NAME

OSSL_CRMF_MSG_get0_tmpl, OSSL_CRMF_CERTTEMPLATE_get0_serialNumber, OSSL_CRMF_CERTTEMPLATE_get0_subject, OSSL_CRMF_CERTTEMPLATE_get0_issuer, OSSL_CRMF_CERTTEMPLATE_get0_extensions, OSSL_CRMF_CERTID_get0_serialNumber, OSSL_CRMF_CERTID_get0_issuer, OSSL_CRMF_ENCRYPTEDVALUE_get1_encCert, OSSL_CRMF_MSG_get_certReqId - functions reading from CRMF CertReqMsg structures

SYNOPSIS

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

OSSL_CRMF_CERTTEMPLATE *OSSL_CRMF_MSG_get0_tmpl(const OSSL_CRMF_MSG *crm);
const ASN1_INTEGER
*OSSL_CRMF_CERTTEMPLATE_get0_serialNumber(const OSSL_CRMF_CERTTEMPLATE *tmpl);
const X509_NAME
*OSSL_CRMF_CERTTEMPLATE_get0_subject(const OSSL_CRMF_CERTTEMPLATE *tmpl);
const X509_NAME
*OSSL_CRMF_CERTTEMPLATE_get0_issuer(const OSSL_CRMF_CERTTEMPLATE *tmpl);
X509_EXTENSIONS
*OSSL_CRMF_CERTTEMPLATE_get0_extensions(const OSSL_CRMF_CERTTEMPLATE *tmpl);

const ASN1_INTEGER
*OSSL_CRMF_CERTID_get0_serialNumber(const OSSL_CRMF_CERTID *cid);
const X509_NAME *OSSL_CRMF_CERTID_get0_issuer(const OSSL_CRMF_CERTID *cid);

X509
*OSSL_CRMF_ENCRYPTEDVALUE_get1_encCert(const OSSL_CRMF_ENCRYPTEDVALUE *ecert,
                                       OSSL_LIB_CTX *libctx, const char *propq,
                                       EVP_PKEY *pkey);

int OSSL_CRMF_MSG_get_certReqId(const OSSL_CRMF_MSG *crm);
```

DESCRIPTION

OSSL_CRMF_MSG_get0_tmpl() retrieves the certificate template of *crm*.

OSSL_CRMF_CERTTEMPLATE_get0_serialNumber() retrieves the serialNumber of the given certificate template *tmpl*.

OSSL_CRMF_CERTTEMPLATE_get0_subject() retrieves the subject name of the given certificate template *tmpl*.

OSSL_CRMF_CERTTEMPLATE_get0_issuer() retrieves the issuer name of the given certificate template *tmpl*.

OSSL_CRMF_CERTTEMPLATE_get0_extensions() retrieves the X.509 extensions of the given certificate template *tmpl*, or NULL if not present.

OSSL_CRMF_CERTID_get0_serialNumber retrieves the serialNumber of the given CertId *cid*.

OSSL_CRMF_CERTID_get0_issuer retrieves the issuer name of the given CertId *cid*, which must be of ASN.1 type GEN_DIRNAME.

OSSL_CRMF_ENCRYPTEDVALUE_get1_encCert() decrypts the certificate in the given encryptedValue *ecert*, using the private key *pkey*, library context *libctx* and property query string *propq* (see **OSSL_LIB_CTX**(3)). This is needed for the indirect POPO method as in RFC 4210 section 5.2.8.2. The function returns the decrypted certificate as a copy, leaving its ownership with the caller, who is responsible for freeing it.

OSSL_CRMF_MSG_get_certReqId() retrieves the certReqId of *crm*.

RETURN VALUES

OSSL_CRMF_MSG_get_certReqId() returns the certificate request ID as a nonnegative integer or -1 on error.

All other functions return a pointer with the intended result or NULL on error.

SEE ALSO

RFC 4211

HISTORY

The OpenSSL CRMF support was added in OpenSSL 3.0.

COPYRIGHT

Copyright 2007-2021 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.