OpenSSL - verify

Vérifier les chaînes de certificat

OPTIONS

-CApath directory Répertoire des certificats de confiance
-CAfile file Fichier de certificats de confiance
-untrusted file Fichiers de certificats non trustés
-purpose purpose Utilisation du certificat
-verbose mode verbeux
-issuer_checks Affiche des info liés à la recherche du certifieurs.
-policy arg Active le traitement de stratégie et ajoute 'arg' au user-initial-policy-set (RFC5280)
-policy_check Active le traitement de stratégie de certificat
-explicit_policy définis require-explicite-policy (RFC5280)
-inhibit_any définis inhibit-any-policy (see RFC5280)
-inhibit_map définis inhibit-policy-mapping (see RFC5280)
-policy_print Affiche des info sur le traitement des tratégies
-crl_check Vérifie la crl
-crl_check_all Vérifie la validité de toute la chaîne de certificat
-ignore_critical Ignore les extension critique non gérées
-x509_strict mode strict X.509 compliance
-extended_crl Active les fonctionnalités étendues de CRL
-use_deltas Active le support des CRL delta
-check_ss_sig Vérifie la signature du root CA
- indique la dernière option, les arguments suivants sont des certificats
certificates Un ou plusieurs certificats à vérifier

Opérations de vérification

verify utilise les même fonctions que la vérification SSL et S/MIME. La différence entre **verify** et les opérations de vérification est que **verify** peut passer les erreurs et de continuer les opérations de vérifications.

Diagnostique

Quand une opération échoue, un message d'erreur est affiché du type :
server.pem : /C=AU/ST=Queensland/O=CryptSoft Pty Ltd/CN=Test CA (1024 bit)
error 24 at 1 depth lookup :invalid CA certificate

La première ligne contient le nom du certificat qui a été vérifié, suivi du sujet.

La seconde ligne contient le numéro d'erreur est une courte description de l'erreur

```
0 X509_V_OK : ok
2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT : unable to get issuer certificate
3 X509_V_ERR_UNABLE_TO_GET_CRL : unable to get certificate CRL
4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE : unable to decrypt certificate's signature
5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE : unable to decrypt CRL's signature
6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY : unable to decode issuer public key
7 X509_V_ERR_CERT_SIGNATURE_FAILURE : certificate signature failure
8 X509_V_ERR_CRL_SIGNATURE_FAILURE : CRL signature failure
9 X509_V_ERR_CERT_NOT_YET_VALID : certificate is not yet valid
10 X509_V_ERR_CERT_HAS_EXPIRED : certificate has expired
11 X509_V_ERR_CRL_NOT_YET_VALID : CRL is not yet valid
12 X509_V_ERR_CRL_HAS_EXPIRED : CRL has expired
13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD : format error in certificate's notBefore field
14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD : format error in certificate's notAfter field
15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD : format error in CRL's lastUpdate field
16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD : format error in CRL's nextUpdate field
17 X509_V_ERR_OUT_OF_MEM : out of memory
18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT : self signed certificate
19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN : self signed certificate in certificate chain
20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY : unable to get local issuer certificate
21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE : unable to verify the first certificate
22 X509_V_ERR_CERT_CHAIN_TOO_LONG : certificate chain too long
23 X509_V_ERR_CERT_REVOKED : certificate revoked
24 X509_V_ERR_INVALID_CA : invalid CA certificate
25 X509_V_ERR_PATH_LENGTH_EXCEEDED : path length constraint exceeded
26 X509_V_ERR_INVALID_PURPOSE : unsupported certificate purpose
27 X509_V_ERR_CERT_UNTRUSTED : certificate not trusted
28 X509_V_ERR_CERT_REJECTED : certificate rejected
29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH : subject issuer mismatch
30 X509_V_ERR_AKID_SKID_MISMATCH : authority and subject key identifier mismatch
31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH : authority and issuer serial number mismatch
32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN:key usage does not include certificate signing
50 X509_V_ERR_APPLICATION_VERIFICATION : application verification failure
```