NAME

OSSL_CMP_validate_msg, OSSL_CMP_validate_cert_path - functions for verifying CMP message protection

SYNOPSIS

```
#include <openssl/cmp.h>
int OSSL_CMP_validate_msg(OSSL_CMP_CTX *ctx, OSSL_CMP_MSG *msg);
int OSSL_CMP_validate_cert_path(const OSSL_CMP_CTX *ctx,
                                X509_STORE *trusted_store, X509 *cert);
```

DESCRIPTION

This is the API for validating the protection of CMP messages, which includes validating CMP message sender certificates and their paths while optionally checking the revocation status of the certificates(s).

OSSL_CMP_validate_msg() validates the protection of the given *msg*, which must be signature-based or using password-based MAC (PBM). In the former case a suitable trust anchor must be given in the CMP context *ctx*, and in the latter case the matching secret must have been set there using **OSSL_CMP_CTX_set1_secretValue**(3).

In case of signature algorithm, the certificate to use for the signature check is preferably the one provided by a call to **OSSL_CMP_CTX_set1_srvCert**(3). If no such sender cert has been pinned then candidate sender certificates are taken from the list of certificates received in the *msg* extraCerts, then any certificates provided before via **OSSL_CMP_CTX_set1_untrusted**(3), and then all trusted certificates provided via **OSSL_CMP_CTX_set0_trustedStore**(3), where a candidate is acceptable only if has not expired, its subject DN matches the *msg* sender DN (as far as present), and its subject key identifier is present and matches the senderKID (as far as the latter present). Each acceptable cert is tried in the given order to see if the message signature check succeeds and the cert and its path can be verified using any trust store set via **OSSL_CMP_CTX_set0_trustedStore**(3).

If the option OSSL_CMP_OPT_PERMIT_TA_IN_EXTRACERTS_FOR_IR was set by calling **OSSL_CMP_CTX_set_option**(3), for an Initialization Response (IP) message any self-issued certificate from the *msg* extraCerts field may also be used as trust anchor for the path verification of an acceptable cert if it can be used also to validate the issued certificate returned in the IP message. This is according to TS 33.310 [Network Domain Security (NDS); Authentication Framework (AF)] document specified by the The 3rd Generation Partnership Project (3GPP).

Any cert that has been found as described above is cached and tried first when validating the signatures of subsequent messages in the same transaction.

OSSL_CMP_validate_cert_path() attempts to validate the given certificate and its path using the given store of trusted certs (possibly including CRLs and a cert verification callback) and non-trusted intermediate certs from the *ctx*.

NOTES

CMP is defined in RFC 4210 (and CRMF in RFC 4211).

RETURN VALUES

OSSL_CMP_validate_msg() and **OSSL_CMP_validate_cert_path()** return 1 on success, 0 on error or validation failed.

SEE ALSO

OSSL_CMP_CTX_new(3), **OSSL_CMP_exec_certreq**(3), **OSSL_CMP_CTX_set1_secretValue**(3), **OSSL_CMP_CTX_set1_srvCert**(3), **OSSL_CMP_CTX_set1_untrusted**(3), **OSSL_CMP_CTX_set0_trustedStore**(3)

HISTORY

The OpenSSL CMP support was added in OpenSSL 3.0.

COPYRIGHT