on reflector (28-May). Not yet proposal.

CKA_PUBLIC_KEY_INFO (MikeS): proposal on reflector updated 28-May

Define constants for (CK_ULONG)-1 (CK_INVALID_LENGTH) (StefW/MikeS): last update 14-May on reflector

CKA_CERTIFICATE_CATEGORY constants (StefW): on reflector, updated 28-May

CKA_JAVA_MIDP_SECURITY_DOMAIN constants (StefW): on reflector 27-May

Close sessions with regards to multiple callers (StefW): on reflector 27-May

New CKA_DESTROYABLE attribute (StefW): proposed on reflector 27-May

All constants should have UL suffix (StefW): proposed on reflector 27-May

Remove restrictions on R/O sessions with CKU_SO (StefW): proposed on reflector 27-May

Use CK_UNAVAILABLE_INFORMATION with C_GetAttributeValue (StefW): proposed on reflector 27-May

C_ChangeLabel/C_ClearToken (Dina). Raised on reflector (9-May). Not yet proposal

Extraction attacks (ChrisD), raised on wiki, 19-Apr). Not yet proposal

Public/private key (PeterG): raised on wiki (2-Apr). Not yet proposal.

Common bugs (PeterG): raised on wiki (8-Mar). Not yet proposal.

Deferred, dropped and/or inactive V2.40 items (AI brought forward from F2F)

MikeS: Clarifying CK_ULONG and 64 bit lengths for C_Encrypt, C_Decrypt (updated 28-May)

Provisioning Tokens with PKCS #11 (Anders Rundgren): (on comment list 22-May)

AI: Tim: proposal for extensions process, function tables etc (4 weeks)

AI: Peter, Tim, BobR, Stef: identify ambiguities/inconsistencies in current

AI: Peter: go through list and identify near-term guidance or enhancements (2 weeks)

AI: Stef : identify any near-term issues in spec (2 weeks)

AI: Chris: identify any near-term issues with error reporting / response (2 weeks?)

AI: Doron: Bring forward discussion of secure key import (4 weeks)

AI: Brian: bring the TLS mechanisms (potentially others as well) forward (2 weeks)

AI: Brian: constant time HMAC modules: consider whether to bring this forward (4 weeks)

AI: Tim/Lawrence: look at bringing near-term profiles forward, such as symmetric key usage (4 weeks)

AI: Rayees: review the TPM mechanism in v2.30 (2 weeks)

AI: Dina: bring forward in passphrase-based encryption issues/fixes (2 weeks)

AI: Rob: talk to RSA folks and bring forward any issues (2 weeks)

AI: Andrey/Stef/Valerie: bring forward comment/ suggestion on module discovery etc (4 weeks)

AI: Lawrence Lee: In the next four weeks discuss with Tim H. and return feedback to the TC. (profiles for mobile phones)

AI: Dina: bring forward in passphrase-based encryption issues/fixes (2 weeks)

AI: Valerie: look into whether test farm / accounts is available

AI: build/use conformant implementation?

AI: Sven/MikeS/BobR: mini-driver for PKCS #11

AI: BobG: email to request participants in small group working on extensions (process, api, mining, etc)

AI: BobG: coordinate setting up smaller group to look into promoting wide-spread adoption of PKCS #11

AI: BobG; send around Statement of Use information from OASIS process

AI: BobG to look into members common between web crypto and PKCS 11 TC.

AI: Peter G., Tim H., Robert R., GilA, AndreyJ: look into what to do with CKA_ID; come back to the TC. In 2 weeks/

AI: ? BoF at Usenix?