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

$ man SSL_get_signature_nid.3ossl

SSL_GET_PEER_SIGNATURE_NID(3ossl) OpenSSL SSL_GET_PEER_SIGNATURE_NID(3ossl)

NAME

SSL_get_peer_signature_nid, SSL_get_peer_signature_type_nid,

SSL_get_signature_nid, SSL_get_signature_type_nid - get TLS message

signing types

SYNOPSIS

#include <openssl/ssl.h>

int SSL_get_peer_signature_nid(SSL *ssl, int *psig_nid);

int SSL_get_peer_signature_type_nid(const SSL *ssl, int *psigtype_nid);

int SSL_get_signature_nid(SSL *ssl, int *psig_nid);

int SSL_get_signature_type_nid(const SSL *ssl, int *psigtype_nid);

DESCRIPTION

SSL_get_peer_signature_nid() sets *psig_nid to the NID of the digest

used by the peer to sign TLS messages. It is implemented as a macro.

SSL_get_peer_signature_type_nid() sets *psigtype_nid to the signature type used by the peer to sign TLS messages. Currently the signature type is the NID of the public key type used for signing except for PSS signing where it is EVP_PKEY_RSA_PSS. To differentiate between rsa_pss_rsae_* and rsa_pss_pss_* signatures, it's necessary to check the type of public key in the peer's certificate.

SSL_get_signature_nid() and SSL_get_signature_type_nid() return the equivalent information for the local end of the connection.

RETURN VALUES

These functions return 1 for success and 0 for failure. There are several possible reasons for failure: the cipher suite has no signature (e.g. it uses RSA key exchange or is anonymous), the TLS version is below 1.2 or the functions were called too early, e.g. before the peer signed a message.

SEE ALSO

ssl(7), SSL_get_peer_certificate(3),

COPYRIGHT