Protocolo en línea de estado de certificados

El título de esta sección corresponder a la expresión en inglés "Online Certificate Status Protocol".

El Online Certificate Status Protocol (OCSP) fue creado como una alternativa a las listas de revocación de certificados (CRL). Al igual que en las CRL, OCSP permite a una parte solicitante (por ejemplo, un navegador web) determinar el estado de revocación de un certificado.

Cuando una CA firma un certificado normalmente incluye en el certificado una dirección de servidor OCSP (por ejemplo, http://ocsp.example.com). Esto es similar en función a utilicar `crlDistributionPoints` en las CRL.

A modo de ejemplo, cuando un navegador web se presenta con un certificado de servidor, se enviará una consulta a la dirección del servidor OCSP especificado en el certificado. En esta dirección, un servidor OCSP escucha las preguntas y responde con el estado de revocación del certificado.

```
----------------------------------------------------------------
(¡!) Nota

Se recomienda el uso de OCSP cada vez que sea posible, aunque en
realidad sólo necesitará OCSP para certificados de sitios
web. Algunos navegadores web han desaprobado o eliminado el
soporte a las CRL.
----------------------------------------------------------------
```

Preparar el archivo de configuración.

Para utilizar OCSP, la CA debe codificar la ubicación del servidor OCSP en los certificados que firme. Utilice la opción `authorityInfoAccess` en las secciones correspondientes, que en nuestro caso significa la sección `[ server_cert ]`.

```
[ server_cert ]
# ... snipped ...
authorityInfoAccess = OCSP;URI:http://ocsp.example.com
```

Crear el par para OCSP

El servicio de respuesta OCSP requiere un par criptográfico para la firma de la respuesta que es enviada a la parte solicitante. El par criptográfico de OCSP deberá ser firmado por la misma CA que firmó el certificado en fase de comprobación.

Cree una clave privada y cífrela con un cifrado AES-256.

```
# cd /root/ca
# openssl genrsa -aes256 \
      -out intermediate/private/ocsp.example.com.key.pem 4096
```

Cree un certificado de solicitud de firma (CSR). Los detalles deben adaptarse generalmente a los de la CA que firma. El Common Name, sin embargo, debe ser un nombre de dominio completo.

```
# cd /root/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.key.pem: secretpassword
You are about to be asked to enter information that will be incorporated
into your certificate request.
-----
Country Name (2 letter code) [XX]:GB
State or Province Name []:England
Locality Name []:
Organization Name []:Alice Ltd
Organizational Unit Name []:Alice Ltd Certificate Authority
Common Name []:ocsp.example.com
Email Address []:
```

Firme la CSR con la CA intermedia.

```
# openssl ca -config intermediate/openssl.cnf \
      -extensions ocsp -days 375 -notext -md sha256 \
      -in intermediate/csr/ocsp.example.com.csr.pem \
      -out intermediate/certs/ocsp.example.com.cert.pem
```

Verifique que el certificado tiene las correctas **extensiones X509v3**.

```
# openssl x509 -noout -text \
      -in intermediate/certs/ocsp.example.com.cert.pem

    X509v3 Key Usage: critical
        Digital Signature
    X509v3 Extended Key Usage: critical
        OCSP Signing
```

Revocar un certificado

La herramienta ocsp de OpenSSL puede actuar como un servidor OCSP, pero sólo está destinada al ensayo. Existe un dispensador de respuestas OCSP preparado, pero su tratamiento está más allá del alcance de esta guía.

Cree un certificado de servidor para probar. Para ello, ejecútese lo siguiente y téngase en cuenta que al usar `req` el proceso demanda un **Common Name**, que debe ser provisto o si no fallará el proceso.

```
# cd /root/ca
# openssl genrsa -out intermediate/private/test.example.com.key.pem 2048
# openssl req -config intermediate/openssl.cnf \
      -key intermediate/private/test.example.com.key.pem \
      -new -sha256 -out intermediate/csr/test.example.com.csr.pem
# openssl ca -config intermediate/openssl.cnf \
      -extensions server_cert -days 375 -notext -md sha256 \
      -in intermediate/csr/test.example.com.csr.pem \
      -out intermediate/certs/test.example.com.cert.pem
```

Haga correr el dispensador de respuesta de OCSP en `localhost`. En lugar de almacenar el estado de revocación en un archivo separado CRL, OCSP lee directamente `index.txt`. La respuesta está firmado con el par criptográfico de OCSP (usando las opciones `-rkey` y `-rsigner`).

```
# openssl ocsp -port 127.0.0.1:2560 -text -sha256 \
      -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 ocsp.example.com.key.pem: secretpassword
```

En otro terminal, envíe una consulta al servidor OCSP. La opción `-cert` especifica el certificado que desea consultar.

```
# 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
```

El inicio de la salida muestra:

- si se recibe una respuesta correcta (`OCSP Response Status`)
- la identidad de servicio de respuesta (`Responder Id`)
- el estado de revocación del certificado (`Cert Status`)

```
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: ... CN = ocsp.example.com
    Produced At: Apr 11 12:59:51 2015 GMT
    Responses:
    Certificate ID:
```

```
        Hash Algorithm: sha1
        Issuer Name Hash: E35979B6D0A973EBE8AEDED75D8C27D67D2A0334
        Issuer Key Hash: 69E8EC547F252360E5B6E77261F1D4B921D445E9
        Serial Number: 1003
      Cert Status: good
      This Update: Apr 11 12:59:51 2015 GMT
```

Revoque el certificado.

```
# openssl ca -config intermediate/openssl.cnf \
      -revoke intermediate/certs/test.example.com.cert.pem

Enter pass phrase for intermediate.key.pem: secretpassword
Revoking Certificate 1003.
Data Base Updated
```

Al igual que antes, ejecute el servicio de respuesta de OCSP y en otra terminal envíe una consulta. Esta vez, la salida muestra `Cert Status: revoked` y un `Revocation Time`.

```
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: ... CN = ocsp.example.com
    Produced At: Apr 11 13:03:00 2015 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: E35979B6D0A973EBE8AEDED75D8C27D67D2A0334
      Issuer Key Hash: 69E8EC547F252360E5B6E77261F1D4B921D445E9
      Serial Number: 1003
    Cert Status: revoked
    Revocation Time: Apr 11 13:01:09 2015 GMT
    This Update: Apr 11 13:03:00 2015 GMT
```