
*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_ESS_check_signing_certs.3ossl' command*

***$ man OSSL_ESS_check_signing_certs.3ossl***

OSSL_ESS_CHECK_SIGNING_CERTS(3ossl) OpenSSLOSSL_ESS_CHECK_SIGNING_CERTS(3ossl)

NAME

OSSL_ESS_signing_cert_new_init, OSSL_ESS_signing_cert_v2_new_init,

OSSL_ESS_check_signing_certs - Enhanced Security Services (ESS)

functions

SYNOPSIS

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

ESS_SIGNING_CERT *OSSL_ESS_signing_cert_new_init(const X509 *signcert,
                                                 const STACK_OF(X509) *certs,
                                                 int set_issuer_serial);
ESS_SIGNING_CERT_V2 *OSSL_ESS_signing_cert_v2_new_init(const EVP_MD *hash_alg,
                                                       const X509 *signcert,
                                                       const
                                                       STACK_OF(X509) *certs,
                                                       int set_issuer_serial);
int OSSL_ESS_check_signing_certs(const ESS_SIGNING_CERT *ss,
                                 const ESS_SIGNING_CERT_V2 *ssv2,
                                 const STACK_OF(X509) *chain,
                                 int require_signing_cert);
```

## DESCRIPTION

OSSL_ESS_signing_cert_new_init() generates a new ESS_SIGNING_CERT structure referencing the given signcert and any given further certs using their SHA-1 fingerprints. If set_issuer_serial is nonzero then also the issuer and serial number of signcert are included in the ESS_CERT_ID as the issuerSerial field. For all members of certs the issuerSerial field is always included.

OSSL_ESS_signing_cert_v2_new_init() is the same as OSSL_ESS_signing_cert_new_init() except that it uses the given hash_alg and generates a ESS_SIGNING_CERT_V2 structure with ESS_CERT_ID_V2 elements.

OSSL_ESS_check_signing_certs() checks if the validation chain chain contains the certificates required by the identifiers given in ss and/or ssv2. If require_signing_cert is nonzero, ss or ssv2 must not be NULL. If both ss and ssv2 are not NULL, they are evaluated independently. The list of certificate identifiers in ss is of type ESS_CERT_ID, while the list contained in ssv2 is of type ESS_CERT_ID_V2. As far as these lists are present, they must be nonempty. The certificate identified by their first entry must be the first element of chain, i.e. the signer certificate. Any further certficates referenced in the list must also be found in chain. The matching is done using the given certificate hash algorithm and value. In addition to the checks required by RFCs 2624 and 5035, if the issuerSerial field is included in an ESSCertID or ESSCertIDv2 it must match the certificate issuer and serial number attributes.

## NOTES

ESS has been defined in RFC 2634, which has been updated in RFC 5035 (ESS version 2) to support hash algorithms other than SHA-1. This is used for TSP (RFC 3161) and CAdES-BES (informational RFC 5126).

## RETURN VALUES

OSSL_ESS_signing_cert_new_init() and
OSSL_ESS_signing_cert_v2_new_init() return a pointer to the new structure or NULL on malloc failure.

OSSL_ESS_check_signing_certs() returns 1 on success, 0 if a required certificate cannot be found, -1 on other error.

## SEE ALSO

TS_VERIFY_CTX_set_certs(3), CMS_verify(3)

## HISTORY

OSSL_ESS_signing_cert_new_init(), OSSL_ESS_signing_cert_v2_new_init(), and OSSL_ESS_check_signing_certs() were added in OpenSSL 3.0.

## COPYRIGHT