OpenSSL - ocsp

Utilitaire OCSP

Options client

-out filename Fichier de sortie

-issuer filename Spécifie l'issuer du certificat courant. Peut-être spécifié plusieurs fois et doit être au format PEM. Doit être spécifié avant -cert

-cert filename Ajoute le certificat spécifié à la requête.

-serial num Idem à cert excepté que le certificat avec le numéro de série spécifié est ajouté à la requête, en entier décimal précédé par 0x. Des valeurs négatives sont acceptées.

-signer filename, -signkey filename Signe la requête OCSP en utilisant le certificat spécifié par signer et la clé privée spécifiée par signkey. Sans signkey, lit la clé privée depuis le certificat du signer. Sans ces 2 options, la requête n'est pas signée.

-sign_other filename Certificats additionnels à inclure dans la requête signée.

-nonce, -no-once Ajoute ou désactive une extension OCSP nonce d'une requête. Normalement si une requête OCSP est entrée en utilisant respin, nonce n'est pas ajouté. Si une requête OCSP est créée, un nonce est automatiquement ajouté.

-req_text, -resp_text, -text Affiche la forme texte d'une requête ou d'une réponse OCSP ou les 2 respectivement.

-reqout file, respout file Écrit la requête ou la réponse en DER

-reqin file, respin file Lit la requête ou la réponse depuis le fichier spécifié.

-url responder_url Spécifie l'url du répondeur.

-host hostname :port, path pathname La requête est envoyée à l'hôte spécifié, ou le chemin HTTP (défaut : /)

-CAfile file, -CApath pathname Fichier ou répertoire contenant les certificats CA. Utilisé pour vérifier la réponse OCSP.

-verify_other file Fichier contenant des certificats additionnels à rechercher lors de la tentative de localisation du certificat de signature de la réponse OCSP.

-trust_other Les certificats spécifié par -verify_other sont explicitement trustés sans vérification additionnelles. Utile pour une chaîne complète de certificat.

-VAfile file Fichier contenant les certificats du répondeur trustés explicitement. Equivalent à -verify_other et -trust_other.

-noverify Ne vérifie par la signature du répondeur OCSP ou les valeurs nonce.

-no_intern Ignore les certificats contenus dans la réponse OCSP lors de la recherche du certificat du signataire.

-no_signature_verify Ne vérifie pas la signature de la réponse OCSP.

-no_cert_verify Ne vérifie par les certifications des signataires de la réponse OCSP.

-no_chain N'utilise pas les certificats dans la réponse comme certificats CA additionnels non-trustés.

-no_cert_checks N'effectue aucune vérification supplémentaire sur les certificats des signataires de la réponse OCSP

-validity_period nsec, -status_age age Spécifie la plage de temps en secondes toléré dans une réponse OCSP. Chaque réponse de statut de certificat inclus notBefore et notAfter. Le temps courant devrait être entre ces 2 valeurs. Cette options permet de spécifier une autre plage de temps.

-md5|-sha1|-sha256|-ripemod160|... Définis l'algorithme digest à utiliser pour l'identification du certificat dans la requête OCSP. Défa

Options serveur

-index indexfile Fichier d'index au format ca contenant les informations de révocation de certificat. Si cette option est spécifiée, ocsp est en mode répondeur, sinon il est en mode client.

-CA file Certificat CA correspondant aux informations de révocation dans indexfile.

-rsigner file Certificat pour signer les réponses

-rother file Certificats additionnels à inclure dans la réponse

-resp_no_certs N'inclus pas de certificat dans la réponse.

-resp_key_id Identifie le certificat signataire en utilisant l'ID de clé. Défaut : utilise le nom du sujet.

-rkey file La clé privée pour signer les réponses.

-port portnum Port d'écoute des requêtes OCSP. Doit être spécifié dans l'option url.

-nrequest number Le serveur va quitter après avoir reçu number requêtes, défaut : illimité.

-nmin minutes, -ndays days Nombre de minutes ou de jours où de nouvelles informations de révocation sont disponibles. Utilisé dans le champ nextUpdate. Sans cette option, ce champ est omis, les nouvelles informations sont immédiatement disponible.

Exemples

Créer une requête OCSP et l'écrire dans un fichier :
openssl ocsp -issuer issuer.pem -cert c1.pem -cert c2.pem -reqout req.der
Envoyer une requête à un répondeur OCSP :
openssl ocsp -issuer issuer.pem -cert c1.pem -cert c2.pem -url http ://ocsp.myhost.com/ -resp_text -respout resp.der
Lire une réponse OCSP et l'afficher au format texte :
openssl ocsp -respin resp.der -text
Serveur OCSP sur le port 8888 en utilisant une configuration standard CA, et un certificat de répondeur séparé :
openssl ocsp -index demoCA/index.txt -port 8888 -rsigner rcert.pem -CA demoCA/cacert.pem -text -out log.txt
Idem, mais quitte après 1 requête :
openssl ocsp -index demoCA/index.txt -port 8888 -rsigner rcert.pem -CA demoCA/cacert.pem -nrequest 1
Demander des informations de statut en utilisant une requête générée en interne :
openssl ocsp -index demoCA/index.txt -rsigner rcert.pem -CA demoCA/cacert.pem -issuer demoCA/cacert.pem -serial 1
Demander des informations de statut en utilisant une requête lu depuis un fichier, sort la réponse dans un autre fichier :
openssl ocsp -index demoCA/index.txt -rsigner rcert.pem -CA demoCA/cacert.pem -reqin req.der -respout resp.der