Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'OSSL_CRMF_pbm_new.3ossl' command

$ man OSSL_CRMF_pbm_new.3ossl

OSSL_CRMF_PBMP_NEW(3ossl) OpenSSL OSSL_CRMF_PBMP_NEW(3ossl)

NAME

OSSL_CRMF_pbm_new, OSSL_CRMF_pbmp_new - functions for producing Password-Based MAC (PBM)

SYNOPSIS

```
#include <openssl/crmf.h>
int OSSL_CRMF_pbm_new(OSSL_LIB_CTX *libctx, const char *propq,
                      const OSSL_CRMF_PBMPARAMETER *pbmp,
                      const unsigned char *msg, size_t msglen,
                      const unsigned char *sec, size_t seclen,
                      unsigned char **mac, size_t *maclen);
OSSL_CRMF_PBMPARAMETER *OSSL_CRMF_pbmp_new(OSSL_LIB_CTX *libctx, size_t saltlen,
                                           int owfnid, size_t itercnt,
                                           int macnid);
```

DESCRIPTION

OSSL_CRMF_pbm_new() generates a PBM (Password-Based MAC) based on given PBM parameters pbmp, message msg, and secret sec, along with the respective lengths msglen and seclen. The optional library context libctx and propq parameters may be used to influence the selection of the MAC algorithm referenced in the pbmp; see "ALGORITHM FETCHING" in crypto(7) for further information. On success writes the address of the newly allocated MAC via the mac reference parameter and writes the length via the maclen reference parameter unless it its NULL.

OSSL_CRMF_pbmp_new() initializes and returns a new PBMParameter structure with a new random salt of given length saltlen, OWF (one-way function) NID owfnid, OWF iteration count itercnt, and MAC NID macnid. The library context libctx parameter may be used to select the provider for the random number generation (DRBG) and may be NULL for the default.

NOTES

The algorithms for the OWF (one-way function) and for the MAC (message authentication code) may be any with a NID defined in <openssl/objects.h>. As specified by RFC 4210, these should include NID_hmac_sha1.

RFC 4210 recommends that the salt SHOULD be at least 8 bytes (64 bits) long, where 16 bytes is common.

The iteration count must be at least 100, as stipulated by RFC 4211, and is limited to at most 100000 to avoid DoS through manipulated or otherwise malformed input.

RETURN VALUES

OSSL_CRMF_pbm_new() returns 1 on success, 0 on error.

OSSL_CRMF_pbmp_new() returns a new and initialized OSSL_CRMF_PBMPARAMETER structure, or NULL on error.

EXAMPLES

```
OSSL_CRMF_PBMPARAMETER *pbm = NULL;
unsigned char *msg = "Hello";
unsigned char *sec = "SeCrEt";
unsigned char *mac = NULL;
size_t maclen;
if ((pbm = OSSL_CRMF_pbmp_new(16, NID_sha256, 500, NID_hmac_sha1) == NULL))
    goto err;
if (!OSSL_CRMF_pbm_new(pbm, msg, 5, sec, 6, &mac, &maclen))
    goto err;
```

SEE ALSO

RFC 4211 section 4.4

HISTORY

The OpenSSL CRMF support was added in OpenSSL 3.0.

COPYRIGHT