## PKCS #5 and PKCS #5-style password-based encryption (PBE)

The mechanisms in this section are for generating keys and IVs for performing password-based encryption. The method used to generate keys and IVs is specified in PKCS #5.

|  | **Functions** |
| --- | --- |
| **Mechanism** | **Encrypt****&****Decrypt** | **Sign****&****Verify** | **SR****&****VR**1 | **Digest** | **Gen.** **Key/****Key****Pair** | **Wrap****&****Unwrap** | **Derive** |
| CKM\_PBE\_SHA1\_DES3\_EDE\_CBC |  |  |  |  | ✓ |  |  |
| CKM\_PBE\_SHA1\_DES2\_EDE\_CBC |  |  |  |  | ✓ |  |  |
| CKM\_PBA\_SHA1\_WITH\_SHA1\_HMAC |  |  |  |  | ✓ |  |  |
| CKM\_PKCS5\_PBKD2 |  |  |  |  | ✓ |  |  |
| CKM\_PKCS5\_PBKD2\_FIX |  |  |  |  | ✓ |  |  |

### Definitions

Mechanisms:

CKM\_PBE\_SHA1\_DES3\_EDE\_CBC

CKM\_PBE\_SHA1\_DES2\_EDE\_CBC

CKM\_PKCS5\_PBKD2

CKM\_PKCS5\_PBKD2\_FIX

CKM\_PBA\_SHA1\_WITH\_SHA1\_HMAC

### Password-based encryption/authentication mechanism parameters

1. CK\_PBE\_PARAMS; CK\_PBE\_PARAMS\_PTR

**CK\_PBE\_PARAMS** is a structure which provides all of the necessary information required by the CKM\_PBE mechanisms (see PKCS #5 and PKCS #12 for information on the PBE generation mechanisms) and the CKM\_PBA\_SHA1\_WITH\_SHA1\_HMAC mechanism. It is defined as follows:

typedef struct CK\_PBE\_PARAMS {

 CK\_BYTE\_PTR pInitVector;

 CK\_UTF8CHAR\_PTR pPassword;

 CK\_ULONG ulPasswordLen;

 CK\_BYTE\_PTR pSalt;

 CK\_ULONG ulSaltLen;

 CK\_ULONG ulIteration;

} CK\_PBE\_PARAMS;

The fields of the structure have the following meanings:

 *pInitVector* pointer to the location that receives the 8-byte initialization vector (IV), if an IV is required;

 *pPassword* points to the password to be used in the PBE key generation;

 *ulPasswordLen* length in bytes of the password information;

 *pSalt* points to the salt to be used in the PBE key generation;

 *ulSaltLen* length in bytes of the salt information;

 *ulIteration* number of iterations required for the generation.

**CK\_PBE\_PARAMS\_PTR** is a pointer to a **CK\_PBE\_PARAMS**.

### PKCS #5 PBKDF2 key generation mechanism parameters

1. CK\_PKCS5\_PBKD2\_PSEUDO\_RANDOM\_FUNCTION\_TYPE; CK\_PKCS5\_PBKD2\_PSEUDO\_RANDOM\_FUNCTION\_TYPE\_PTR

**CK\_PKCS5\_PBKD2\_PSEUDO\_RANDOM\_FUNCTION\_TYPE** is used to indicate the Pseudo-Random Function (PRF) used to generate key bits using PKCS #5 PBKDF2. It is defined as follows:

typedef CK\_ULONG CK\_PKCS5\_PBKD2\_PSEUDO\_RANDOM\_FUNCTION\_TYPE;

The following PRFs are defined in PKCS #5 v2.0. The following table lists the defined functions.

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

|  |  |  |
| --- | --- | --- |
| **PRF Identifier** | **Value** | **Parameter Type** |
| CKP\_PKCS5\_PBKD2\_HMAC\_SHA1 | 0x00000001 | No Parameter. *pPrfData* must be NULL and *ulPrfDataLen* must be zero. |
| CKP\_PKCS5\_PBKD2\_HMAC\_GOSTR3411 | 0x00000002 | This PRF uses GOST R34.11-94 hash to produce secret key value. *pPrfData* should point to DER-encoded OID, indicating GOSTR34.11-94 parameters. *ulPrfDataLen* holds encoded OID length in bytes. If *pPrfData* is set to NULL\_PTR, then *id-GostR3411-94-CryptoProParamSet* parameters will be used (RFC 4357, 11.2), and *ulPrfDataLen* must be 0. |

**CK\_PKCS5\_PBKD2\_PSEUDO\_RANDOM\_FUNCTION\_TYPE\_PTR** is a pointer to a **CK\_PKCS5\_PBKD2\_PSEUDO\_RANDOM\_FUNCTION\_TYPE**.

1. CK\_PKCS5\_PBKDF2\_SALT\_SOURCE\_TYPE; CK\_PKCS5\_PBKDF2\_SALT\_SOURCE\_TYPE\_PTR

**CK\_PKCS5\_PBKDF2\_SALT\_SOURCE\_TYPE** is used to indicate the source of the salt value when deriving a key using PKCS #5 PBKDF2. It is defined as follows:

typedef CK\_ULONG CK\_PKCS5\_PBKDF2\_SALT\_SOURCE\_TYPE;

The following salt value sources are defined in PKCS #5 v2.0. The following table lists the defined sources along with the corresponding data type for the *pSaltSourceData* field in the **CK\_PKCS5\_PBKD2\_PARAM** structure defined below.

Table , PKCS #5 PBKDF2 Key Generation: Salt sources

|  |  |  |
| --- | --- | --- |
| **Source Identifier** | **Value** | **Data Type** |
| CKZ\_SALT\_SPECIFIED | 0x00000001 | Array of CK\_BYTE containing the value of the salt value. |

**CK\_PKCS5\_PBKDF2\_SALT\_SOURCE\_TYPE\_PTR** is a pointer to a **CK\_PKCS5\_PBKDF2\_SALT\_SOURCE\_TYPE**.

1. CK\_ PKCS5\_PBKD2\_PARAMS; CK\_PKCS5\_PBKD2\_PARAMS\_PTR

**CK\_PKCS5\_PBKD2\_PARAMS** is a structure that provides the parameters to the **CKM\_PKCS5\_PBKD2** mechanism. The structure is defined as follows:

typedef struct CK\_PKCS5\_PBKD2\_PARAMS {

 CK\_PKCS5\_PBKDF2\_SALT\_SOURCE\_TYPE saltSource;

 CK\_VOID\_PTR pSaltSourceData;

 CK\_ULONG ulSaltSourceDataLen;

 CK\_ULONG iterations;

 CK\_PKCS5\_PBKD2\_PSEUDO\_RANDOM\_FUNCTION\_TYPE prf;

 CK\_VOID\_PTR pPrfData;

 CK\_ULONG ulPrfDataLen;

 CK\_UTF8CHAR\_PTR pPassword;

 CK\_ULONG\_PTR ulPasswordLen;

} CK\_PKCS5\_PBKD2\_PARAMS;

The fields of the structure have the following meanings:

 *saltSource* source of the salt value

 *pSaltSourceData* data used as the input for the salt source

 *ulSaltSourceDataLen* length of the salt source input

 *iterations* number of iterations to perform when generating each block of random data

 *prf* pseudo-random function to used to generate the key

 *pPrfData* data used as the input for PRF in addition to the salt value

 *ulPrfDataLen* length of the input data for the PRF

 *pPassword* points to the password to be used in the PBE key generation

 *ulPasswordLen* pointer to the length in bytes of the password information[[1]](#footnote-1)

**CK\_PKCS5\_PBKD2\_PARAMS**\_**PTR** is a pointer to a **CK\_PKCS5\_PBKD2\_PARAMS**.

1. CK\_ PKCS5\_PBKD2\_FIX\_PARAMS; CK\_PKCS5\_PBKD2\_FIX\_PARAMS\_PTR

**CK\_PKCS5\_PBKD2\_FIX\_PARAMS** is a structure that provides the parameters to the **CKM\_PKCS5\_PBKD2\_FIX** mechanism. The structure is defined as follows:

typedef struct CK\_PKCS5\_PBKD2\_PARAMS {

 CK\_PKCS5\_PBKDF2\_SALT\_SOURCE\_TYPE saltSource;

 CK\_VOID\_PTR pSaltSourceData;

 CK\_ULONG ulSaltSourceDataLen;

 CK\_ULONG iterations;

 CK\_PKCS5\_PBKD2\_PSEUDO\_RANDOM\_FUNCTION\_TYPE prf;

 CK\_VOID\_PTR pPrfData;

 CK\_ULONG ulPrfDataLen;

 CK\_UTF8CHAR\_PTR pPassword;

 CK\_ULONG ulPasswordLen;

} CK\_PKCS5\_PBKD2\_PARAMS;

The fields of the structure have the following meanings:

 *saltSource* source of the salt value

 *pSaltSourceData* data used as the input for the salt source

 *ulSaltSourceDataLen* length of the salt source input

 *iterations* number of iterations to perform when generating each block of random data

 *prf* pseudo-random function to used to generate the key

 *pPrfData* data used as the input for PRF in addition to the salt value

 *ulPrfDataLen* length of the input data for the PRF

 *pPassword* points to the password to be used in the PBE key generation

 *ulPasswordLen* length in bytes of the password information

**CK\_PKCS5\_PBKD2\_FIX\_PARAMS**\_**PTR** is a pointer to a **CK\_PKCS5\_PBKD2\_FIX\_PARAMS**.

### PKCS #5 PBKD2 key generation

PKCS #5 PBKDF2 key generation, denoted **CKM\_PKCS5\_PBKD2**, is a mechanism used for generating a secret key from a password and a salt value. This functionality is defined in PKCS#5 as PBKDF2.

It has a parameter, a **CK\_PKCS5\_PBKD2\_PARAMS** structure. The parameter specifies the salt value source, pseudo-random function, and iteration count used to generate the new key.

Since this mechanism can be used to generate any type of secret key, new key templates must contain the **CKA\_KEY\_TYPE** and **CKA\_VALUE\_LEN** attributes. If the key type has a fixed length the **CKA\_VALUE\_LEN** attribute may be omitted.

The mechanism **CK\_PKCS5\_PBKD2\_FIX** is the exact same mechanism as **CKM\_PKCS5\_PBKD2**, but uses **CK\_PKCS5\_PBKD2\_FIX\_PARAMS** structure as its parameter. This mechanism was added as of 2.40 to fix a typo in the definition of ulPasswordLen in **CK\_PKCS5\_PBKD2\_PARAMS.** It was mis-defined as **CK\_ULONG\_PTR**, and has been changed to **CK\_ULONG** in **CK\_PKCS5\_PBKD2\_FIX\_PARAMS**. **CKM\_PKCS5\_PBKD2** is deprecated as of 2.40.

1. The typing of this field as CK\_ULONG\_PTR was an error, and disagreed with the descriptive text for the field. The descriptive text has been updated to agree with the field type. A new mechanism (CKM\_PKCS5\_PBKD2\_FIX) and structure (CK\_PKCS5\_PBKD2\_FIX\_PARAMS) have been added as of 2.40 to fix the type error. [↑](#footnote-ref-1)