1.1 SHA-512/224

Mechanism	Functions						
	Encrypt & Decrypt	Sign & Verify	SR & VR[1]	Digest	Gen. Key / Key Pair	Wrap & Unwrap	Derive
CKM_SHA512_224				✓			
CKM_SHA512_224_HMAC_GENERAL		✓					
CKM_SHA512_224_HMAC		✓					
CKM_SHA512_224_KEY_DERIVATION							✓

1.1.1 Definitions

CKM_SHA512_224
CKM_SHA512_224_HMAC
CKM_SHA512_224_HMAC_GENERAL
CKM_SHA512_224_KEY_DERIVATION

CKK_SHA512_224_HMAC

1.1.2 SHA-512/224 digest

The SHA-512/224 mechanism, denoted **CKM_SHA512_224**, is a mechanism for message digesting, following the Secure Hash Algorithm with a 512-bit message digest truncated to 224 bits defined in FIPS PUB 180-4.

It does not have a parameter.

Constraints on the length of input and output data are summarized in the following table. For single-part digesting, the data and the digest may begin at the same location in memory.

Table 1, SHA-512/224: Data Length

Function	Input length	Digest length
C_Digest	any	28

1.1.3 General-length SHA-512/224-HMAC

The general-length SHA-512/224-HMAC mechanism, denoted **CKM_SHA512_224_HMAC_GENERAL**, is the same as the general-length SHA-1-HMAC mechanism in Section Error: Reference source not found, except that it uses the HMAC construction based on the SHA-512/224 hash function and length of the output should be in the range 0-28.

1.1.4 SHA-512/224-HMAC

The SHA-512/224-HMAC mechanism, denoted **CKM_SHA512_224_HMAC**, is a special case of the general-length SHA-512/224-HMAC mechanism.

It has no parameter, and always produces an output of length 28.

1.1.5 SHA-512/224 key derivation

SHA-512/224 key derivation, denoted **CKM_SHA512_224_KEY_DERIVATION**, is the same as the SHA-1 key derivation mechanism in Section Error: Reference source not found, except that it uses the SHA-512/224 hash function and the relevant length is 28 bytes.

1.2 SHA-512/256

Mechanism	Functions						
	Encrypt & Decrypt	Sign & Verify	SR & VR[1]	Digest	Gen. Key / Key Pair	Wrap & Unwrap	Derive
CKM_SHA512_256				✓			
CKM_SHA512_256_HMAC_GENERAL		✓					
CKM_SHA512_256_HMAC		✓					
CKM_SHA512_256_KEY_DERIVATION							✓

1.2.1 Definitions

CKM_SHA512_256

CKM_SHA512_256_HMAC

CKM_SHA512_256_HMAC_GENERAL

CKM_SHA512_256_KEY_DERIVATION

CKK_SHA512_256_HMAC

1.2.2 SHA-512/256 digest

The SHA-512/224 mechanism, denoted **CKM_SHA512_256**, is a mechanism for message digesting, following the Secure Hash Algorithm with a 512-bit message digest truncated to 256 bits defined in FIPS PUB 180-4.

It does not have a parameter.

Constraints on the length of input and output data are summarized in the following table. For single-part digesting, the data and the digest may begin at the same location in memory.

Table 2, SHA-512/256: Data Length

Function	Input length	Digest length
C_Digest	any	32

1.2.3 General-length SHA-512/256-HMAC

The general-length SHA-512/256-HMAC mechanism, denoted **CKM_SHA512_256_HMAC_GENERAL**, is the same as the general-length SHA-1-HMAC mechanism in Section Error: Reference source not found, except that it uses the HMAC construction based on the SHA-512/256 hash function and length of the output should be in the range 0-32.

1.2.4 SHA-512/256-HMAC

The SHA-512/256-HMAC mechanism, denoted **CKM_SHA512_256_HMAC**, is a special case of the general-length SHA-512/256-HMAC mechanism.

It has no parameter, and always produces an output of length 32.

1.2.5 SHA-512/256 key derivation

SHA-512/256 key derivation, denoted **CKM_SHA512_256_KEY_DERIVATION**, is the same as the SHA-1 key derivation mechanism in Section Error: Reference source not found, except that it uses the SHA-512/256 hash function and the relevant length is 32 bytes.

1.3 General SHA-512/t

Mechanism	**Functions**						
	Encrypt & Decrypt	**Sign & Verify**	**SR & VR**[1]	**Digest**	**Gen. Key / Key Pair**	**Wrap & Unwrap**	**Derive**
CKM_SHA512_T				✓			
CKM_SHA512_T_HMAC_GENERAL		✓					
CKM_SHA512_T_HMAC		✓					
CKM_SHA512_T_KEY_DERIVATION							✓

1.3.1 Definitions

CKM_SHA512_T
CKM_SHA512_T_HMAC
CKM_SHA512_T_HMAC_GENERAL
CKM_SHA512_T_KEY_DERIVATION

CKK_SHA512_T_HMAC

1.3.2 SHA-512/t digest

The SHA-512/t mechanism, denoted **CKM_SHA512_T**, is a mechanism for message digesting, following the Secure Hash Algorithm with a 512-bit message digest truncated to t bits defined in FIPS PUB 180-4.

It has a parameter, a **CK_MAC_GENERAL_PARAMS**, which holds the length in bytes of the desired output. This length should be in the range 0-(t/8), where 0 < t < 512, t <> 384.

Constraints on the length of input and output data are summarized in the following table. For single-part digesting, the data and the digest may begin at the same location in memory.

Table 3, SHA-512/t: Data Length

Function	**Input length**	**Digest length**
C_Digest	any	t/8, where 0 < t < 512, t <> 384

1.3.3 General-length SHA-512/t-HMAC

The general-length SHA-512/t-HMAC mechanism, denoted **CKM_SHA512_T_HMAC_GENERAL**, is the same as the general-length SHA-1-HMAC mechanism in Section Error: Reference source not found, except that it uses the HMAC construction based on the SHA-512/t hash function and length of the output should be in the range 0-(t/8), where 0 < t < 512, t <> 384.

1.3.4 SHA-512/t-HMAC

The SHA-512/t-HMAC mechanism, denoted **CKM_SHA512_T_HMAC**, is a special case of the general-length SHA-512/t-HMAC mechanism.

It has a parameter, a **CK_MAC_GENERAL_PARAMS**, which holds the length in bytes of the desired output. This length should be in the range 0-(t/8), where 0 < t < 512, t <> 384.

1.3.5 SHA-512/t key derivation

SHA-512/256 key derivation, denoted **CKM_SHA512_T_KEY_DERIVATION**, is the same as the SHA-1 key derivation mechanism in Section Error: Reference source not found, except that it uses the SHA-512/t hash function and the relevant length is t/8 bytes, where 0 < t < 512, t <> 384.

2 Manifest Constants

The following definitions can be found in the appropriate header file.

Also, refer [PKCS #11-Base] for additional definitions.

```
   #define CKK_SHA512_224_HMAC               0x00000033
   #define CKK_SHA512_256_HMAC               0x00000034
   #define CKK_SHA512_T_HMAC                 0x00000035

   #define CKM_SHA512_224                    0x00000280
   #define CKM_SHA512_224_HMAC               0x00000281
   #define CKM_SHA512_224_HMAC_GENERAL       0x00000282
   #define CKM_SHA512_256                    0x00000290
   #define CKM_SHA512_256_HMAC               0x00000291
   #define CKM_SHA512_256_HMAC_GENERAL       0x00000292
   #define CKM_SHA512_T                      0x000002A0
   #define CKM_SHA512_T_HMAC                 0x000002A1
   #define CKM_SHA512_T_HMAC_GENERAL         0x000002A2
```