Ecole Centrale Polytechnique d'Ingénieurs

Mise en place d'une PKI - OPENSSL

Cycle : ING1

Module : Sécurité informatique

Table des matières

1. Introduction 3

2. Créer la paire racine 4

2.1. Préparer le répertoire 4
2.2. Préparer le fichier de configuration 5
2.3. Créer la clé racine 6
2.4. Créer le certificat racine 6
2.5. Vérifier le certificat racine 7

3. Créer la paire intermédiaire 8

3.1. Préparer le répertoire 9
3.2. Créer la clé intermédiaire 10
3.3. Créer le certificat intermédiaire 10
3.4. Vérifier le certificat intermédiaire 11
3.5. Créer le fichier de chaîne de certificats 12

4. Signer les certificats serveur et client 13

4.1. Créer une clé 14
4.2. Créer un certificat 14
4.3. Vérifier le certificat 15
4.4. Déployer le certificat 17

5. Liste de révocation de certificats 18

5.1. Préparer le fichier de configuration 19
5.2. Créer la liste de révocation de certificats 19
5.3. Révoquer un certificat 21
5.4. Utiliser le côté serveur de la liste de révocation de certificats 25
5.5. Utiliser le côté client de la liste de révocation de certificats 25

6. Protocole d'état du certificat en ligne 26

6.1. Préparer le fichier de configuration 27
6.2. Créer la paire OCSP 28
6.3. Révoquer un certificat 31

1. Introduction

OpenSSL est une bibliothèque cryptographique gratuite et open-source qui fournit plusieurs Outils de ligne de commande pour la gestion des certificats numériques. Certains de ces outils peuvent être utilisé pour agir en tant qu'autorité de certification.

Une autorité de certification (CA) est une entité qui signe des certificats numériques. Les sites Web doivent informer leurs clients que la connexion est sécurisée, afin qu'ils payent une autorité de certification de confiance internationale (par exemple, VeriSign, DigiCert) pour signer un certificat pour leur domaine.

Dans certains cas, il peut être plus logique d'agir comme votre propre CA, plutôt que de payer un CA comme DigiCert. Les cas courants incluent la sécurisation d'un site Web intranet, ou pour l'émission de certificats aux clients pour leur permettre de s'authentifier auprès d'un serveur (par exemple, Apache, OpenVPN).

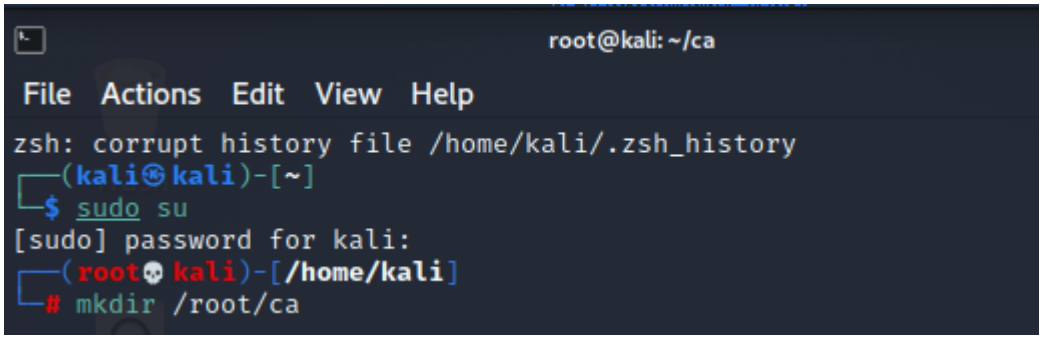
2. Créer la paire racine

Agir en tant qu'autorité de certification (CA) signifie traiter des paires cryptographiques de Clés privées et certificats publics. La toute première paire cryptographique que nous allons créer est la paire racine. Il se compose de la clé racine () et de la racine certificat (). Cette paire forme l'identité de votre autorité de certification. `ca.key.pem` `ca.cert.pem`

En règle générale, l'autorité de certification racine ne signe pas directement les certificats serveur ou client. Le L'autorité de certification racine n'est utilisée que pour créer une ou plusieurs autorités de certification intermédiaires, qui sont approuvé par l'autorité de certification racine pour signer les certificats en son nom. C'est le meilleur pratique. Il permet à la clé racine d'être conservée hors ligne et inutilisée autant que possible, car toute compromission de la clé racine est désastreuse.

2.1. Préparer le répertoire

Choisissez un répertoire () pour stocker toutes les clés et tous les certificats. `/root/ca`



Créez la structure de répertoires. Les fichiers et agissent comme un Base de données de fichiers plats pour garder une trace des certificats signés. `index.txt` `serial`

2.2. Préparer le fichier de configuration

Vous devez créer un fichier de configuration pour OpenSSL à utiliser.

```
┌──(root💀kali)-[~/ca]
└─# touch openssl.cnf

┌──(root💀kali)-[~/ca]
└─# nano openssl.cnf
```

Copier l'autorité de certification racine de *l'annexe* à ./root/ca/openssl.cnf

```
  GNU nano 5.9                                                    openssl.cnf
# OpenSSL root CA configuration file.
# Copy to `/root/ca/openssl.cnf`.

[ ca ]
# `man ca`
default_ca = CA_default

[ CA_default ]
# Directory and file locations.
dir               = /root/ca
certs             = $dir/certs
crl_dir           = $dir/crl
new_certs_dir     = $dir/newcerts
database          = $dir/index.txt
serial            = $dir/serial
RANDFILE          = $dir/private/.rand

# The root key and root certificate.
private_key       = $dir/private/ca.key.pem
certificate       = $dir/certs/ca.cert.pem

# For certificate revocation lists.
crlnumber         = $dir/crlnumber
crl               = $dir/crl/ca.crl.pem
crl_extensions    = crl_ext
default_crl_days  = 30

# SHA-1 is deprecated, so use SHA-2 instead.
default_md        = sha256

name_opt          = ca_default
                                                  [ Read 132 lines ]
```

2.3. Créer la clé racine

Créez la clé racine () et conservez-la absolument sécurisée. N'importe qui dans La possession de la clé racine peut émettre des certificats approuvés. Chiffrer la clé racine avec cryptage AES 256 bits et un mot de passe fort.ca.key.pem

```
┌──(root💀kali)-[~/ca]
└─# cd /root/ca

┌──(root💀kali)-[~/ca]
└─# openssl genrsa -aes256 -out private/ca.key.pem 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................++++
.....................................................................................................................................................
....++++
e is 65537 (0×010001)
Enter pass phrase for private/ca.key.pem:
Verifying - Enter pass phrase for private/ca.key.pem:

┌──(root💀kali)-[~/ca]
└─# chmod 400 private/ca.key.pem
```

2.4. Créer le certificat racine

Utilisez la clé racine () pour créer un certificat racine (). Donnez au certificat racine une longue date d'expiration, par exemple vingt ans. Une fois que le certificat racine expire, tous les certificats signés par l'autorité de certification deviennent non valides.ca.key.pemca.cert.pem

```
┌──(root💀kali)-[~/ca]
└─# openssl req -config openssl.cnf \
      -key private/ca.key.pem \
      -new -x509 -days 7300 -sha256 -extensions v3_ca \
      -out certs/ca.cert.pem
Enter pass phrase for private/ca.key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:GB
State or Province Name [England]:England
Locality Name []:
Organization Name [Alice Ltd]:Alice Ltd
Organizational Unit Name []:Alice Ltd Certificate Authority
Common Name []:Alice Ltd Root CA
Email Address []:

┌──(root💀kali)-[~/ca]
└─# chmod 444 certs/ca.cert.pem
```

2.5. Vérifier le certificat racine

La sortie montre :

- L'occasion Signature Algorithm
- Les dates du certificat Validity
- La longueur en bits Public-Key
- Qui est l'entité qui a signé le certificat Issuer
- Qui fait référence au certificat lui-même Subject

Notez que tous les certificats racines sont auto-signés. Issuer Subject

```
┌──(root💀kali)-[~/ca]
└─#  openssl x509 -noout -text -in certs/ca.cert.pem
Certificate:
    Data:
        Version: 3 (0×2)
        Serial Number:
            3b:81:d2:00:de:c5:9e:34:48:ad:fd:0b:f7:48:0d:fe:ea:12:80:29
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = GB, ST = England, O = Alice Ltd, OU = Alice Ltd Certificate Authority, CN = Alice Ltd Root CA
        Validity
            Not Before: Apr  6 14:49:42 2023 GMT
            Not After : Apr  1 14:49:42 2043 GMT
        Subject: C = GB, ST = England, O = Alice Ltd, OU = Alice Ltd Certificate Authority, CN = Alice Ltd Root CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
```

La sortie montre également les **extensions X509v3**. Nous avons appliqué l'extension, de sorte que les options de devraient être reflétées dans la sortie. v3_ca[v3_ca]

```
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                2E:91:2E:97:CE:F9:4E:F3:1B:FD:23:3A:3C:A1:74:A0:4A:22:79:75
            X509v3 Authority Key Identifier:
                keyid:2E:91:2E:97:CE:F9:4E:F3:1B:FD:23:3A:3C:A1:74:A0:4A:22:79:75

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```


3. Créer la paire intermédiaire

Une autorité de certification intermédiaire est une entité qui peut signer certificats pour le compte de l'autorité de certification racine. L'autorité de certification racine signe l'intermédiaire certificat, formant une chaîne de confiance.

L'utilisation d'une autorité de certification intermédiaire a principalement pour but de sécurité. La clé racine peut être conservé hors ligne et utilisé aussi rarement que possible. Si l'intermédiaire est compromise, l'autorité de certification racine peut révoquer le certificat intermédiaire et Créez une nouvelle paire cryptographique intermédiaire.

3.1. Préparer le répertoire

Les fichiers d'autorité de certification racine sont conservés. Choisissez un autre répertoire () pour stocker les fichiers d'autorité de certification intermédiaires. /root/ca/root/ca/intermediate

```
┌──(root💀kali)-[~/ca]
└─# mkdir /root/ca/intermediate
```

Créez la même structure de répertoires que celle utilisée pour les fichiers d'autorité de certification racine. C'est pratique pour également créer un répertoire contenant les demandes de signature de certificat.csr

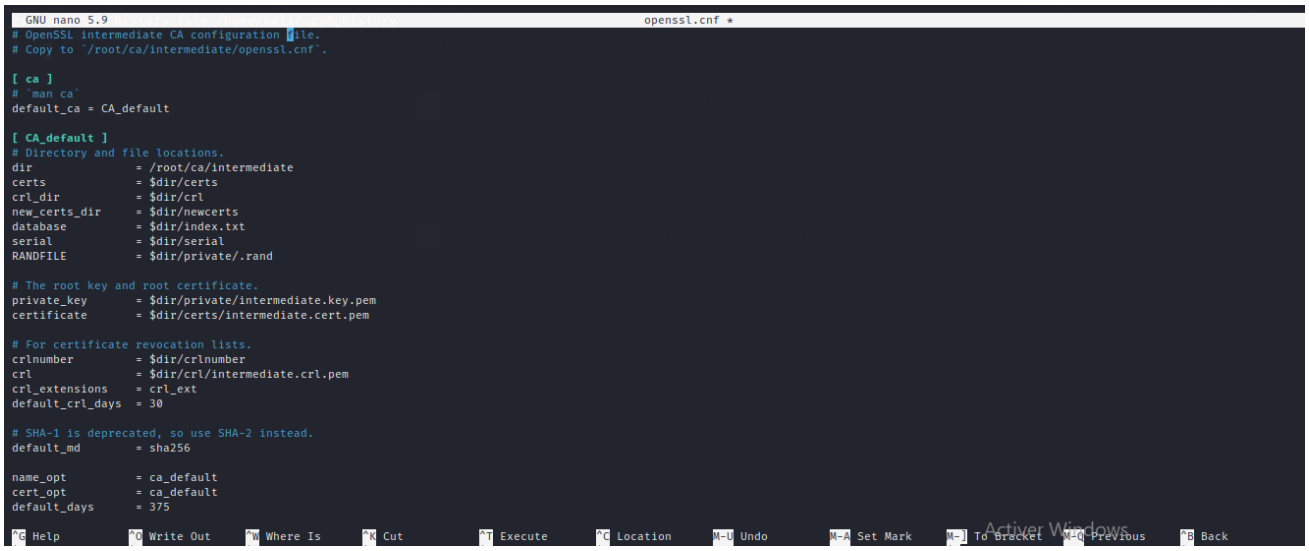
```
┌──(root💀kali)-[~/ca]
└─# cd /root/ca/intermediate

┌──(root💀kali)-[~/ca/intermediate]
└─# mkdir certs crl csr newcerts private

┌──(root💀kali)-[~/ca/intermediate]
└─# chmod 700 private

┌──(root💀kali)-[~/ca/intermediate]
└─# touch index.txt

┌──(root💀kali)-[~/ca/intermediate]
└─# echo 1000 > serial
```

Ajoutez un fichier à l'arborescence de répertoires de l'autorité de certification intermédiaire. Il est utilisé pour effectuer le suivi des *listes de révocation de certificats*.crlnumbercrlnumber

```
┌──(root💀kali)-[~/ca/intermediate]
└─# echo 1000 > /root/ca/intermediate/crlnumber
```

Copiez le fichier de configuration de l'autorité de certification intermédiaire de *l'annexe* vers. Cinq options ont été modifiées par rapport à au fichier de configuration de l'autorité de certification racine :/root/ca/intermediate/openssl.cnf

```
┌──(root💀kali)-[~/ca/intermediate]
└─# touch openssl.cnf

┌──(root💀kali)-[~/ca/intermediate]
└─# nano openssl.cnf
```



3.2. Créer la clé intermédiaire

Créez la clé intermédiaire (). Chiffrer l'intermédiaire avec cryptage AES 256 bits et un mot de passe fort.intermediate.key.pem

3.3. Créer le certificat intermédiaire

Utilisez la clé intermédiaire pour créer une demande de signature de certificat (CSR). Les détails doivent généralement correspondre à l'autorité de certification racine. Le **commun Le nom**, cependant, doit être différent.

```
┌──(root💀kali)-[~/ca]
└─# openssl req -config intermediate/openssl.cnf -new -sha256 \
      -key intermediate/private/intermediate.key.pem \
      -out intermediate/csr/intermediate.csr.pem
Enter pass phrase for intermediate/private/intermediate.key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:GB
State or Province Name [England]:England
Locality Name []:
Organization Name [Alice Ltd]:Alice Ltd
Organizational Unit Name []:Alice Ltd Certificate Authority
Common Name []:Alice Ltd Intermediate CA
Email Address []:

┌──(root💀kali)-[~/ca]
└─#
```

Pour créer un certificat intermédiaire, utilisez l'autorité de certification racine avec l'extension pour signer la demande de signature de certificat intermédiaire. L'intermédiaire Le certificat doit être valide pour une période plus courte que le certificat racine. Dix ans seraient raisonnables. v3_intermediate_ca

```
┌──(root💀kali)-[~/ca]
└─# openssl ca -config openssl.cnf -extensions v3_intermediate_ca \
      -days 3650 -notext -md sha256 \
      -in intermediate/csr/intermediate.csr.pem \
      -out intermediate/certs/intermediate.cert.pem
Using configuration from openssl.cnf
Enter pass phrase for /root/ca/private/ca.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Apr  6 22:26:19 2023 GMT
            Not After : Apr  3 22:26:19 2033 GMT
        Subject:
            countryName               = GB
            stateOrProvinceName       = England
            organizationName          = Alice Ltd
            organizationalUnitName    = Alice Ltd Certificate Authority
            commonName                = Alice Ltd Intermediate CA
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                49:B9:5E:4D:81:25:6E:83:10:F1:8E:68:38:E4:59:3E:8C:B9:0E:EE
            X509v3 Authority Key Identifier:
                keyid:2E:91:2E:97:CE:F9:4E:F3:1B:FD:23:3A:3C:A1:74:A0:4A:22:79:75

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
Certificate is to be certified until Apr  3 22:26:19 2033 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

```
┌──(root💀kali)-[~/ca]
└─# chmod 444 intermediate/certs/intermediate.cert.pem
```

3.4. Vérifier le certificat intermédiaire

Comme nous l'avons fait pour le certificat racine, vérifiez que les détails de l'intermédiaire sont corrects.

```
┌──(root💀 kali)-[~/ca]
└─# openssl x509 -noout -text \
    -in intermediate/certs/intermediate.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = GB, ST = England, O = Alice Ltd, OU = Alice Ltd Certificate Authority, CN = Alice Ltd Root CA
        Validity
            Not Before: Apr  6 22:26:19 2023 GMT
            Not After : Apr  3 22:26:19 2033 GMT
        Subject: C = GB, ST = England, O = Alice Ltd, OU = Alice Ltd Certificate Authority, CN = Alice Ltd Intermediate CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:ba:cf:c3:54:dd:ca:95:f0:84:c0:05:07:ca:06:
                    a4:e8:d1:7b:75:e0:12:11:51:ac:bc:f2:26:ee:64:
                    60:19:9e:b4:e5:c9:70:be:34:b3:00:47:d3:aa:8d:
                    8d:ec:a0:e1:c5:59:b3:17:3e:4b:a1:0a:3a:24:78:
                    14:89:f2:d4:5e:c6:8e:58:ce:90:6d:80:d3:98:44:
                    da:33:7c:76:9e:9b:83:7a:1a:e8:6e:db:10:a5:a3:
                    36:90:02:8a:b4:b1:5c:0e:58:31:6a:55:3b:8b:14:
                    fb:34:88:3e:22:be:d0:16:76:b3:87:55:66:d1:50:
                    9f:49:02:2c:47:3e:56:27:17:6c:78:85:f5:59:6c:
                    51:76:60:98:56:81:10:e0:44:90:33:35:72:aa:0a:
                    d9:05:c6:02:cb:a4:de:df:23:3d:a0:56:20:b6:ae:
                    71:90:f4:b6:9f:2d:05:ec:0d:38:22:f1:e6:3b:72:
                    3f:7f:34:f1:d1:5d:2b:96:88:25:ae:39:09:e5:7e:
                    cf:58:12:39:ad:0b:e5:0f:24:38:f6:69:c2:cf:71:
                    4d:e6:1c:7c:8a:06:1e:fb:84:90:2c:c8:38:d8:07:
                    34:c0:0f:c1:7c:53:52:7c:77:e0:c0:ba:44:db:39:
                    39:b4:85:15:6e:c4:df:a6:bc:cd:bd:79:f3:7f:0e:
                    3f:66:cc:de:42:dd:5f:7d:fb:1e:c4:3b:d1:ea:e8:
                    17:ff:f2:33:39:82:6d:4c:eb:6f:7e:ef:bf:b6:7d:
```

Vérifiez le certificat intermédiaire par rapport au certificat racine. Un indique que la chaîne de confiance est intacte.OK

```
┌──(root💀 kali)-[~/ca]
└─# openssl verify -CAfile certs/ca.cert.pem \
     intermediate/certs/intermediate.cert.pem
intermediate/certs/intermediate.cert.pem: OK

┌──(root💀 kali)-[~/ca]
└─#
```

3.5. Créer le fichier de chaîne de certificats

Lorsqu'une application (par exemple, un navigateur Web) tente de vérifier un certificat signé par l'autorité de certification intermédiaire, elle doit également vérifier le certificat intermédiaire par rapport à le certificat racine. Pour compléter la chaîne de confiance, créez un certificat d'autorité de certification à présenter à l'application. Pour créer la chaîne de certificats d'autorité de certification, concaténer l'intermédiaire et la racine certificats ensemble. Nous utiliserons ce fichier ultérieurement pour vérifier les certificats signés par l'autorité de certification intermédiaire.

```
┌──(root💀 kali)-[~/ca]
└─# cat intermediate/certs/intermediate.cert.pem \
    certs/ca.cert.pem > intermediate/certs/ca-chain.cert.pem

┌──(root💀 kali)-[~/ca]
└─# chmod 444 intermediate/certs/ca-chain.cert.pem
```

4. Signer les certificats serveur et client

Nous signerons les certificats à l'aide de notre autorité de certification intermédiaire. Vous pouvez utiliser ces certificats signés dans diverses situations, par exemple pour sécuriser les connexions à un serveur Web ou pour authentifier les clients qui se connectent à un service.

4.1. Créer une clé

Nos paires racine et intermédiaire sont de 4096 bits. Certificats serveur et client expirent normalement après un an, nous pouvons donc utiliser en toute sécurité 2048 bits à la place.

Si vous créez une paire cryptographique à utiliser avec un serveur Web (par exemple, Apache), vous devrez entrer ce mot de passe chaque fois que vous redémarrez le Web serveur. Vous pouvez omettre l'option permettant de créer une clé sans mot de passe.-aes256

```
┌──(root💀 kali)-[~/ca]
└─# openssl genrsa -aes256 \
      -out intermediate/private/www.example.com.key.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....................................................................+++++
.....................................................................................................................................+++++
e is 65537 (0×010001)
Enter pass phrase for intermediate/private/www.example.com.key.pem:
Verifying - Enter pass phrase for intermediate/private/www.example.com.key.pem:

┌──(root💀 kali)-[~/ca]
└─# chmod 400 intermediate/private/www.example.com.key.pem

┌──(root💀 kali)-[~/ca]
└─#
```

4.2. Créer un certificat

Utilisez la clé privée pour créer une demande de signature de certificat (CSR). La RSE les détails n'ont pas besoin de correspondre à l'autorité de certification intermédiaire. Pour les certificats de serveur, le nom commun doit être un **nom** de domaine complet (par exemple,), alors que pour les certificats clients, il peut s'agir de n'importe quel identifiant unique (par exemple, un e-mail adresse). Notez que le **nom commun** ne peut pas être identique à votre racine. Ou certificat intermédiaire.www.example.com

```
┌──(root💀 kali)-[~/ca]
└─# openssl req -config intermediate/openssl.cnf \
      -key intermediate/private/www.example.com.key.pem \
      -new -sha256 -out intermediate/csr/www.example.com.csr.pem
Enter pass phrase for intermediate/private/www.example.com.key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name [England]:California
Locality Name []:Mountain View
Organization Name [Alice Ltd]:Alice Ltd
Organizational Unit Name []:Alice Ltd Web Services
Common Name []:www.example.com
Email Address []:

┌──(root💀 kali)-[~/ca]
└─#
```


Pour créer un certificat, utilisez l'autorité de certification intermédiaire pour signer la demande de signature de certificat. Si l'Le certificat va être utilisé sur un serveur, utilisez l'extension. Si le certificat doit être utilisé pour l'authentification des utilisateurs, utilisez l'extension. Les certificats ont généralement une validité d'un an, bien qu'un CA accorde généralement quelques jours supplémentaires pour plus de commodité.server_certusr_cert

```
┌──(root💀kali)-[~/ca]
└─# openssl ca -config intermediate/openssl.cnf \
      -extensions server_cert -days 375 -notext -md sha256 \
      -in intermediate/csr/www.example.com.csr.pem \
      -out intermediate/certs/www.example.com.cert.pem
Using configuration from intermediate/openssl.cnf
Enter pass phrase for /root/ca/intermediate/private/intermediate.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Apr  6 22:57:07 2023 GMT
            Not After : Apr 15 22:57:07 2024 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = California
            localityName              = Mountain View
            organizationName          = Alice Ltd
            organizationalUnitName    = Alice Ltd Web Services
            commonName                = www.example.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
            Netscape Comment:
                OpenSSL Generated Server Certificate
            X509v3 Subject Key Identifier:
                4D:4B:25:DE:5A:1A:30:F3:95:83:BE:C6:DD:F5:BB:30:EE:11:37:D3
            X509v3 Authority Key Identifier:
                keyid:49:B9:5E:4D:81:25:6E:83:10:F1:8E:68:38:E4:59:3E:8C:B9:0E:EE
                DirName:/C=GB/ST=England/O=Alice Ltd/OU=Alice Ltd Certificate Authority/CN=Alice Ltd Root CA
                serial:10:00

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
```

```
┌──(root💀kali)-[~/ca]
└─# chmod 444 intermediate/certs/www.example.com.cert.pem

┌──(root💀kali)-[~/ca]
└─#
```

4.3. Vérifier le certificat

```
┌──(root💀kali)-[~/ca]
└─# openssl x509 -noout -text \
      -in intermediate/certs/www.example.com.cert.pem
```

L'émetteur est l'autorité de certification intermédiaire. **L'objet** fait référence au certificat lui-même.

```
┌──(root💀kali)-[~/ca]
└─# openssl x509 -noout -text \
     -in intermediate/certs/www.example.com.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = GB, ST = England, O = Alice Ltd, OU = Alice Ltd Certificate Authority, CN = Alice Ltd Intermediate CA
        Validity
            Not Before: Apr  6 22:57:07 2023 GMT
            Not After : Apr 15 22:57:07 2024 GMT
        Subject: C = US, ST = California, L = Mountain View, O = Alice Ltd, OU = Alice Ltd Web Services, CN = www.example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:d1:25:db:4a:d8:39:6a:43:d2:db:6b:50:06:b0:
                    25:05:84:9b:43:32:9b:ab:cd:d8:51:d1:95:0e:c3:
                    3d:dc:10:9d:0e:d1:92:2c:d7:08:78:8f:3e:11:cd:
                    f9:7f:46:ba:98:ee:14:d2:00:19:a0:bc:2b:28:94:
                    42:c0:0e:cc:95:4b:27:1f:03:ce:51:12:5e:be:55:
                    f3:37:61:ee:9f:c8:98:83:9b:6e:5d:fb:96:73:ac:
                    0d:b2:82:39:a8:00:bf:0d:97:fb:1b:63:5b:0f:f2:
                    9a:e0:20:8b:64:ef:95:44:5c:36:71:a8:d2:13:2a:
                    45:2a:fc:5a:b5:a1:39:0d:b1:3f:59:2f:97:b7:85:
                    b7:8a:da:5d:ee:ee:f3:90:46:4f:b8:c2:da:0f:ef:
                    e2:0f:42:e5:fb:b3:98:74:f3:b1:3e:8c:50:39:84:
                    ca:6c:40:65:b4:8d:f0:0c:75:d8:a4:ba:9b:d8:3b:
                    2d:8c:28:fe:61:b0:35:65:36:55:da:cf:06:c4:39:
                    3e:20:78:21:fb:33:f1:93:d8:4c:a7:a2:97:ed:1d:
                    6b:b3:ad:7d:c7:cf:d1:19:b1:62:5a:9e:35:f0:64:
                    b7:63:43:e7:d5:3e:98:af:c6:ce:54:f3:da:28:e5:
                    68:73:1d:b3:83:df:d6:07:20:8d:90:59:ff:27:7f:
                    35:6d
                Exponent: 65537 (0x10001)
```

La sortie affichera également les **extensions X509v3**. Lors de la création de l'icône, vous avez utilisé l'extension ou. Le Les options de la section Configuration correspondante seront reflétées dans la sortie.server_certusr_cert

```
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
            Netscape Comment:
                OpenSSL Generated Server Certificate
            X509v3 Subject Key Identifier:
                4D:4B:25:DE:5A:1A:30:F3:95:83:BE:C6:DD:F5:BB:30:EE:11:37:D3
            X509v3 Authority Key Identifier:
                keyid:49:B9:5E:4D:81:25:6E:83:10:F1:8E:68:38:E4:59:3E:8C:B9:0E:EE
                DirName:/C=GB/ST=England/O=Alice Ltd/OU=Alice Ltd Certificate Authority/CN=Alice Ltd Root CA
                serial:10:00

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
         0f:c2:b9:52:65:0c:34:52:41:c4:ab:16:dc:de:be:fe:06:87:
         4a:8e:2e:50:ac:60:bc:2c:68:4a:73:7c:34:d1:39:b8:d8:94:
         0e:25:7d:1c:20:bb:29:c6:21:e8:30:56:54:f1:1e:9b:9f:b7:
         90:9a:ec:a2:80:d5:28:30:cd:3d:dc:f0:5f:46:3e:fd:ed:7b:
         ee:90:d2:fc:94:39:a1:97:50:9d:fa:ee:6c:cf:b5:c4:d0:fa:
         c3:47:e1:da:28:ea:4d:6f:98:f3:f2:81:09:49:06:77:bc:a5:
         25:68:e6:8f:2b:07:9e:4d:de:d4:7b:54:91:68:df:d5:44:44:
         a3:49:a4:a7:74:36:1f:09:bb:3d:5a:38:d9:9f:7f:30:b6:ba:
         cd:38:bd:e1:b3:96:6b:a7:a5:07:b5:93:b2:be:de:03:ad:22:
         85:a5:be:35:cf:01:97:c9:bc:f2:aa:85:61:6e:d0:36:fa:bd:
         30:a0:01:b0:46:f7:f4:32:e5:9a:60:ce:0c:fd:e0:d7:eb:98:
         8d:39:68:af:90:82:7d:0e:64:48:2e:7b:e6:63:19:f6:d9:f2:
         44:22:2e:f4:8f:81:dd:c6:17:cf:5c:a6:b1:26:ab:cb:9c:9b:
         b8:28:c9:61:d7:53:48:a9:b4:3a:3c:69:96:cb:00:ad:72:6b:
         ba:ff:a9:47:32:d7:95:c3:30:19:4e:97:3e:23:b3:81:21:52:
         2a:15:0b:39:42:d9:b0:0d:20:42:ff:de:af:5c:3f:b4:93:0f:
         13:4e:ce:82:d5:dc:8b:2b:cd:df:18:31:71:1e:c1:19:34:d8:
```


Utilisez le fichier de chaîne de certificats d'autorité de certification que nous avons créé précédemment () pour Vérifiez que le nouveau certificat dispose d'une chaîne de confiance valide.ca-chain.cert.pem

```
┌──(root💀kali)-[~/ca]
└─# openssl verify -CAfile intermediate/certs/ca-chain.cert.pem \
      intermediate/certs/www.example.com.cert.pem
intermediate/certs/www.example.com.cert.pem: OK
```

4.4. Déployer le certificat

Vous pouvez désormais déployer votre nouveau certificat sur un serveur ou distribuer le à un client. Lors du déploiement sur une application serveur (par exemple, Apache), Vous devez rendre les fichiers suivants disponibles :

- ca-chain.cert.pem
- www.example.com.key.pem
- www.example.com.cert.pem

Si vous signez un CSR d'un tiers, vous n'avez pas accès à son clé privée afin que vous n'ayez qu'à leur rendre le fichier de chaîne () et le certificat (). ca-chain.cert.pemwww.example.com.cert.pem

5. Liste de révocation de certificats

Une liste de révocation de certificats (CRL) fournit une liste de certificats qui ont été révoqués. Une application cliente, telle qu'un navigateur Web, peut utiliser une liste de révocation de certificats pour Vérifiez l'authenticité d'un serveur. Une application serveur, telle qu'Apache ou OpenVPN, peut utiliser une liste de révocation de certificats pour refuser l'accès aux clients qui ne sont plus approuvés.

Publiez la liste de révocation de certificats à un emplacement accessible au public (par exemple). Les tiers peuvent récupérer la liste de révocation de certificats à partir de cet emplacement pour vérifier si les certificats sur lesquels ils s'appuient ont été Révoqué.http://example.com/intermediate.crl.pem

5.1. Préparer le fichier de configuration

Lorsqu'une autorité de certification signe un certificat, elle encode normalement l'Emplacement de la liste de révocation de certificats dans le certificat. Ajouter à la les sections appropriées. Dans notre cas, ajoutez-le à la section.crlDistributionPoints[server_cert]

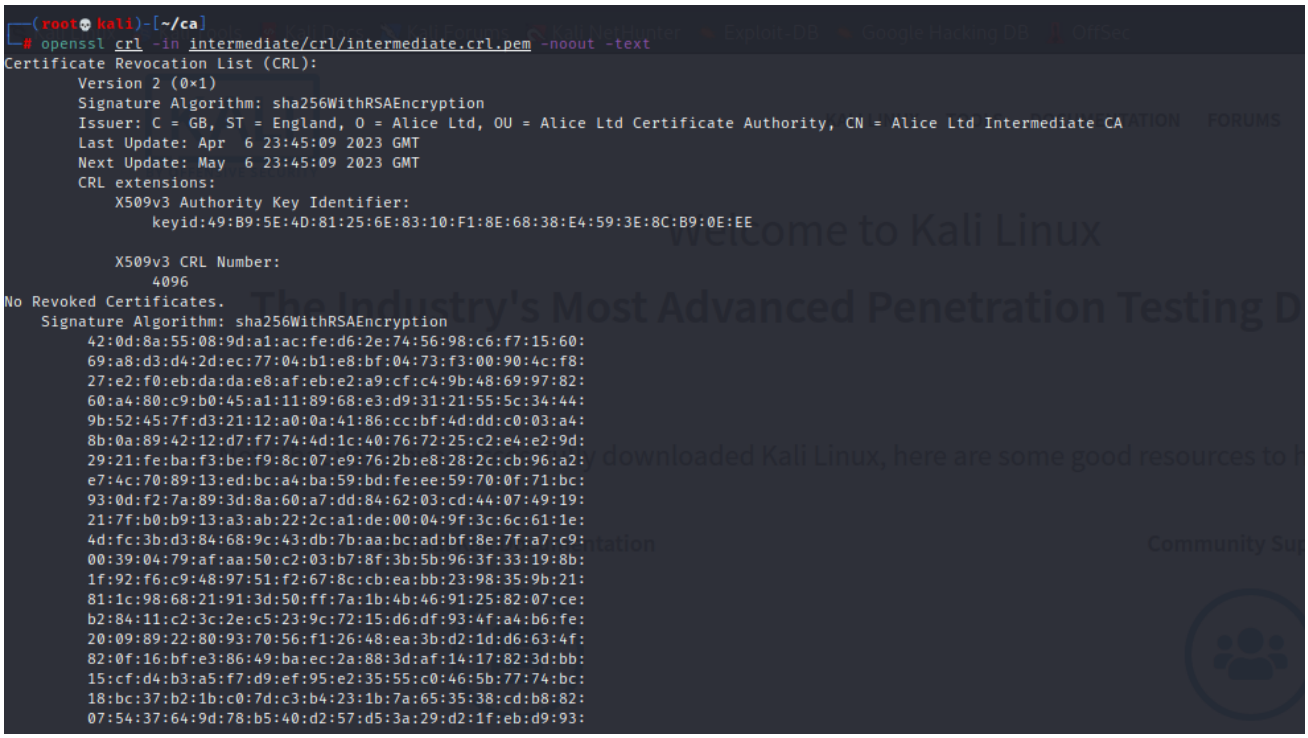
```
┌──(root💀kali)-[~/ca]
└─# nano openssl.cnf
```

```
File  Actions  Edit  View  Help
  GNU nano 5.9                                                openssl.cnf
basicConstraints = CA:FALSE
nsCertType = client, email
nsComment = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, emailProtection

[ server_cert ]
# Extensions for server certificates (`man x509v3_config`).
basicConstraints = CA:FALSE
nsCertType = server
nsComment = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
crlDistributionPoints = URI:http://example.com/path/to/crl.crl

[ crl_ext ]
# Extension for CRLs (`man x509v3_config`).
authorityKeyIdentifier=keyid:always

[ ocsp ]
# Extension for OCSP signing certificates (`man ocsp`).
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, digitalSignature
extendedKeyUsage = critical, OCSPSigning
```

5.2. Créer la liste de révocation de certificats

```
┌──(root💀kali)-[~/ca]
└─# openssl ca -config intermediate/openssl.cnf \
      -gencrl -out intermediate/crl/intermediate.crl.pem
Using configuration from intermediate/openssl.cnf
Enter pass phrase for /root/ca/intermediate/private/intermediate.key.pem:

┌──(root💀kali)-[~/ca]
└─#
```

Vous pouvez vérifier le contenu de la liste de révocation de certificats avec l'outil. crl

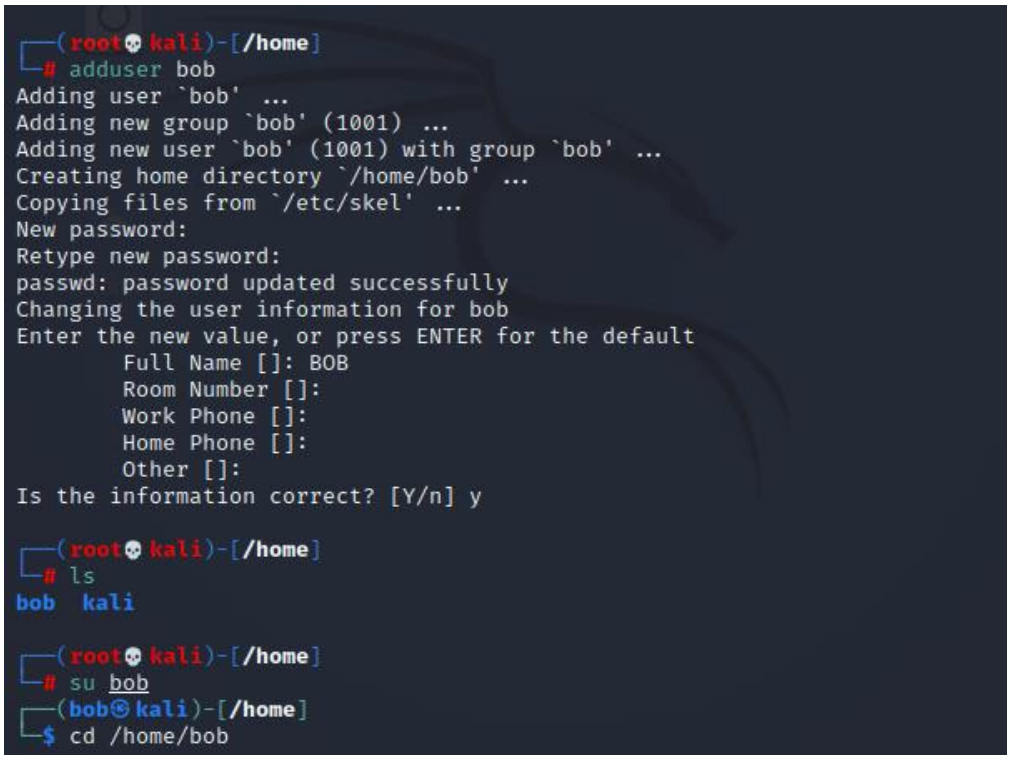


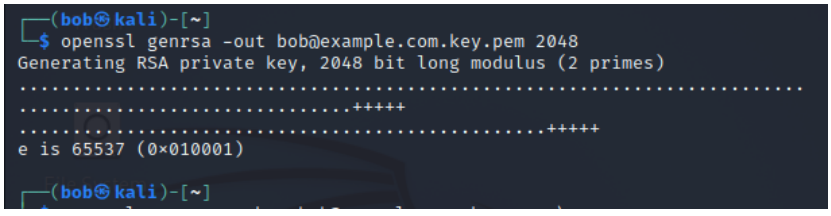
Aucun certificat n'a encore été révoqué, la sortie indiquera donc. No Revoked Certificates

5.3. Révoquer un certificat

Passons en revue un exemple. Alice exécute le serveur Web Apache et dispose d'un Dossier privé de photos de chatons mignons qui font fondre le cœur. Alice veut lui accorder ami, Bob, accès à cette collection.

Bob crée une clé privée et une demande de signature de certificat (CSR).





```
┌──(bob㉿kali)-[~]
└─$ openssl req -new -key bob@example.com.key.pem \
      -out bob@example.com.csr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a D
N.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Francisco
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Bob Ltd
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:bob@example.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

┌──(bob㉿kali)-[~]
└─$
```

Bob envoie son CSR à Alice, qui le signe ensuite.

```
┌──(root㉿kali)-[~/ca]
└─# openssl ca -config intermediate/openssl.cnf \
      -extensions usr_cert -notext -md sha256 \
      -in /home/bob/bob@example.com.csr.pem \
      -out intermediate/certs/bob@example.com.cert.pem
Using configuration from intermediate/openssl.cnf
Enter pass phrase for /root/ca/intermediate/private/intermediate.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Apr 10 20:03:08 2023 GMT
            Not After : Apr 19 20:03:08 2024 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = California
            localityName              = San Francisco
            organizationName          = Bob Ltd
            commonName                = bob@example.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            Netscape Comment:
                OpenSSL Generated Client Certificate
            X509v3 Subject Key Identifier:
                86:DE:99:FD:DD:2E:30:2F:74:07:9E:9F:27:51:E1:22:41:41:C3:1
7
            X509v3 Authority Key Identifier:
                keyid:CC:A0:F0:A5:C1:2B:10:2A:4A:87:60:EE:E8:04:82:2B:9C:9
C:5B:9D
```

```
7
            X509v3 Authority Key Identifier:
                keyid:CC:A0:F0:A5:C1:2B:10:2A:4A:87:60:EE:E8:04:82:2B:9C:9
C:5B:9D

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
Certificate is to be certified until Apr 19 20:03:08 2024 GMT (375 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

┌──(root💀kali)-[~/ca]
└─#
```

Alice vérifie que le certificat est valide :

```
┌──(root💀kali)-[~/ca]
└─# openssl verify -CAfile intermediate/certs/ca-chain.cert.pem \
      intermediate/certs/bob@example.com.cert.pem
intermediate/certs/bob@example.com.cert.pem: OK

┌──(root💀kali)-[~/ca]
└─#
```

Alice envoie à Bob le certificat signé. Bob installe le certificat dans son site Web navigateur et est maintenant en mesure d'accéder aux photos de chaton d'Alice.

Malheureusement, il s'avère que Bob se comporte mal. Bob a posté le chaton d'Alice photos à Hacker News, affirmant qu'elles sont les siennes et gagnant énormément popularité. Alice le découvre et doit révoquer son accès immédiatement.


```
┌──(root💀kali)-[~/ca]
└─# openssl ca -config intermediate/openssl.cnf \
      -revoke intermediate/certs/bob@example.com.cert.pem
Using configuration from intermediate/openssl.cnf
Enter pass phrase for /root/ca/intermediate/private/intermediate.key.pem:
Revoking Certificate 1001.
Data Base Updated

┌──(root💀kali)-[~/ca]
└─#
```

Après avoir révoqué le certificat de Bob, Alice doit recréer la liste de révocation de certificats.

```
┌──(root💀kali)-[~/ca]
└─# openssl crl -in intermediate/crl/intermediate.crl.pem -noout -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = GB, ST = England, O = Alice Ltd, OU = Alice Ltd Certif
icate Authority, CN = Alice Ltd Intermediate CA
        Last Update: Apr 10 17:24:58 2023 GMT
        Next Update: May 10 17:24:58 2023 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:CC:A0:F0:A5:C1:2B:10:2A:4A:87:60:EE:E8:04:82:2B:9C:9
C:5B:9D

            X509v3 CRL Number:
                4096
No Revoked Certificates.
    Signature Algorithm: sha256WithRSAEncryption
         55:95:9a:24:02:e5:1f:8c:a1:37:61:3b:10:c3:2a:0e:83:ee:
         51:74:7c:36:7f:aa:0a:3b:3e:e1:c2:30:19:35:0f:7a:1d:f3:
         b1:aa:6a:d7:97:42:56:89:6a:33:16:71:9a:c6:30:95:cf:87:
         cb:66:91:ac:21:5f:1f:d3:5d:8f:fd:92:f1:82:74:04:08:af:
         71:73:7f:11:c0:40:50:a3:86:bc:fe:3d:04:f5:a1:50:21:4d:
         8f:6e:83:ff:86:ac:2d:ed:67:bb:6b:3a:48:eb:84:ca:8b:0c:
         85:48:c2:ba:dc:dd:da:06:fe:70:41:1a:60:b7:75:74:cb:02:
         70:8e:fe:ba:cd:f5:0c:7c:a6:0f:94:ec:1d:ab:3d:e5:e8:aa:
         72:c5:30:36:e2:bd:a1:e2:2e:13:3e:c9:ae:b9:55:86:89:6e:
         12:b0:25:67:ae:10:4a:59:f3:80:53:31:8b:be:43:40:1a:6a:
         4c:8f:48:9e:05:8f:87:a3:d5:0c:c7:e7:4c:84:4c:11:ae:93:
         b7:20:3a:77:0a:ad:32:4f:7d:87:41:f9:f1:fe:e1:b8:ae:9d:
         5e:ea:72:20:c0:d4:4f:c4:c2:20:c7:7b:98:7e:c7:86:06:d2:
         b6:b9:d9:17:22:cc:5a:89:a7:ec:26:36:ff:bb:f1:6c:75:e2:
         53:f0:a6:7a:f1:5a:51:fe:0f:75:0c:28:e5:55:66:b8:c3:7f:
         6b:09:4b:93:e7:f0:cc:87:c4:d0:88:1f:2c:8e:af:5f:21:3d:
         bb:2c:e5:1c:12:b4:96:8b:df:24:4f:fe:61:27:b2:66:fe:17:
```

5.4. Utiliser le côté serveur de la liste de révocation de certificats

Pour les certificats clients, il s'agit généralement d'une application côté serveur (par exemple, Apache) C'est faire la vérification. Cette application doit avoir un accès local à la CRL.

Dans le cas d'Alice, elle peut ajouter la directive à son Apache et copiez la liste de révocation de certificats sur son serveur Web. La prochaine fois que Bob se connecte au serveur web, Apache vérifiera son certificat client par rapport au CRL et refuser l'accès.SSLCARevocationPath

De même, OpenVPN a une directive afin qu'il puisse bloquer les clients dont le certificat a été révoqué.crl-verify

5.5. Utiliser le côté client de la liste de révocation de certificats

Pour les certificats de serveur, il s'agit généralement d'une application côté client (par exemple, un site Web navigateur) qui effectue la vérification. Cette application doit avoir une télécommande l'accès aux LCR.

Si un certificat a été signé avec une extension qui inclut, une application côté client peut lire ces informations et récupérez la liste de révocation de certificats à partir de l'emplacement spécifié.crlDistributionPoints

Les points de distribution de la liste de révocation de certificats sont visibles dans les détails du certificat **X509v3**.

6. Protocole d'état du certificat en ligne

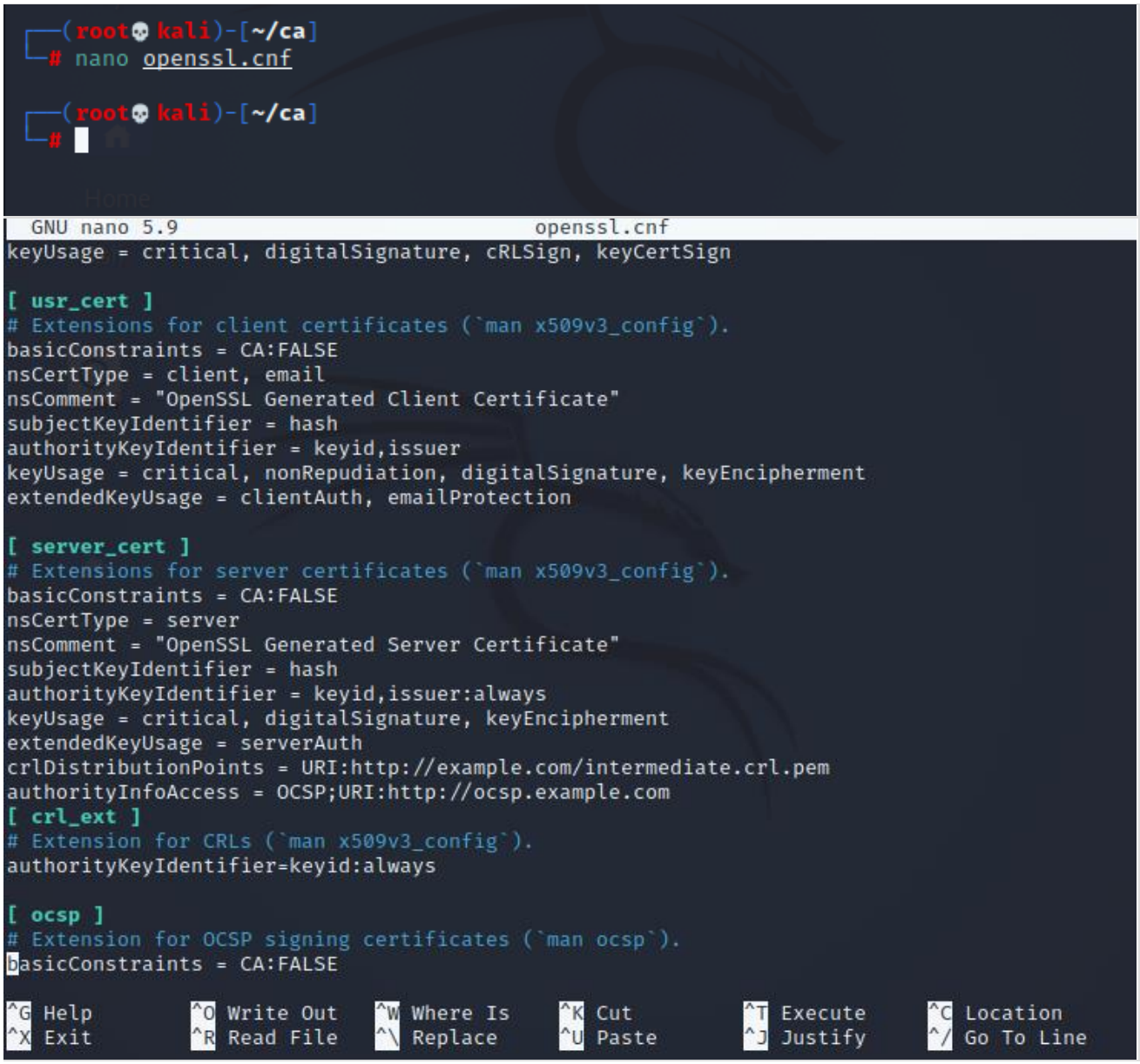
Le protocole OCSP (Online Certificate Status Protocol) a été créé comme alternative aux *listes de révocation de certificats* (CRL). Semblable aux listes de révocation de certificats, OCSP permet à une partie requérante (par exemple, un navigateur Web) de Déterminer l'état de révocation d'un certificat.

Lorsqu'une autorité de certification signe un certificat, elle inclut généralement un serveur OCSP adresse (par exemple) dans le certificat. Il en va de même dans les à utiliser pour les listes de révocation de certificats. http://ocsp.example.comcrlDistributionPoints

Par exemple, lorsqu'un navigateur Web est présenté avec un certificat de serveur, il enverra une requête à l'adresse du serveur OCSP spécifiée dans le certificat. À cette adresse, un répondant OCSP écoute les requêtes et répond avec le État de révocation du certificat.

6.1. Préparer le fichier de configuration

Pour utiliser OCSP, l'autorité de certification doit coder l'emplacement du serveur OCSP dans les certificats qu'il signe. Utilisez l'option dans le , ce qui, dans notre cas, signifie l'article.authorityInfoAccess[server_cert]



6.2. Créer la paire OCSP

Le répondeur OCSP a besoin d'une paire cryptographique pour signer la réponse qui il envoie à la partie requérante. La paire cryptographique OCSP doit être signée par la même autorité de certification qui a signé le certificat en cours de vérification.

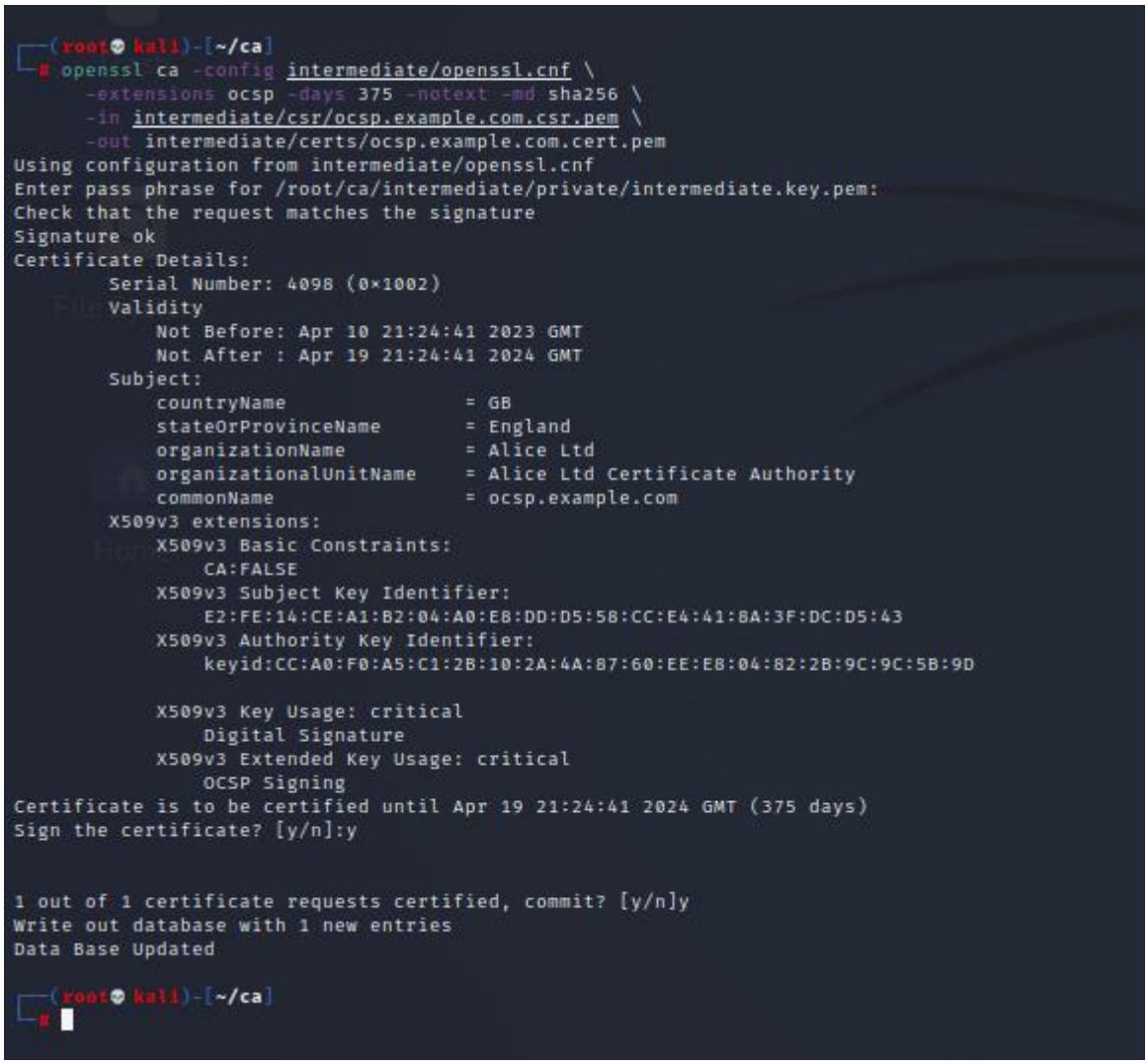
Créez une clé privée et chiffrez-la avec le chiffrement AES-256.

```
┌──(root💀 kali)-[~/ca]
└─# openssl genrsa -aes256 \
      -out intermediate/private/ocsp.example.com.key.pem 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................++++
.....................................++++
e is 65537 (0×010001)
Enter pass phrase for intermediate/private/ocsp.example.com.key.pem:
Verifying - Enter pass phrase for intermediate/private/ocsp.example.com.key.pem:

┌──(root💀 kali)-[~/ca]
└─#
```

Créez une demande de signature de certificat (CSR). Les détails doivent généralement correspondre celles de l'autorité de certification signataire. Le **nom usuel**, cependant, doit être un nom de domaine.

```
┌──(root💀 kali)-[~/ca]
└─# openssl req -config intermediate/openssl.cnf -new -sha256 \
      -key intermediate/private/ocsp.example.com.key.pem \
      -out intermediate/csr/ocsp.example.com.csr.pem
Enter pass phrase for intermediate/private/ocsp.example.com.key.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:GB
State or Province Name [England]:England
Locality Name []:
Organization Name [Alice Ltd]:Alice Ltd
Organizational Unit Name []:Alice Ltd Certificate Authority
Common Name []:ocsp.example.com
Email Address []:

┌──(root💀 kali)-[~/ca]
└─#
```


Signez la CSR avec l'autorité de certification intermédiaire.



Vérifiez que le certificat possède les **extensions X509v3 correctes**.

```
┌──(root㉿kali)-[~/ca]
└─# openssl x509 -noout -text \
    -in intermediate/certs/ocsp.example.com.cert.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4098 (0x1002)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = GB, ST = England, O = Alice Ltd, OU = Alice Ltd Certificate Authority, CN = Alice Ltd Intermediate CA
        Validity
            Not Before: Apr 10 21:24:41 2023 GMT
            Not After : Apr 19 21:24:41 2024 GMT
        Subject: C = GB, ST = England, O = Alice Ltd, OU = Alice Ltd Certificate Authority, CN = ocsp.example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:df:5a:8c:e6:56:13:75:09:93:c8:55:5b:69:4f:
                    bd:c9:26:94:38:3e:28:a6:73:e2:c7:33:c9:a7:03:
                    a1:97:06:3a:9f:e2:d3:bd:04:26:cc:87:32:db:01:
                    7e:36:5f:99:ff:9e:f4:28:e0:b3:af:91:56:3f:6f:
                    08:fe:fb:a4:2d:da:b6:39:3f:f1:b9:79:2a:18:df:
                    b5:21:8e:7f:89:70:a4:2f:9d:9c:66:80:a2:26:ed:
                    e1:98:8c:c0:3d:af:94:2f:0d:ed:fd:a7:ad:9a:a1:
                    cb:a3:58:c7:0e:0b:7f:95:b9:dc:e3:07:3b:1b:b9:
                    95:ce:3f:53:89:61:b4:82:54:c4:cc:71:f7:d3:f7:
                    ce:12:8c:af:5e:51:6a:84:53:24:ab:28:6f:80:4b:
                    44:8d:77:aa:11:1b:3f:35:e0:d3:c2:1c:80:b7:86:
                    0b:30:6e:0f:8f:2b:ba:06:d6:03:d4:b5:b2:eb:4a:
                    48:2d:32:2d:5b:78:95:3f:45:6f:43:f6:ea:44:a4:
                    63:77:26:9c:c7:ed:6d:53:4b:73:40:c9:7a:10:4d:
                    7f:05:25:93:90:ba:71:c3:be:de:53:05:3b:f9:fb:
                    7a:b4:56:fc:ef:c5:00:04:34:81:23:4e:4d:08:2c:
                    7b:e6:cd:69:e1:a8:f4:9d:0d:48:0e:69:c0:07:35:
                    0d:5f:05:fb:43:1c:44:50:11:e0:d2:fb:ab:54:4c:
                    e9:6b:07:94:ef:9b:bd:c2:35:29:ec:c4:9b:a9:cf:
                    44:53:2b:1f:9c:fd:74:8a:fa:a9:6d:b7:d7:1e:7c:
                    9f:fa:15:43:5b:15:38:80:72:72:23:b6:f1:d2:e9:
                    62:e0:05:93:e7:6e:19:8a:77:bb:05:f9:38:9a:d0:
                    bf:9d:fc:06:07:88:eb:71:56:4a:61:46:b7:de:3e:
                    2a:cd:15:f8:ae:b0:67:47:b5:9e:58:3b:ec:e4:4e:
                    be:1b:94:2a:a7:8c:ad:75:dd:32:bc:72:b6:86:0b:
                    da:91:7c:9f:aa:c5:27:55:d6:8e:b6:0c:19:f9:6d:
                    00:3f:fc:c6:a1:4e:35:92:97:ae:c2:e5:e9:9e:5e:
                    b0:f8:fa:d3:3e:12:17:26:48:d6:15:73:6a:ec:c8:
                    c8:f4:54:5d:1a:e3:5f:fc:b4:01:7f:95:1a:88:77:
                ad:02:c9
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                E2:FE:14:CE:A1:B2:04:A0:E8:DD:D5:58:CC:E4:41:8A:3F:DC:D5:43
            X509v3 Authority Key Identifier:
                keyid:CC:A0:F0:A5:C1:2B:10:2A:4A:87:60:EE:E8:04:82:2B:9C:9C:5B:9D

            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage: critical
                OCSP Signing
    Signature Algorithm: sha256WithRSAEncryption
         84:9e:7c:c0:28:a2:f5:2f:c0:8a:ba:3a:91:35:71:85:b9:71:
         86:c1:01:9c:57:24:cd:74:28:ee:50:01:22:8c:91:ac:cd:cb:
         b0:03:e0:9e:d8:d3:40:89:54:2f:16:63:9b:b7:36:23:27:79:
         51:4a:99:21:fa:cc:70:dd:81:79:c3:23:b8:84:15:d3:db:b2:
         1f:8b:c6:a1:82:ea:64:8c:30:af:ea:b8:ad:20:0c:2b:e2:a0:
         83:2f:60:9d:49:ed:13:e7:3b:d0:2a:22:cb:50:bf:9d:cd:2c:
         88:b0:89:2b:8e:e3:b5:71:26:c0:0b:b4:d9:c5:dc:25:76:a4:
         4a:76:a1:c0:7d:1e:36:b6:6e:f6:fd:f9:1b:d5:f7:6e:af:96:
         ba:76:d6:a0:ec:81:56:ca:a9:52:1a:e1:46:88:be:55:49:ec:
         b5:b9:85:09:81:6f:5b:e0:03:97:da:be:8d:2f:28:f8:10:0d:
         00:a5:0d:8a:fb:fe:0e:4a:ec:d8:c0:5e:67:70:fd:0a:55:03:
         2c:ef:01:3c:4a:a1:ca:fc:3a:8d:e8:0d:7b:12:61:80:20:de:
         71:5e:6b:6e:73:b6:3f:9e:92:87:c2:24:8d:8d:da:d1:62:55:
         0f:06:87:fb:d4:82:11:da:aa:3b:2b:53:9b:3b:38:22:28:f6:
         fb:53:88:62:ae:31:c5:53:57:0c:60:3e:cb:60:62:59:2b:10:
         f6:2d:f7:a2:97:e3:a7:b1:62:50:15:e8:4f:c4:10:ab:0a:b9:
         ac:38:ae:77:82:bb:3c:b0:2c:4e:33:15:96:5e:39:5d:77:08:
         2a:7f:09:1d:35:bf:13:4e:bd:c6:84:a5:a2:4d:84:12:7e:5a:
         d4:ff:fc:84:99:24:d5:4e:77:f6:ef:6e:7f:c3:74:60:1d:ba:
         38:8f:bd:49:5c:d3:05:09:2a:36:61:77:7d:84:66:c2:ba:3f:
         6b:3f:dc:fa:f4:3c:74:09:0e:99:49:34:9c:cf:b7:a0:a2:3d:
         91:00:75:a2:cd:12:e8:e4:8f:e1:fa:bf:d5:c6:ac:e8:b8:96:
         5d:f6:a0:da:e7:9c:0c:f7:aa:2d:20:ef:7d:ac:f2:83:fe:23:
         32:f0:0f:b4:28:6f:a3:fb:8e:05:c7:92:09:5e:b3:5f:10:e6:
         32:5c:12:58:35:64:8f:07:e4:5b:88:7b:6b:af:95:84:d0:b6:
         5f:81:a2:61:44:c9:21:4d:a5:91:f9:83:31:7d:ba:28:c1:47:
         79:54:b2:cc:40:4a:94:01:c8:01:5d:a5:f2:62:fe:c9:4f:31:
         67:7d:21:f7:f9:19:de:e3:b2:83:0d:7e:44:a0:ef:82:1c:4e:
         fc:cb:f8:56:a1:95:1f:53
┌──(root㉿kali)-[~/ca]
```

6.3. Révoquer un certificat

L'outil OpenSSL peut agir en tant que répondeur OCSP, mais il n'est destiné qu'à pour les tests. Il existe des intervenants OCSP prêts pour la production, mais ceux-ci vont au-delà de la Portée du présent guide.ocsp

Créez un certificat de serveur à tester

```
┌──(root💀 kali)-[~/ca]
└─# openssl genrsa -out intermediate/private/test.examp
le.com.key.pem 2048
Generating RSA private key, 2048 bit long modulus (2 pr
imes)
.....................+++++
.+++++
e is 65537 (0×010001)

┌──(root💀 kali)-[~/ca]
└─# openssl req -config intermediate/openssl.cnf \
      -key intermediate/private/test.example.com.key.pe
m \
      -new -sha256 -out intermediate/csr/test.example.c
om.csr.pem
You are about to be asked to enter information that wil
l be incorporated
into your certificate request.
What you are about to enter is what is called a Disting
uished Name or a DN.
There are quite a few fields but you can leave some bla
nk
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:GB
State or Province Name [England]:England
Locality Name []:
Organization Name [Alice Ltd]:Alice Ltd
Organizational Unit Name []:
Common Name []:lll
Email Address []:

┌──(root💀 kali)-[~/ca]
```

```
┌──(root💀 kali)-[~/ca]
└─# openssl ca -config intermediate/openssl.cnf \
      -extensions server_cert -days 375 -notext -md sha
256 \
      -in intermediate/csr/test.example.com.csr.pem \
      -out intermediate/certs/test.example.com.cert.pem

Using configuration from intermediate/openssl.cnf
Enter pass phrase for /root/ca/intermediate/private/int
ermediate.key.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4099 (0x1003)
        Validity
            Not Before: Apr 10 21:33:35 2023 GMT
            Not After : Apr 19 21:33:35 2024 GMT
        Subject:
            countryName               = GB
            stateOrProvinceName       = England
            organizationName          = Alice Ltd
            commonName                = lll
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Server
            Netscape Comment:
                OpenSSL Generated Server Certificate
            X509v3 Subject Key Identifier:
                C4:A9:64:30:E8:30:A3:E2:DC:88:6F:53:A2:
1D:47:4F:B6:C2:48:9A
            X509v3 Authority Key Identifier:
                keyid:CC:A0:F0:A5:C1:2B:10:2A:4A:87:60:
EE:E8:04:82:2B:9C:9C:5B:9D
                DirName:/C=GB/ST=England/O=Alice Ltd/OU
=Alice Ltd Certificate Authority/CN=Alice Ltd Root CA
                serial:10:00

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
Certificate is to be certified until Apr 19 21:33:35 20
24 GMT (375 days)
```

```
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n
]y
Write out database with 1 new entries
Data Base Updated

┌──(root💀 kali)-[~/ca]
└─#
```

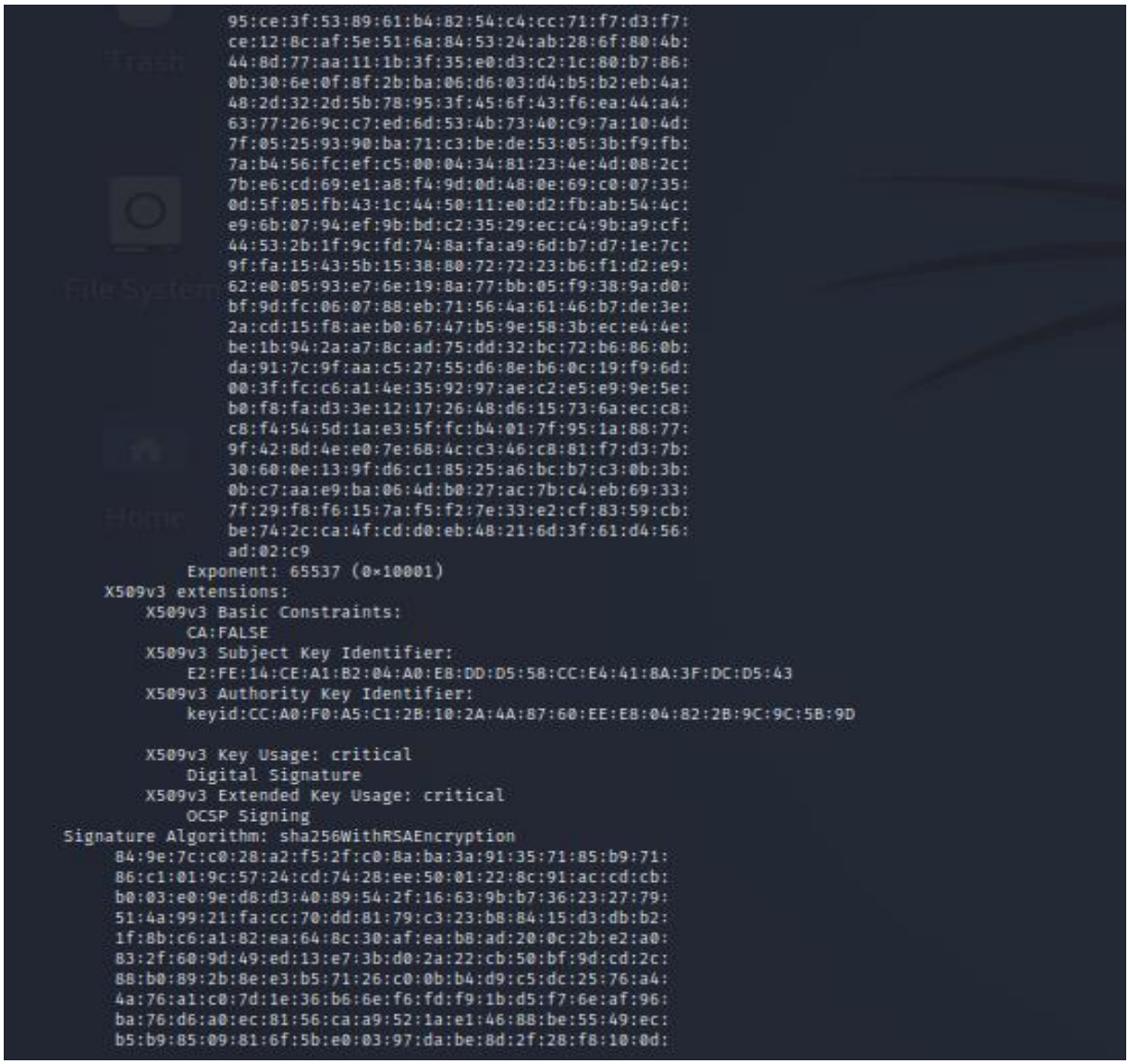
Exécutez le répondeur OCSP sur . Plutôt que de stocker l'état de révocation dans un fichier CRL séparé, le répondeur OCSP lit directement. Le La réponse est signée avec la paire cryptographique OCSP (à l'aide des options et).localhostindex.txt-rkey-rsigner

```
┌──(root💀 kali)-[~/ca]
└─# openssl ocsp -url http://127.0.0.1:2560 \
      -index intermediate/index.txt \
      -CA intermediate/certs/ca-chain.cert.pem \
      -rkey intermediate/private/ocsp.example.com.key.pem \
      -rsigner intermediate/certs/ocsp.example.com.cert.pem \
      -nrequest 1
Enter pass phrase for intermediate/private/ocsp.example.com.key.pem:
ocsp: waiting for OCSP client connections ...
```

Dans un autre terminal, envoyez une requête au répondeur OCSP. L'option Spécifie le certificat à interroger. -cert

```
┌──(root💀kali)-[~/ca]
└─# openssl ocsp -CAfile intermediate/certs/ca-chain.cert.pem \
      -url http://127.0.0.1:2560 -resp_text \
      -issuer intermediate/certs/intermediate.cert.pem \
      -cert intermediate/certs/test.example.com.cert.pem
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = GB, ST = England, O = Alice Ltd, OU = Alice Ltd Certificate Authority, CN = ocsp.example.com
    Produced At: Apr 11 23:00:21 2023 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: E35979B6D0A973EBE8AEDED75D8C27D67D2A0334
      Issuer Key Hash: CCA0F0A5C12B102A4A8760EEE804822B9C9C5B9D
      Serial Number: 1003
    Cert Status: good
    This Update: Apr 11 23:00:21 2023 GMT

    Response Extensions:
        OCSP Nonce:
            041014A37B64A7A3E2AE30FDE442FF203240
    Signature Algorithm: sha256WithRSAEncryption
         6f:7e:21:15:df:c0:9b:9c:84:e1:e5:74:52:a2:b3:82:4d:59:
         00:18:ea:53:33:74:7b:d2:58:39:54:ac:44:19:f8:9b:77:1d:
         7d:9a:3e:e7:c3:1c:9d:43:f1:5f:f0:48:62:27:35:03:af:29:
         61:05:25:fe:ee:81:2d:0c:be:db:ab:bd:fb:ec:a0:41:d4:62:
         e7:e2:2e:c0:66:37:28:2f:e5:97:c3:41:d8:51:14:0b:76:d7:
```

```
         e7:e2:2e:c0:66:37:28:2f:e5:97:c3:41:d8:51:14:0b:76:d7:
         97:d0:83:25:0d:a8:45:21:f6:06:d6:cb:92:c2:c7:40:f4:ac:
         d9:d5:fc:45:64:e7:0d:64:bf:5f:85:4f:eb:92:d9:48:3f:73:
         53:b7:7e:18:84:79:f6:da:ce:4f:74:ae:a2:8d:46:66:b3:0e:
         89:d1:68:d9:99:97:d2:e0:43:81:e9:68:e7:3f:5b:12:e9:8e:
         d8:aa:db:ea:eb:03:49:7d:85:af:0c:e3:cd:1d:ee:a2:73:f3:
         08:7a:4c:c6:3c:c0:93:d1:6d:d7:e1:7b:a5:41:0c:e4:59:b6:
         19:27:ee:e7:dc:22:48:cc:a3:69:f3:71:f5:d6:4b:7b:eb:8a:
         86:85:ed:46:f0:59:9c:c2:c3:ff:a8:b1:3d:20:ba:96:f9:c6:
         3b:a7:b3:55:30:f6:9d:6b:37:cb:61:8f:62:f8:cd:16:85:83:
         fc:91:64:79:4a:a1:d2:c2:39:80:41:25:69:c1:84:9f:39:06:
         d8:35:04:b7:29:23:c4:1c:1d:8c:da:aa:fe:fe:b3:30:5c:28:
         ef:cb:0e:41:c3:29:d5:82:e6:42:67:2d:cd:fd:05:05:04:fc:
         8d:86:db:f6:a7:a0:f0:e5:10:c8:19:4d:49:c2:fc:9b:0b:e8:
         e8:0d:c5:55:2d:3c:66:4e:f6:f7:f5:9c:09:3f:96:12:e8:31:
         cf:55:1e:7a:6d:f6:00:e5:e3:9f:aa:18:bb:4f:cf:03:42:a9:
         f8:6a:d3:6d:8a:99:ae:10:c4:56:fd:fa:c6:10:bd:5e:54:fc:
         c9:20:83:1d:d9:a2:71:c2:06:6b:85:19:68:f0:a5:07:37:16:
         0c:e6:6a:08:31:0a:75:c5:b9:05:6c:e7:ba:fd:00:22:88:6a:
         31:43:db:f4:ad:ff:46:6c:2e:06:26:61:8a:c4:bb:65:50:97:
         48:d7:20:ed:12:78:02:38:50:79:c4:25:c8:02:2b:0b:82:5f:
         a8:44:aa:bd:93:3e:9d:1c:2e:71:c1:74:c7:61:f0:4d:bf:4a:
         19:f1:fc:f6:92:d9:7e:73:fe:2e:c4:6e:01:1e:07:69:29:50:
         e1:a6:f5:54:da:e9:6e:a5:58:56:7d:91:23:93:1d:94:b0:9e:
         07:fd:66:fe:5f:7b:a2:c6
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4098 (0x1002)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, ST=England, O=Alice Ltd, OU=Alice Ltd Certificate Authority, CN=Alice Ltd Intermediate CA
        Validity
            Not Before: Apr 10 21:24:41 2023 GMT
            Not After : Apr 19 21:24:41 2024 GMT
        Subject: C=GB, ST=England, O=Alice Ltd, OU=Alice Ltd Certificate Authority, CN=ocsp.example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:df:5a:8c:e6:56:13:75:09:93:c8:55:5b:69:4f:
                    bd:c9:26:94:38:3e:28:a6:73:e2:c7:33:c9:a7:03:
                    a1:97:06:3a:9f:e2:d3:bd:04:26:cc:87:32:db:01:
                    7e:36:5f:99:ff:9e:f4:28:e0:b3:af:91:56:3f:6f:
                    08:fe:fb:a4:2d:da:b6:39:3f:f1:b9:79:2a:18:df:
                    b5:21:8e:7f:89:70:a4:2f:9d:9c:66:80:a2:26:ed:
                    e1:98:8c:c0:3d:af:94:2f:0d:ed:fd:a7:ad:9a:a1:
                    cb:a3:58:c7:0e:0b:7f:95:b9:dc:e3:07:3b:1b:b9:
                    95:ce:3f:53:89:61:b4:82:54:c4:cc:71:f7:d3:f7:
                    ce:12:8c:af:5e:51:6a:84:53:24:ab:28:6f:80:4b:
                    44:8d:77:aa:11:1b:3f:35:e0:d3:c2:1c:80:b7:86:
```



```
                95:ce:3f:53:89:61:b4:82:54:c4:cc:71:f7:d3:f7:
                ce:12:8c:af:5e:51:6a:84:53:24:ab:28:6f:80:4b:
                44:8d:77:aa:11:1b:3f:35:e0:d3:c2:1c:80:b7:86:
                0b:30:6e:0f:8f:2b:ba:06:d6:03:d4:b5:b2:eb:4a:
                48:2d:32:2d:5b:78:95:3f:45:6f:43:f6:ea:44:a4:
                63:77:26:9c:c7:ed:6d:53:4b:73:40:c9:7a:10:4d:
                7f:05:25:93:90:ba:71:c3:be:de:53:05:3b:f9:fb:
                7a:b4:56:fc:ef:c5:00:04:34:81:23:4e:4d:08:2c:
                7b:e6:cd:69:e1:a8:f4:9d:0d:48:0e:69:c0:07:35:
                0d:5f:05:fb:43:1c:44:50:11:e0:d2:fb:ab:54:4c:
                e9:6b:07:94:ef:9b:bd:c2:35:29:ec:c4:9b:a9:cf:
                44:53:2b:1f:9c:fd:74:8a:fa:a9:6d:b7:d7:1e:7c:
                9f:fa:15:43:5b:15:38:80:72:72:23:b6:f1:d2:e9:
                62:e0:05:93:e7:6e:19:8a:77:bb:05:f9:38:9a:d0:
                bf:9d:fc:06:07:88:eb:71:56:4a:61:46:b7:de:3e:
                2a:cd:15:f8:ae:b0:67:47:b5:9e:58:3b:ec:e4:4e:
                be:1b:94:2a:a7:8c:ad:75:dd:32:bc:72:b6:86:0b:
                da:91:7c:9f:aa:c5:27:55:d6:8e:b6:0c:19:f9:6d:
                00:3f:fc:c6:a1:4e:35:92:97:ae:c2:e5:e9:9e:5e:
                b0:f8:fa:d3:3e:12:17:26:48:d6:15:73:6a:ec:c8:
                c8:f4:54:5d:1a:e3:5f:fc:b4:01:7f:95:1a:88:77:
                9f:42:8d:4e:e0:7e:68:4c:c3:46:c8:81:f7:d3:7b:
                30:60:0e:13:9f:d6:c1:85:25:a6:bc:b7:c3:0b:3b:
                0b:c7:aa:e9:ba:06:4d:b0:27:ac:7b:c4:eb:69:33:
                7f:29:f8:f6:15:7a:f5:f2:7e:33:e2:cf:83:59:cb:
                be:74:2c:ca:4f:cd:d0:eb:48:21:6d:3f:61:d4:56:
                ad:02:c9
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                E2:FE:14:CE:A1:B2:04:A0:E8:DD:D5:58:CC:E4:41:8A:3F:DC:D5:43
            X509v3 Authority Key Identifier:
                keyid:CC:A0:F0:A5:C1:2B:10:2A:4A:B7:60:EE:E8:04:82:2B:9C:9C:5B:9D

            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Extended Key Usage: critical
                OCSP Signing
    Signature Algorithm: sha256WithRSAEncryption
         84:9e:7c:c0:28:a2:f5:2f:c0:8a:ba:3a:91:35:71:85:b9:71:
         86:c1:01:9c:57:24:cd:74:28:ee:50:01:22:8c:91:ac:cd:cb:
         b0:03:e0:9e:d8:d3:40:89:54:2f:16:63:9b:b7:36:23:27:79:
         51:4a:99:21:fa:cc:70:dd:81:79:c3:23:b8:84:15:d3:db:b2:
         1f:8b:c6:a1:82:ea:64:8c:30:af:ea:b8:ad:20:0c:2b:e2:a0:
         83:2f:60:9d:49:ed:13:e7:3b:d0:2a:22:cb:50:bf:9d:cd:2c:
         88:b0:89:2b:8e:e3:b5:71:26:c0:0b:b4:d9:c5:dc:25:76:a4:
         4a:76:a1:c0:7d:1e:36:b6:6e:f6:fd:f9:1b:d5:f7:6e:af:96:
         ba:76:d6:a0:ec:81:56:ca:a9:52:1a:e1:46:88:be:55:49:ec:
         b5:b9:85:09:81:6f:5b:e0:03:97:da:be:8d:2f:28:f8:10:0d:
```



```
        b5:b9:85:09:81:6f:5b:e0:03:97:da:be:8d:2f:28:f8:10:0d:
        00:a5:0d:8a:fb:fe:0e:4a:ec:d8:c0:5e:67:70:fd:0a:55:03:
        2c:ef:01:3c:4a:a1:ca:fc:3a:8d:e8:0d:7b:12:61:80:20:de:
        71:5e:6b:6e:73:b6:3f:9e:92:87:c2:24:8d:8d:da:d1:62:55:
        0f:06:87:fb:d4:82:11:da:aa:3b:2b:53:9b:3b:38:22:28:f6:
        fb:53:88:62:ae:31:c5:53:57:0c:60:3e:cb:60:62:59:2b:10:
        f6:2d:f7:a2:97:e3:a7:b1:62:50:15:e8:4f:c4:10:ab:0a:b9:
        ac:38:ae:77:82:bb:3c:b0:2c:4e:33:15:96:5e:39:5d:77:08:
        2a:7f:09:1d:35:bf:13:4e:bd:c6:84:a5:a2:4d:84:12:7e:5a:
        d4:ff:fc:84:99:24:d5:4e:77:f6:ef:6e:7f:c3:74:60:1d:ba:
        38:8f:bd:49:5c:d3:05:09:2a:36:61:77:7d:84:66:c2:ba:3f:
        6b:3f:dc:fa:f4:3c:74:09:0e:99:49:34:9c:cf:b7:a0:a2:3d:
        91:00:75:a2:cd:12:e8:e4:8f:e1:fa:bf:d5:c6:ac:e8:b8:96:
        5d:f6:a0:da:e7:9c:0c:f7:aa:2d:20:ef:7d:ac:f2:83:fe:23:
        32:f0:0f:b4:28:6f:a3:fb:8e:05:c7:92:09:5e:b3:5f:10:e6:
        32:5c:12:58:35:64:8f:07:e4:5b:88:7b:6b:af:95:84:d0:b6:
        5f:81:a2:61:44:c9:21:4d:a5:91:f9:83:31:7d:ba:28:c1:47:
        79:54:b2:cc:40:4a:94:01:c8:01:5d:a5:f2:62:fe:c9:4f:31:
        67:7d:21:f7:f9:19:de:e3:b2:83:0d:7e:44:a0:ef:82:1c:4e:
        fc:cb:f8:56:a1:95:1f:53
-----BEGIN CERTIFICATE-----
MIIF6zCCA9OgAwIBAgICEAIwDQYJKoZIhvcNAQELBQAwgYExCzAJBgNVBAYTAkdC
MRAwDgYDVQQIDAdFbmdsYW5kMRIwEAYDVQQKDAlBbGljZSBMdGQxKDAmBgNVBAsM
H0FsaWNlIEx0ZCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkxIjAgBgNVBAMMGUFsaWNl
IEx0ZCBJbnRlcm1lZGlhdGUgQ0EwHhcNMjMwNDEwMjEyNDQxWhcNMjQwNDE5MjEy
NDQxWjB4MQswCQYDVQQGEwJHQjEQMA4GA1UECAwHRW5nbGFuZDE5MBAGA1UECgwJ
QWxpY2UgTHRkMSgwJgYDVQQLDB9BbGljZSBMdGQgQ2VydGlmaWNhdGUgQXV0aG9y
aXR5MRkwFwYDVQQDDBBvY3NwLmV4YW1wbGUuY29tMIICIjANBgkqhkiG9w0BAQEF
AAOCAg8AMIICCgKCAgEA31qM5lYTdQmTyFVbaU+9y5aUOD4opnPixzPJpwOhlwY6
n+LTvQQmzIcy2wF+Nl+Z/570KOCzr5FWP28I/vukLdq2OT/xuXkqGN+1IY5/iXCk
L52cZoCiJu3hmIzAPa+ULw3t/aetmqHLo1jHDgt/lbnc4wc7G7mVzj9TiWG0glTE
zHH30/fOEoyvXlFqhFMkqyhvgEtEjXeqERs/NeDTwhyAt4YLMG4Pjyu6BtYD1LWy
60pILTItW3iVP0VvQ/bqRKRjdyacx+1tU0tzQMl6EE1/B5WTkLpxw77eUwU7+ft6
tFb878UABD5BI05NCCx75s1p4aj0nQ1IDmnABzUNXwX7QxxEUBHg0vurVEzpaweU
75u9wjUp7MSbqc9EUysfnP10ivqpbbfXHnyf+hVDWxU4gHJyI7bx0uli4AWT524Z
ine7Bfk4mtC/nfwGB4jrcVZKYUa33j4qzRX4rrBnR7WeWDvs5E6+G5Qqp4ytdd0y
vHK2hgvakXyfqsUnVdaOtgwZ+W0AP/zGoU41kpeuwuXpnl6w+PrTPhIXJkjWFXNq
7MjI9FRdGuNf/LQBf5UaiHefQo1O4H5oTMNGyIH303swYA4Tn9bBhSWmvLfDCzsL
x6rpugZNsCese8TraTN/Kfj2FXr18n4z4s+DWcu+dCzKT83Q60ghbT9h1FatAskC
AwEAAaN1MHMwCQYDVR0TBAIwADAdBgNVHQ4EFgQU4v4UzqGyBKDo3dVYzORBij/c
1UMwHwYDVR0jBBgwFoAUzKDwpcErECpKh2Du6ASCK5ycW50wDgYDVR0PAQH/BAQD
AgeAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMJMA0GCSqGSIb3DQEBCwUAA4ICAQCE
nnzAKKL1L8CKujqRNXGFuXGGwQGcVyTNdCjuUAEijJGszcuwA+Ce2NNAiVQvFmOb
tzYjJ3lR5pkh+sxw3YF5wyO4hBXT27IfiBahgupkjDCv6ritIAwr4qCDL2CdSe0T
5zvQKiLLUL+dzSyIsIkrjuO1cSbAC7TZxdwldqRKdqHAfR42tm72/fkb1fdur5a6
dtag7IFWyqlSGuFGiL5VSey1uYUJgW9b4AOX2r6NLyj4EA0ApQ2K+/4O5uzYwF5n
cP0KVQMs7wEBSqHK/DqN6A17EmGAIN5xXmtuc7Y/npKHWiSNjdrRYlUPBof71IIR
2qo7K1ObOzgiKPb7U4hirjHFU1cMYD7LYGJZKxD2Lfeil+OnsWJQFehPxBCrCrms
OK53grs8sCxOMxWWXjlddwgqfwkdNb8TTr3GhKWiTYQSflrU//yEm5TVTnf2725/
```

```
OK53grs8sCxOMxWWXjlddwgqfwkdNb8TTr3GhKWiTYQSflrU//yEm5TVTnf2725/
w3RgHbo4j71JXNMFCSo2YXd9hGbCuj9rP9z69Dx0CQ6ZSTScz7egoj2RAHWizRLo
5I/h+r/VxqzouJZd9qDa55wM96otIO99rPKD/iMy8A+0KG+j+44Fx5IJXrNfEOYy
XBJYNW5PB+RbiHtrr5WE0LZfgaJhRMkhTaWR+YMxfboowUd5VLLMQEqUAcgBXaXy
Yv7JTzFnfSH3+Rne47KDDX5EoO+CHE78y/hWoZUfUw==
-----END CERTIFICATE-----
Response verify OK
intermediate/certs/test.example.com.cert.pem: good
        This Update: Apr 11 23:00:21 2023 GMT

┌──(root💀kali)-[~/ca]
└─#
```

Le début de la sortie indique :

- Si une réponse positive a été reçue (OCSP Response Status)
- L'identité de l'intervenant (Responder Id)
- L'état de révocation du certificat (Cert Status)

Révoquez le certificat.

```
┌──(root💀kali)-[~/ca]
└─# openssl ca -config intermediate/openssl.cnf \
      -revoke intermediate/certs/test.example.com.cert.pem
Using configuration from intermediate/openssl.cnf
Enter pass phrase for /root/ca/intermediate/private/intermediate.key.pem:
Revoking Certificate 1003.
Data Base Updated
```

Comme précédemment, exécutez le répondeur OCSP et sur un autre terminal, envoyez une requête. Ceci temps, la sortie s'affiche et un fichier. Cert Status: revokedRevocation Time

```
┌──(root💀kali)-[~/ca]
└─# openssl ca -config intermediate/openssl.cnf \
      -revoke intermediate/certs/test.example.com.cert.pem
Using configuration from intermediate/openssl.cnf
Enter pass phrase for /root/ca/intermediate/private/intermediate.key.pem:
ERROR:Already revoked, serial number 1003

┌──(root💀kali)-[~/ca]
└─#
```