PKCS#11 Items from v3.0 Review

Items found comparing the Current Mechanisms and Header File

| **#** | **Issue** | **Suggestion/Resolution** | **Owner** |
| --- | --- | --- | --- |
| 1 | CKM\_DSA\_FIPS\_G\_GEN (section 2.2), CKM\_EC\_KEY\_PAIR\_GEN\_W\_EXTRA\_BITS (section 2.3), CKM\_SALSA20\_KEY\_GEN (section 2.59) is missing in header. | Review Header file | Bob R |
| 2 | CKM\_TLS10\_MAC\_CLIENT and CKM\_TLS10\_MAC\_SERVER are still contained in the header file, but it was removed from the mech doc in WD10. | Removed from header file (but keep identifier) | Bob R |
| 3 | Also CKM\_TLS\_PRE\_MASTER\_KEY\_GEN is in the header file, but not described in the mech doc. | Double check header file for status and update mech document to suit | Bob R/Dieter |
| 4 | In section 2.1.19 (PKCS #1 RSA PSS signature with SHA3) CKM\_SHA3\_xxx\_RSA\_PSS should be renamed to CKM\_SHA3\_xxx\_RSA\_PKCS\_PSS (already defined, so just a typo). The same is true for CKM\_SHAX\_RSA\_PSS in section 2.1.16. | **Amend mechanisms document to include “PKCS”** | Dieter B **Complete** |
| 5 | CKM\_SHA1 in section 2.2 (possible value of CK\_DSA\_PARAMETER\_GEN\_PARAM's hash field) should be CKM\_SHA\_1 (just a typo). | **Amend to read CKM\_SHA\_1** | Dieter B **Complete** |
| 6 | In section 2.2 and several subsections (DSA) CKM\_DSA\_PROBABALISTIC\_PARAMETER\_GEN should be CKM\_DSA\_PROBABLISTIC\_PARAMETER\_GEN. The former does not exist in the header. The latter is misspelled, but at least it exists. We could also introduce CKM\_DSA\_PROBABILISTIC\_PARAMETER\_GEN (and leave the old one for backwards compatibility) and change the spec overall. | Fix the header file to use correct English spelling and leave an alias in the header file to retain existing spelling also **Fix the mechanisms file to use correct English spelling** | Bob R  Dieter B **Complete** |
| 7 | In section 2.2.21 (DSA with SHA3-512) CKM\_DSA\_SHA3-512 should be CKM\_DSA\_SHA3\_512 (just a typo). | **Amend to read CKM\_DSA\_SHA3\_512** | Dieter B **Complete** |
| 8 | In section 2.3.14 (EdDSA) CKM\_TOKEN\_RESOURCE\_EXCEEDED should be CKR\_TOKEN\_RESOURCE\_EXCEEDED (it's an error code, not a mechanism). | **Amend to read CKR\_TOKEN\_RESOURCE\_EXCEEDED** | Dieter B **Complete** |
| 9 | The paragraph before 2.3.15 (XEdDSA) seems to be part of the heading. At least, it appears in the TOC of the HTML version. | **Correct formatting issue** | Dieter B **Complete** |
| 10 | Table 53 in section 2.4 () contains CKM\_X9\_42\_DH\_PKCS\_PARAMETER\_GEN (also appendix B.4), which is not explained and not in the header file. Remove? | **Amend entry in table and reformat table and appendix to match.** | Dieter B **Complete** |
| 11 | In 2.5 (Extended Triple Diffie-Hellman (x3dh)) mechanism is called CKM\_X3DH\_INITIATE, but CKM\_X3DH\_INITIALIZE in header. It should be INITIALIZE as for Double Ratchet. | **Confirm to match INITIALIZE in the header File** | Dieter B **Complete** |
| 12 | In section 2.6 (Double Ratchet) CKM\_X2RATCHET\_INITALIZE should be CKM\_X2RATCHET\_INITIALIZE (just a typo). | **Correct typo to read CKM\_X2RATCHET\_INITIALIZE** | Dieter B **Complete** |
| 13 | In section 2.6.3 (Double Ratchet key derivation) descriptions of field aeadMechanism contain reference to CKM\_XCHACHA20 as example, which does not exist. Remove example? | **Remove example** | Dieter B **Complete** |
| 14 | In section 2.15.1 (part of AES XTS) CKM\_AES\_CTS\_KEY\_GEN should be CKM\_AES\_XTS\_KEY\_GEN. The former does not exist. | **Amend to read CKM\_AES\_XTS\_KEY\_GEN – also update appendix B.4** | Dieter B **Complete** |
| 15 | The header file values CKM\_SHA3\_xxx\_KEY\_DERIVE should be renamed to CKM\_SHA3\_xxx\_KEY\_DERIVATION of sections 2.28 to 2.31 (SHA3-xxx). This is also consistent with the SHA-2 mechanisms. | Add alias to header file to match Mechanisms | Bob R |
| 16 | The header file values CKM\_SHAKE\_xxx\_KEY\_DERIVE should be renamed to CKM\_SHAKE\_xxx\_KEY\_DERIVATION of section 2.32 (SHAKE). | Add alias to header file to match Mechanisms | Bob R |
| 17 | Table 162 in section 2.42.2 (part of SP 800-108 Key Derivation) contains CKM\_3DES\_CMAC, which does not exist. It should probably be CKM\_DES3\_CMAC. | **Amend Mechanisms file to reflect the header file should be CKM\_DES3\_CMAC** | Dieter B **Complete** |
| 18 | Examples in sections 2.42.8.1 to 2.42.8.4 contain CKM\_FLEXIBLE\_KDF. This should be 2x CKM\_SP800\_108\_COUNTER\_KDF, CKM\_SP800\_108\_FEEDBACK\_KDF and CKM\_SP800\_108\_DOUBLE\_PIPELINE\_KDF. | **Amend mechanisms to use CKM\_SP800\_108\_COUNTER\_KDF, CKM\_SP800\_108\_FEEDBACK\_KDF and CKM\_SP800\_108\_DOUBLE\_PIPELINE\_KDF** | Dieter B **Complete** |
| 19 | Table 212 in section 2.57 (GOST R 34.10-2001) contains CKM\_GOSTR3410\_WITH\_GOST3411, which should be CKM\_GOSTR3410\_WITH\_GOSTR3411 (just a typo). | **Amend mechanisms to include KM\_GOSTR3410\_WITH\_GOSTR3411** | Dieter B **Complete** |
| 20 | In section 2.60.1 (part of Poly1305) CKM\_POLY1305\_MAC should be CKM\_POLY1305. The former does not exist. | **Amend mechanisms to include CKM\_POLY1305** | Dieter B **Complete** |
| 21 | "Mechanisms vs Functions" table is missing in 2.61 (Chacha20/Poly1305 and Salsa20/Poly1305 Authenticated Encryption / Decryption) | **Amend mechanisms to include table** | Dieter B **Complete** |
| 22 | In section 2.62.5 (HKDF Key gen) CKM\_HKDF\_KEYGEN should be CKM\_HKDF\_KEY\_GEN (just a typo) | **Amend to read CKM\_HKDF\_ KEY\_GEN** | Dieter B **Complete** |
| 23 | CK\_GCM\_Params & missing ulIvBits | Include some guidance text on wiki to describe Header file vs specification | Tim H & Bob R |