HMAC-SHA-2 Pseudorandom Functions for PBKDF2

Wan-Teh Chang <wtc@google.com>, 2014-02-19

Introduction

This proposal adds six HMAC-SHA-2 pseudorandom functions for PBKDF2, the first four specified in PKCS #5 v2.1.

PKCS #11 Current Mechanisms Specification Version 2.40, Section 2.29.3 “PKCS #5 PBKDF2 key generation mechanism parameters” specifies the pseudorandom function type CK_PKCS5_PBKD2_PSEUDO_RANDOM_FUNCTION_TYPE in Table 99. The type currently has two PRF identifiers defined: CKP_PKCS5_PBKD2_HMAC_SHA1 (0x00000001UL) and CKP_PKCS5_PBKD2_HMAC_GOSTR3411 (0x00000002UL).

Proposed Changes

This proposal adds the following six PRF identifiers to Table 99:

Table 99, PKCS #5 PBKDF2 Key Generation: Pseudo-random functions

PRF Identifier	Value	Parameter Type
...	...	...
CKP_PKCS5_PBKD2_HMAC_SHA224	0x00000003UL	No Parameter. *pPrfData* must be NULL and *ulPrfDataLen* must be zero.
CKP_PKCS5_PBKD2_HMAC_SHA256	0x00000004UL	No Parameter. *pPrfData* must be NULL and *ulPrfDataLen* must be zero.
CKP_PKCS5_PBKD2_HMAC_SHA384	0x00000005UL	No Parameter. *pPrfData* must be NULL and *ulPrfDataLen* must be zero.
CKP_PKCS5_PBKD2_HMAC_SHA512	0x00000006UL	No Parameter. *pPrfData* must be NULL and *ulPrfDataLen* must be zero.
CKP_PKCS5_PBKD2_HMAC_SHA512_224	0x00000007UL	No Parameter. *pPrfData* must be NULL and *ulPrfDataLen* must be zero.

CKP_PKCS5_PBKD2_HMAC_SHA512_256	0x00000008UL	No Parameter. *pPrfData* must be NULL and *ulPrfDataLen* must be zero.

In addition, the sentence “The following PRFs are defined in PKCS #5 v2.0.” should be changed to “**The following PRFs are defined in PKCS #5 v2.1.**” The sentence “The following salt value sources are defined in PKCS #5 v2.0.” should be changed to “**The following salt value sources are defined in PKCS #5 v2.1.**”