AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Guide d'utilisation OCSP

Plateforme de l'IGC Santé

Statut : Final | *Classification : Publique* | *Version : v1.0*

Agence du Numérique en Santé
2 - 10 Rue d'Oradour-sur-Glane – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

Historique du document

Version	Rédigé par	
1.0	ANS	Le 28/11/2024
	Motif et nature de la modification : **Création du document**	
	Motif et nature de la modification :	
	Motif et nature de la modification :	
	Motif et nature de la modification :	
	Motif et nature de la modification :	
	Motif et nature de la modification :	
	Motif et nature de la modification :	
	Motif et nature de la modification :	

SOMMAIRE

1. INTRODUCTION

1.1. Objet

Ce document a pour but de décrire le fonctionnement du répondeur OCSP de l'ANS chargé de la validation des certificats de l'IGC-Santé.

1.2. Présentation générale du protocole OCSP

Le protocole OCSP permet à un utilisateur de certificat de vérifier dynamiquement le statut de révocation d'un certificat X.509, plutôt que d'utiliser le téléchargement périodique de CRL.

L'OCSP est un protocole défini dans le RFC 6960.

2. GLOSSAIRE

Acronyme	Signification
ANS	Agence du Numérique en Santé
IGC	Infrastructure de Gestion de Clés (PKI en anglais, pour Public key Infrastructure).
RFC	Request For Comments
CRL	Certificate Revocation List. Liste des certificats révoqués en français
OCSP	Online Certificate Status Protocol
PFCNG	Plateforme de confiance de nouvelle génération
URL	Uniform Resource Locator
Openssl	Openssl est une boîte à outils de chiffrement comportant deux bibliothèques, libcrypto et libssl, fournissant respectivement une implémentation des algorithmes cryptographiques et du protocole de communication SSL/TLS, ainsi qu'une interface en ligne de commande, openssl.

3. FONCTIONNEMENT DE L'OCSP

L'OCSP est un protocole synchrone : l'utilisateur émet une requête à un serveur OCSP (appelé « répondeur OCSP ») et attend sa réponse avant de valider le certificat. Cela permet de :

1. Vérifier que le certificat a été signé par une autorité connue (AC intermédiaire).
2. Vérifier cette autorité est elle-même signé par une autorité de confiance (AC Racine).
3. Vérifier que le certificat n'est pas expiré.
4. Vérifier que le certificat n'est pas révoqué.

L'IGC Santé met à la disposition des utilisateurs de certificat ce service à l'adresse : http://ocsp.esante.gouv.fr.

3.1. Requête OCSP

Ce paragraphe décrit la requête OCSP à envoyer via Openssl pour interroger le répondeur OCSP. La requête s'exécute en ligne de commande.

La requête est de la forme suivante :

```
openssl ocsp -text -issuer <Certificat Emetteur> -CAfile <Certificat Racine> -url
<adresse du répondeur OCSP> -cert <Certificat à vérifier>
```

Les arguments de la requête sont :

- **text** : augmente la verbosité de la réponse
- **issuer** : le certificat de l'émetteur (ACI intermédiaire qui a signé le certificat à vérifier) au format PEM.
- **CAfile** : le certificat d'autorité racine (ACR qui a signé l'ACI) au format PEM.
- **url** : l'adresse du répondeur OCSP indiquée dans le certificat à vérifier. Dans le cas présent : http://ocsp.esante.gouv.fr
- **cert** : le certificat à vérifier au format PEM.

> ***La requête OCSP contient les informations nécessaires pour identifier le certificat qui doit être vérifié.***

Remarque :

- Indiquer le chemin des certificats, s'ils ne sont pas dans le répertoire courant où s'exécute la commande.
- Utiliser la commande suivante pour convertir les certificats de l'IGC-Santé, téléchargeables au format DER, en format PEM attendu par openssl pour la requête OCSP.
  ```
  openssl x509 -inform der -in ACI-EL-ORG.cer -out ACI-EL-ORG.pem
  ```
- Il est également possible de remplacer l'argument **cert** par **serial**, l'identifiant unique au format hexadécimal. Il se trouve dans l'attribut numéro de série du certificat. Le numéro de série doit être préfixé avec 0x ; la taille est de 32 caractères alphanumériques.

3.1.1. Exemples de requêtes

Le cas d'un certificat valide :

```
openssl ocsp -text -issuer "C:\data\OCSP\ACI-EL-ORG.pem" -CAfile "C:\data\OCSP\ACR-
EL.pem" -url http://ocsp.esante.gouv.fr -cert "C:\data\OCSP\Good.pem"
```

Le cas d'un certificat révoqué :

```
openssl ocsp -text -issuer "C:\data\OCSP\ACI-ST-PP.pem" -CAfile "C:\data\OCSP\ACR-
ST.pem" -url http://ocsp.esante.gouv.fr -cert "C:\data\OCSP\Revoked.pem"
```

Le cas d'un certificat inconnu :

```
openssl ocsp -text -issuer "C:\data\OCSP\ACI-ST-PP.pem" -CAfile "C:\data\OCSP\ACR-
ST.pem" -url http://ocsp.esante.gouv.fr -cert "C:\data\OCSP\Unknown.pem"
```

3.2. Réponse OCSP

Dès lors que la requête OCSP est correctement formée et qu'elle contient toutes les informations nécessaires au serveur, une réponse définitive est renvoyée avec le statut « SUCCESSFUL ». Cette réponse renvoie un état pour le certificat qui peut être GOOD, REVOKED ou UNKNOWN :

- GOOD : Le certificat n'est pas révoqué.
- REVOKED : Le certificat est révoqué.

- UNKNOWN : Le répondeur ne connait pas le statut du certificat (en général parce qu'il ne connait pas l'AC émettrice du certificat).

3.2.1. Exemples de réponse

Dans un souci de clarté le paramètre « text » a été retiré afin d'avoir une réponse OCSP est plus courte.

Le cas d'un certificat valide :

```
Response verify OK
C:\data\OCSP\Good.pem: good
        This Update: Mar 28 15:57:41 2024 GMT
        Next Update: Mar 29 16:27:41 2024 GMT
```

Le cas d'un certificat révoqué :

```
Response verify OK
C:\data\OCSP\Revoked.pem: revoked
        This Update: Mar 28 16:42:48 2024 GMT
        Next Update: Mar 29 13:56:57 2024 GMT
        Revocation Time: Nov 30 20:45:07 2023 GMT
```

Le cas d'un certificat inconnu :

```
Response verify OK
C:\data\OCSP\Unknown.pem: unknown
        This Update: Mar 28 13:26:57 2024 GMT
        Next Update: Mar 29 13:56:57 2024 GMT
```

3.2.2. Signature des réponses

Dans l'implémentation effectuée pour l'IGC-Santé, le certificat utilisé pour signer les réponses OCSP est dédié à cet usage, et émis par la même AC que celle utilisée pour émettre le certificat vérifié. Toutes les réponses définitives sont signées.

3.2.3. Cas d'erreur

Le répondeur OCSP peut aussi être dans l'incapacité de fournir une réponse. Dans ce cas, il renvoie une réponse non signée, avec un statut « malformedRequest », « internalError » ou « tryLater ».

> ***Le service OCSP permet un statut temps réel de l'état de révocation des certificats et une confirmation de son existence au sein de l'IGC en une seule opération. En comparaison , la CRL ne fournit que l'information de son état de révocation si le numéro de série du certificat est présent dans la CRL.***

FIN DU DOCUMENT