ERICSSON

PKCS#11 amendments for WTLS and TLS PRF

Changes since last version of draft:

- New values for CKA_CERTIFICATE_CATEGORY: {token user, authority, other entity, unspecified}. May not be modified after the object is created.
- The old attribute CKA_CertificateURL, that indicated if CKA_VALUE was the actual certificate of a URL, is removed. CKA_VALUE will always contain the certificate if available. CKA_URL is added that is used to store the URL. Due to this CKA_SUBJECT and CKA_VALUE (must be specified when the object is created) are allowed to be empty if the CKA_URL attribute is non-empty.

Ben Smeets, Matthias Esswein, and Per Ståhl

ERICSSON

PKCS#11 amendments cnt'd

- CKA_HASH_OF_ISSUER_PUBLIC_KEY attribute added and CKA_HASH_OF_PUBLIC_KEY attribute renamed to CKA_HASH_OF_SUBJECT_PUBLIC_KEY. They are used to correlate the certificate with private keys and issuer certificates when only the URL is available and can only be empty if CKA_URL is empty.
- CKA_CERTIFICATE_DOMAIN renamed to CKA_JAVA_MIDP_SECURITY_DOMAIN. May not be modified after the object is created.

ERICSSON

Remaining to be done (Slide written by Magnus)

- Assignment of values
  - New object type (WTLS certificate)
  - New mechanisms
  - New attributes
- Inclusion in v2.20
- Suggest doing the assignment on the mailing list and then handover to Simon for inclusion in v2.20