Rocky Enterprise Linux 9.2 Manual Pages on command 'PKCS5_PBKDF2_HMAC_SHA1.3ossl'

$ man PKCS5_PBKDF2_HMAC_SHA1.3ossl

PKCS5_PBKDF2_HMAC(3ossl) OpenSSL PKCS5_PBKDF2_HMAC(3ossl)

NAME

PKCS5_PBKDF2_HMAC, PKCS5_PBKDF2_HMAC_SHA1 - password based derivation routines with salt and iteration count

SYNOPSIS

```
#include <openssl/evp.h>

int PKCS5_PBKDF2_HMAC(const char *pass, int passlen,
                      const unsigned char *salt, int saltlen, int iter,
                      const EVP_MD *digest,
                      int keylen, unsigned char *out);

int PKCS5_PBKDF2_HMAC_SHA1(const char *pass, int passlen,
                           const unsigned char *salt, int saltlen, int iter,
                           int keylen, unsigned char *out);
```

DESCRIPTION

PKCS5_PBKDF2_HMAC() derives a key from a password using a salt and iteration count as specified in RFC 2898.

pass is the password used in the derivation of length passlen. pass is an optional parameter and can be NULL. If passlen is -1, then the function will calculate the length of pass using strlen().

salt is the salt used in the derivation of length saltlen. If the salt is NULL, then saltlen must be 0. The function will not attempt to calculate the length of the salt because it is not assumed to be NULL terminated.

iter is the iteration count and its value should be greater than or equal to 1. RFC 2898 suggests an iteration count of at least 1000. Any iter less than 1 is treated as a single iteration.

digest is the message digest function used in the derivation. PKCS5_PBKDF2_HMAC_SHA1() calls PKCS5_PBKDF2_HMAC() with EVP_sha1().

The derived key will be written to out. The size of the out buffer is specified via keylen.

NOTES

A typical application of this function is to derive keying material for an encryption algorithm from a password in the pass, a salt in salt, and an iteration count.

Increasing the iter parameter slows down the algorithm which makes it harder for an attacker to perform a brute force attack using a large number of candidate passwords.

These functions make no assumption regarding the given password. It

will simply be treated as a byte sequence.

RETURN VALUES

PKCS5_PBKDF2_HMAC() and PBKCS5_PBKDF2_HMAC_SHA1() return 1 on success or 0 on error.

SEE ALSO

evp(7), RAND_bytes(3), EVP_BytesToKey(3), passphrase-encoding(7)

COPYRIGHT