Rocky Enterprise Linux 9.2 Manual Pages on command 'PKCS12_setup_mac.3ossl'

$ man PKCS12_setup_mac.3ossl

PKCS12_GEN_MAC(3ossl) OpenSSL PKCS12_GEN_MAC(3ossl)

NAME

PKCS12_gen_mac, PKCS12_setup_mac, PKCS12_set_mac, PKCS12_verify_mac -

Functions to create and manipulate a PKCS#12 structure

SYNOPSIS

```
#include <openssl/pkcs12.h>
int PKCS12_gen_mac(PKCS12 *p12, const char *pass, int passlen,
                   unsigned char *mac, unsigned int *maclen);
int PKCS12_verify_mac(PKCS12 *p12, const char *pass, int passlen);
int PKCS12_set_mac(PKCS12 *p12, const char *pass, int passlen,
                   unsigned char *salt, int saltlen, int iter,
                   const EVP_MD *md_type);
int PKCS12_setup_mac(PKCS12 *p12, int iter, unsigned char *salt,
                     int saltlen, const EVP_MD *md_type);
```

DESCRIPTION

PKCS12_gen_mac() generates an HMAC over the entire PKCS#12 object using the supplied password along with a set of already configured paramters.

PKCS12_verify_mac() verifies the PKCS#12 object's HMAC using the

supplied password.

PKCS12_setup_mac() sets the MAC part of the PKCS#12 structure with the supplied parameters.

PKCS12_set_mac() sets the MAC and MAC parameters into the PKCS#12 object.

pass is the passphrase to use in the HMAC. salt is the salt value to use, iter is the iteration count and md_type is the message digest function to use.

NOTES

If salt is NULL then a suitable salt will be generated and used.

If iter is 1 then an iteration count will be omitted from the PKCS#12 structure.

PKCS12_gen_mac(), PKCS12_verify_mac() and PKCS12_set_mac() make assumptions regarding the encoding of the given passphrase. See passphrase-encoding(7) for more information.

RETURN VALUES

All functions return 1 on success and 0 if an error occurred.

CONFORMING TO

IETF RFC 7292 (<https://tools.ietf.org/html/rfc7292>)

SEE ALSO

d2i_PKCS12(3), PKCS12_create(3), passphrase-encoding(7)

COPYRIGHT