MANUAL USO OCSP

Resumen

Ejemplo de uso del servicio OCSP para certificados de Firma Electrónica Avanzada de IDOK.

1. Objetivo

Detallar el uso del servicio OCSP para certificados de firma electrónica Avanzada de IDOK, junto con ejemplos de prueba.

2. Requisitos

1.1. OpenSSL

Para las pruebas se requiere el software OpenSSL (https://www.openssl.org/). En nuestro caso, usaremos una consola del software MinGW (http://www.mingw.org/) que es una versión minimalista de GNU para entornos Windows.

1.2. Cadena de Certificación y certificado OCSP

Para poder realizar la verificación de los certificados de pruebas, vamos a requerir los certificados de la cadena, el raíz (BPO IDOK ROOT CA) y el intermedio (CA FIRMA ELECTRÓNICA AVANZADA IDOK), los cuales se pueden obtener en la página de acceso público de la psc (https://psc.idok.cl/), en formato PEM. Adicionalmente se debe obtener el certificado para OCSP en la misma página (OCSP_FEA).

1.3. Certificados de prueba

Los certificados de usuario final de Firma Electrónica Avanzada que utilizaremos en esta prueba serán los incluidos en este directorio, uno vigente (test.pem) y otro revocado (testRev.pem).

3. Procedimiento

3.1. Transformación de Certificados

Si se requiere transformar los formatos de los certificados que se utilizarán, desde la extensión .crt a la extensión .pem se puede realizar con el siguiente comando em openssl:

```
Openssl x509 -in certificado.crt -out certificado.pem -outform PEM
```

Donde certificado.crt es el certificado original y certificado.pem el certificado en el nuevo formato.

3.2.Consulta de un certificado vigente

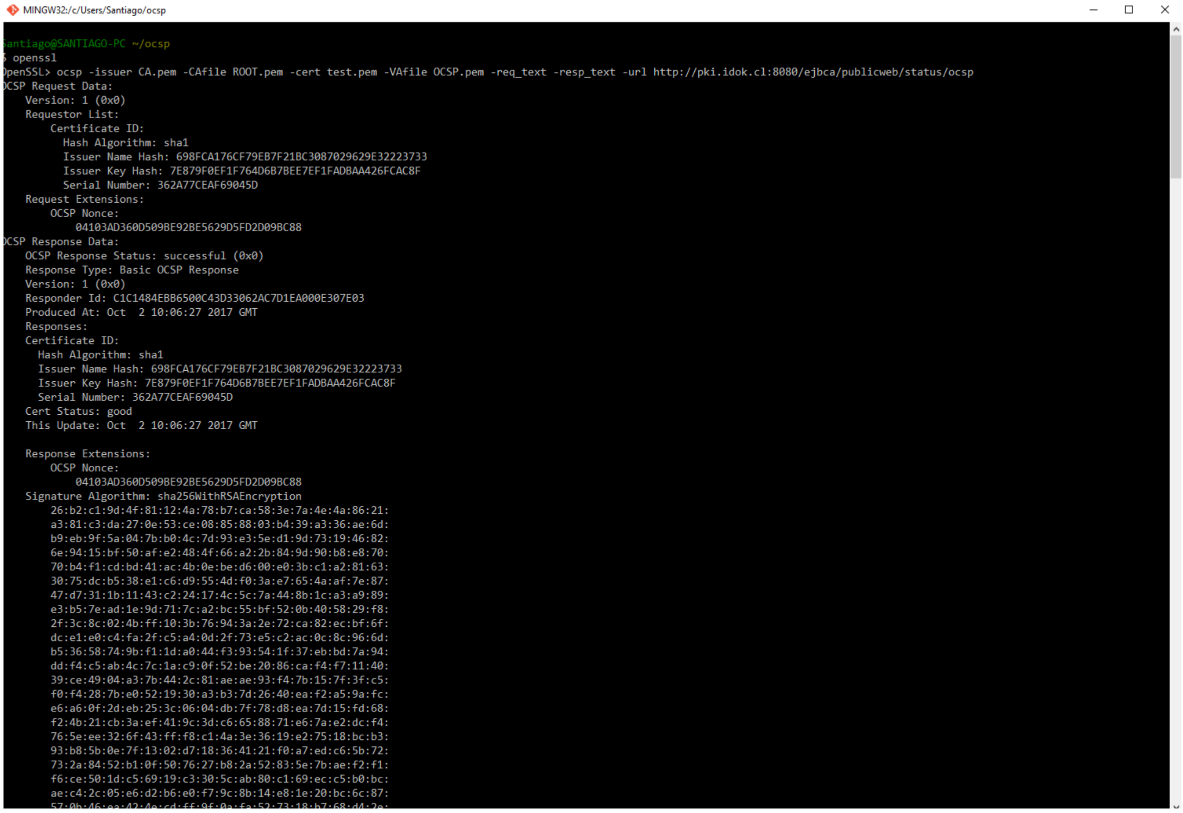
Utilizando la herramienta Openssl se debe ejecutar:

ocsp -issuer CA.pem -CAfile ROOT.pem -cert test.pem -VAfile OCSP.pem -req_text -resp_text -url http://pki.idok.cl:8080/ejbca/publicweb/status/ocsp

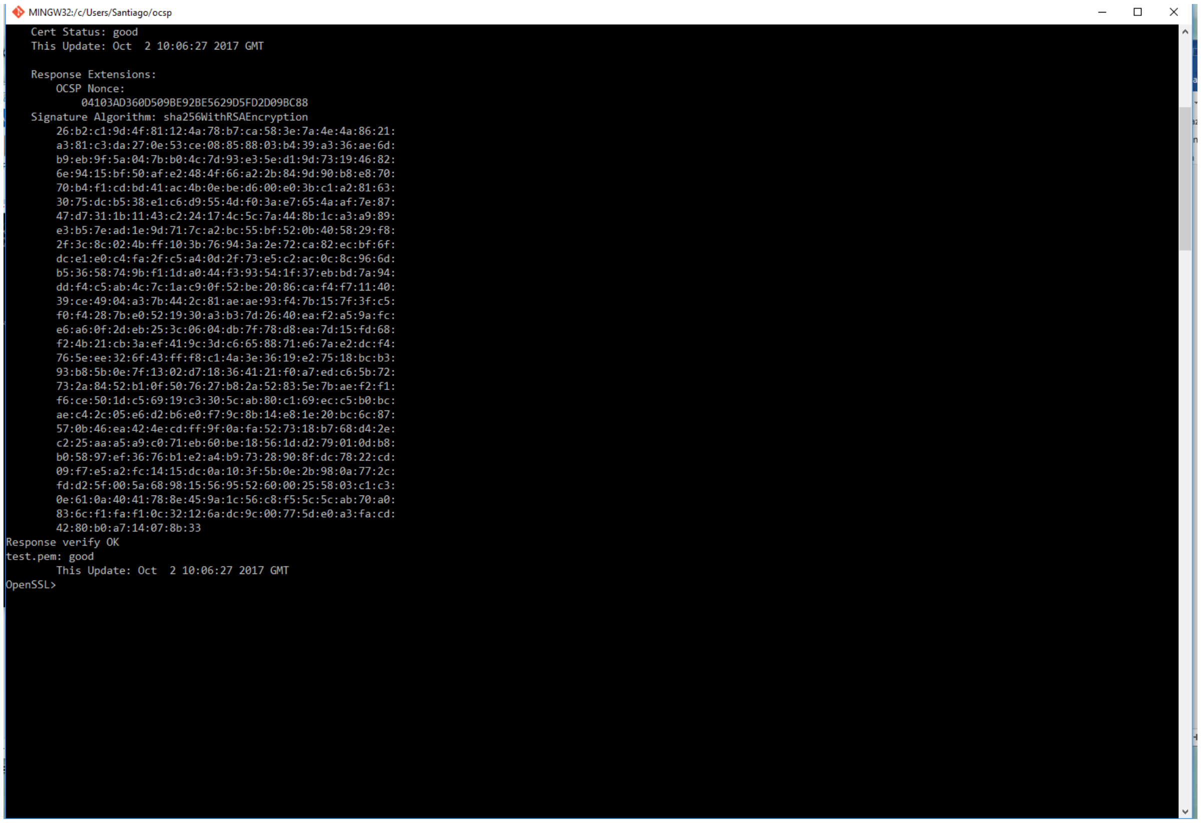
Dnde cada atributo significa:

-issuer : el certificado de la CA que emitió el certificado a verificar.
-CAfile : el certificado de la CA raíz.
-cert : el certificado a verificar.
-VAfile : el certificado que firma el servicio OCSP.
-req_text : se refiere a que mostrará en texto la solicitud.
-resp_text : especifica que muestre la respuesta en texto.
-url : la URL del servicio OCSP

El resultado obtenido es el siguiente:



```
Santiago@SANTIAGO-PC ~/ocsp
$ openssl
OpenSSL> ocsp -issuer CA.pem -CAfile ROOT.pem -cert test.pem -VAfile OCSP.pem -req_text -resp_text -url http://pki.idok.cl:8080/ejbca/publicweb/status/ocsp
OCSP Request Data:
    Version: 1 (0x0)
    Requestor List:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 698FCA176CF79EB7F21BC3087029629E32223733
          Issuer Key Hash: 7E879F0EF1F764D6B7BEE7EF1FADBAA426FCAC8F
          Serial Number: 362A77CEAF69045D
    Request Extensions:
        OCSP Nonce:
            04103AD360D509BE92BE5629D5FD2D09BC88
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C1C1484EBB6500C43D33062AC7D1EA000E307E03
    Produced At: Oct  2 10:06:27 2017 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 698FCA176CF79EB7F21BC3087029629E32223733
      Issuer Key Hash: 7E879F0EF1F764D6B7BEE7EF1FADBAA426FCAC8F
      Serial Number: 362A77CEAF69045D
    Cert Status: good
    This Update: Oct  2 10:06:27 2017 GMT

    Response Extensions:
        OCSP Nonce:
            04103AD360D509BE92BE5629D5FD2D09BC88
    Signature Algorithm: sha256WithRSAEncryption
        26:b2:c1:9d:4f:81:12:4a:78:b7:ca:58:3e:7a:4e:4a:86:21:
        a3:81:c3:da:27:0e:53:ce:08:85:88:03:b4:39:a3:36:ae:6d:
        b9:eb:9f:5a:04:7b:b0:4c:7d:93:e3:5e:d1:9d:73:19:46:82:
        6e:94:15:bf:50:af:e2:48:4f:66:a2:2b:84:9d:90:b8:e8:70:
        70:b4:f1:cd:bd:41:ac:4b:0e:be:d6:00:e0:3b:c1:a2:81:63:
        30:75:dc:b5:38:e1:c6:d9:55:4d:f0:3a:e7:65:4a:af:7e:87:
        47:d7:31:1b:11:43:c2:24:17:4c:5c:7a:44:8b:1c:a3:a9:89:
        e3:b5:7e:ad:1e:9d:71:7c:a2:bc:55:bf:52:0b:40:58:29:f8:
        2f:3c:8c:02:4b:ff:10:3b:76:94:3a:2e:72:ca:82:ec:bf:6f:
        dc:e1:e0:c4:fa:2f:c5:a4:0d:2f:73:e5:c2:ac:0c:8c:96:6d:
        b5:36:58:74:9b:f1:1d:a0:44:f3:93:54:1f:37:eb:bd:7a:94:
        dd:f4:c5:ab:4c:7c:1a:c9:0f:52:be:20:86:ca:f4:f7:11:40:
        39:ce:49:04:a3:7b:44:2c:81:ae:ae:93:f4:7b:15:7f:3f:c5:
        f0:f4:28:7b:e0:52:19:30:a3:b3:7d:26:40:ea:f2:a5:9a:fc:
        e6:a6:0f:2d:eb:25:3c:06:04:db:7f:78:d8:ea:7d:15:fd:68:
        f2:4b:21:cb:3a:ef:41:9c:3d:c6:65:88:71:e6:7a:e2:dc:f4:
        76:5e:ee:32:6f:43:ff:f8:c1:4a:3e:36:19:e2:75:18:bc:b3:
        93:b8:5b:0e:7f:13:02:d7:18:36:41:21:f0:a7:ed:c6:5b:72:
        73:2a:84:52:b1:0f:50:76:27:b8:2a:52:83:5e:7b:ae:f2:f1:
        f6:ce:50:1d:c5:69:19:c3:30:5c:ab:80:c1:69:ec:c5:b0:bc:
        ae:c4:2c:05:e6:d2:b6:e0:f7:9c:8b:14:e8:1e:20:bc:6c:87:
        57:0b:46:ea:42:4e:cd:ff:9f:0a:fa:52:73:18:b7:68:d4:2e:
```



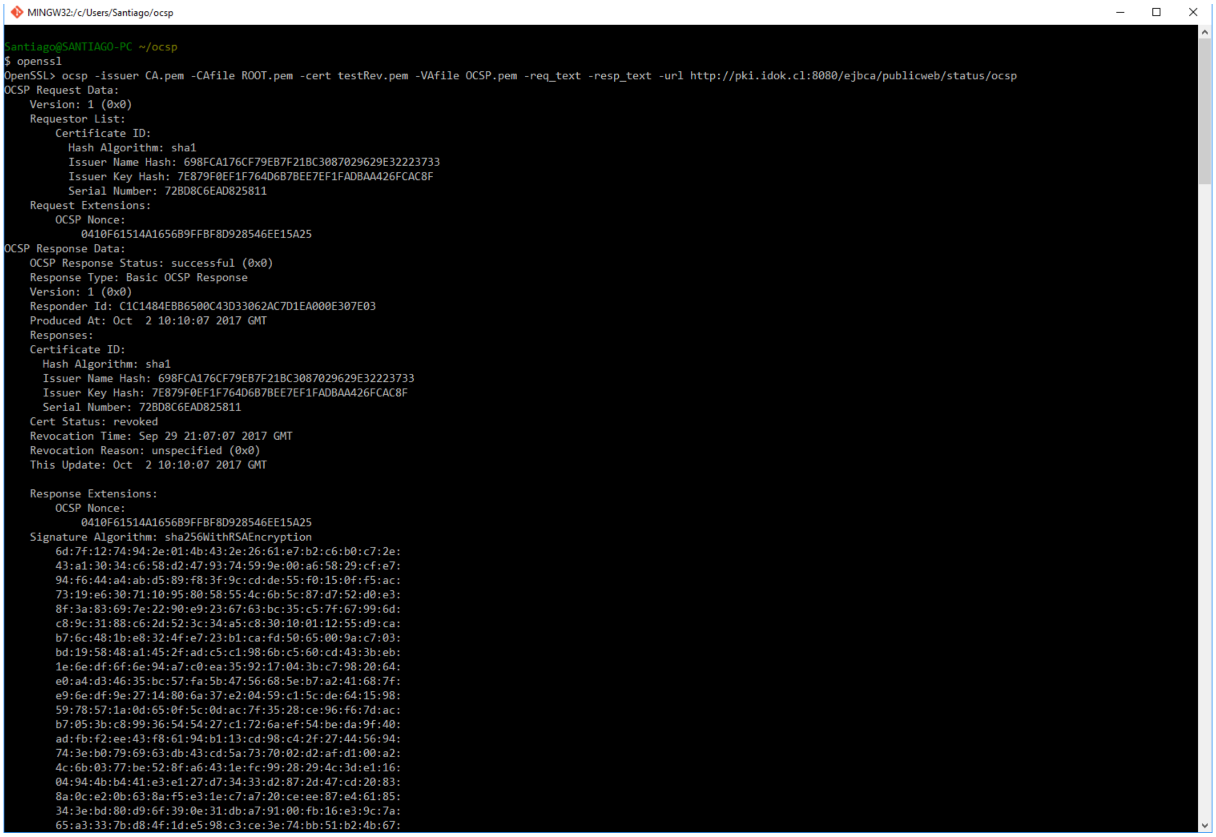
```
    Cert Status: good
    This Update: Oct  2 10:06:27 2017 GMT

    Response Extensions:
        OCSP Nonce:
            04103AD360D509BE92BE5629D5FD2D09BC88
    Signature Algorithm: sha256WithRSAEncryption
        26:b2:c1:9d:4f:81:12:4a:78:b7:ca:58:3e:7a:4e:4a:86:21:
        a3:81:c3:da:27:0e:53:ce:08:85:88:03:b4:39:a3:36:ae:6d:
        b9:eb:9f:5a:04:7b:b0:4c:7d:93:e3:5e:d1:9d:73:19:46:82:
        6e:94:15:bf:50:af:e2:48:4f:66:a2:2b:84:9d:90:b8:e8:70:
        70:b4:f1:cd:bd:41:ac:4b:0e:be:d6:00:e0:3b:c1:a2:81:63:
        30:75:dc:b5:38:e1:c6:d9:55:4d:f0:3a:e7:65:4a:af:7e:87:
        47:d7:31:1b:11:43:c2:24:17:4c:5c:7a:44:8b:1c:a3:a9:89:
        e3:b5:7e:ad:1e:9d:71:7c:a2:bc:55:bf:52:0b:40:58:29:f8:
        2f:3c:8c:02:4b:ff:10:3b:76:94:3a:2e:72:ca:82:ec:bf:6f:
        dc:e1:e0:c4:fa:2f:c5:a4:0d:2f:73:e5:c2:ac:0c:8c:96:6d:
        b5:36:58:74:9b:f1:1d:a0:44:f3:93:54:1f:37:eb:bd:7a:94:
        dd:f4:c5:ab:4c:7c:1a:c9:0f:52:be:20:86:ca:f4:f7:11:40:
        39:ce:49:04:a3:7b:44:2c:81:ae:ae:93:f4:7b:15:7f:3f:c5:
        f0:f4:28:7b:e0:52:19:30:a3:b3:7d:26:40:ea:f2:a5:9a:fc:
        e6:a6:0f:2d:eb:25:3c:06:04:db:7f:78:d8:ea:7d:15:fd:68:
        f2:4b:21:cb:3a:ef:41:9c:3d:c6:65:88:71:e6:7a:e2:dc:f4:
        76:5e:ee:32:6f:43:ff:f8:c1:4a:3e:36:19:e2:75:18:bc:b3:
        93:b8:5b:0e:7f:13:02:d7:18:36:41:21:f0:a7:ed:c6:5b:72:
        73:2a:84:52:b1:0f:50:76:27:b8:2a:52:83:5e:7b:ae:f2:f1:
        f6:ce:50:1d:c5:69:19:c3:30:5c:ab:80:c1:69:ec:c5:b0:bc:
        ae:c4:2c:05:e6:d2:b6:e0:f7:9c:8b:14:e8:1e:20:bc:6c:87:
        57:0b:46:ea:42:4e:cd:ff:9f:0a:fa:52:73:18:b7:68:d4:2e:
        c2:25:aa:a5:a9:c0:71:eb:60:be:18:56:1d:d2:79:01:0d:b8:
        b0:58:97:ef:36:76:b1:e2:a4:b9:73:28:90:8f:dc:78:22:cd:
        09:f7:e5:a2:fc:14:15:dc:0a:10:3f:5b:0e:2b:98:0a:77:2c:
        fd:d2:5f:00:5a:68:98:15:56:95:52:60:00:25:58:03:c1:c3:
        0e:61:0a:40:41:78:8e:45:9a:1c:56:c8:f5:5c:5c:ab:70:a0:
        83:6c:f1:fa:f1:0c:32:12:6a:dc:9c:00:77:5d:e0:a3:fa:cd:
        42:80:b0:a7:14:07:8b:33
Response verify OK
test.pem: good
        This Update: Oct  2 10:06:27 2017 GMT
OpenSSL>
```

3.3.CONSULTA DE UN CERTIFICADO REVOCADO

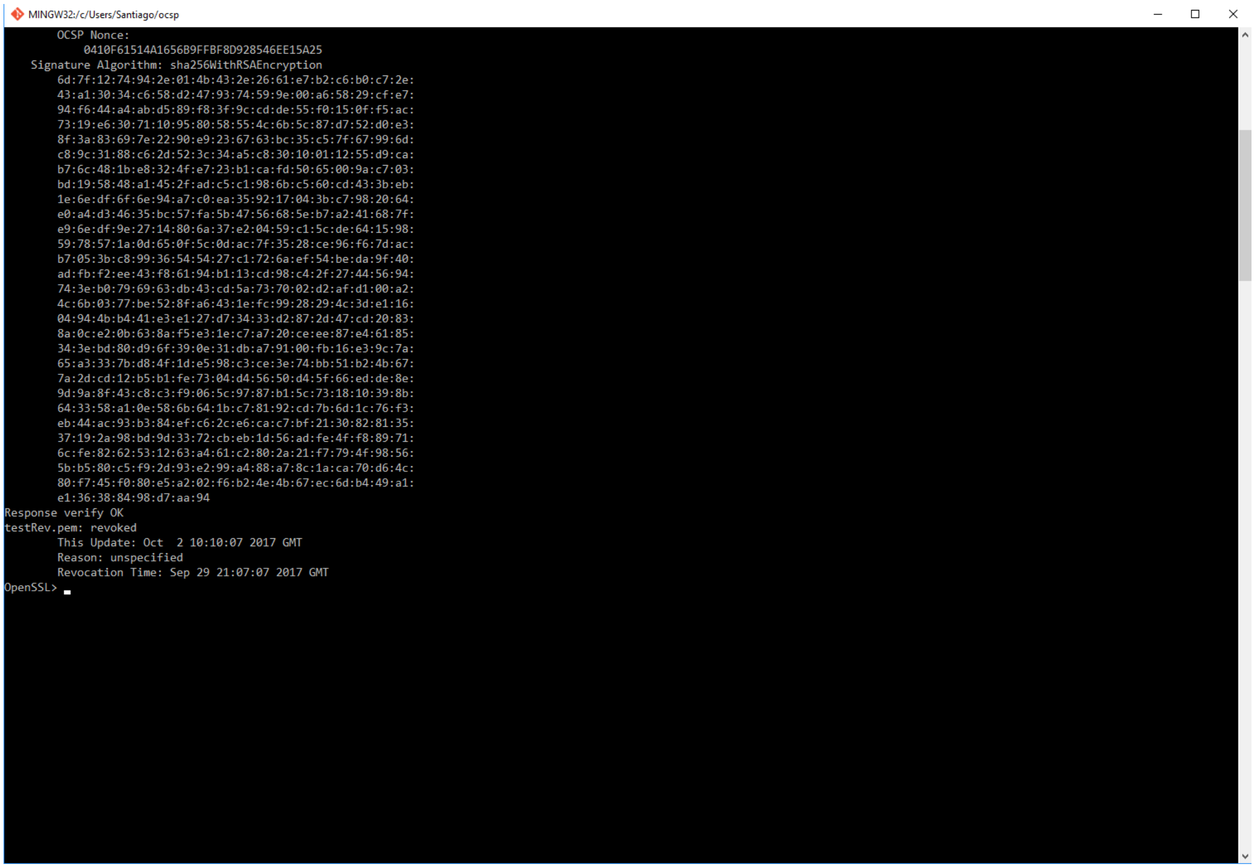
Utilizando la herramienta Openssl se debe ejecutar:

ocsp -issuer CA.pem -CAfile ROOT.pem -cert testRev.pem -VAfile OCSP.pem -req_text -resp_text -url http://pki.idok.cl:8080/ejbca/publicweb/status/ocsp

El resultado obtenido es el siguiente:



```
Santiago@SANTIAGO-PC ~/ocsp
$ openssl
OpenSSL> ocsp -issuer CA.pem -CAfile ROOT.pem -cert testRev.pem -VAfile OCSP.pem -req_text -resp_text -url http://pki.idok.cl:8080/ejbca/publicweb/status/ocsp
OCSP Request Data:
    Version: 1 (0x0)
    Requestor List:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 698FCA176CF79EB7F21BC3087029629E32223733
          Issuer Key Hash: 7E879F0EF1F764D6B7BEE7EF1FADBAA426FCAC8F
          Serial Number: 72BD8C6EAD825811
    Request Extensions:
        OCSP Nonce:
            0410F61514A1656B9FFBF8D928546EE15A25
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C1C1484EBB6500C43D33062AC7D1EA000E307E03
    Produced At: Oct  2 10:10:07 2017 GMT
    Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: 698FCA176CF79EB7F21BC3087029629E32223733
      Issuer Key Hash: 7E879F0EF1F764D6B7BEE7EF1FADBAA426FCAC8F
      Serial Number: 72BD8C6EAD825811
    Cert Status: revoked
    Revocation Time: Sep 29 21:07:07 2017 GMT
    Revocation Reason: unspecified (0x0)
    This Update: Oct  2 10:10:07 2017 GMT

    Response Extensions:
        OCSP Nonce:
            0410F61514A1656B9FFBF8D928546EE15A25
    Signature Algorithm: sha256WithRSAEncryption
        6d:7f:12:74:94:2e:01:4b:43:2e:26:61:e7:b2:c6:b0:c7:2e:
        43:a1:30:34:c6:58:d2:47:93:74:59:9e:00:a6:58:29:cf:e7:
        94:f6:44:a4:ab:d5:89:f8:3f:9c:cd:de:55:f0:15:0f:f5:ac:
        73:19:e6:30:71:10:95:80:58:55:4c:6b:5c:87:d7:52:d0:e3:
        8f:3a:83:69:7e:22:90:e9:23:67:63:bc:35:c5:7f:67:99:6d:
        c8:9c:31:88:c6:2d:52:3c:34:a5:c8:30:10:01:12:55:d9:ca:
        b7:6c:48:1b:e8:32:4f:e7:23:b1:ca:fd:50:65:00:9a:c7:03:
        bd:19:58:48:a1:45:2f:ad:c5:c1:98:6b:c5:60:cd:43:3b:eb:
        1e:6e:df:6f:6e:94:a7:c0:ea:35:92:17:04:3b:c7:98:20:64:
        e0:a4:d3:46:35:bc:57:fa:5b:47:56:68:5e:b7:a2:41:68:7f:
        e9:6e:df:9e:27:14:80:6a:37:e2:04:59:c1:5c:de:64:15:98:
        59:78:57:1a:0d:65:0f:5c:0d:ac:7f:35:28:ce:96:f6:7d:ac:
        b7:05:3b:c8:99:36:54:54:27:c1:72:6a:ef:54:be:da:9f:40:
        ad:fb:f2:ee:43:f8:61:94:b1:13:cd:98:c4:2f:27:44:56:94:
        74:3e:b0:79:69:63:db:43:cd:5a:73:70:02:d2:af:d1:00:a2:
        4c:6b:03:77:be:52:8f:a6:43:1e:fc:99:28:29:4c:3d:e1:16:
        04:94:4b:b4:41:e3:e1:27:d7:34:33:d2:87:2d:47:cd:20:83:
        8a:0c:e2:0b:63:8a:f5:e3:1e:c7:a7:20:ce:ee:87:e4:61:85:
        34:3e:bd:80:d9:6f:39:0e:31:db:a7:91:00:fb:16:e3:9c:7a:
        65:a3:33:7b:d8:4f:1d:e5:98:c3:ce:3e:74:bb:51:b2:4b:67:
```



```
        OCSP Nonce:
            0410F61514A1656B9FFBF8D928546EE15A25
    Signature Algorithm: sha256WithRSAEncryption
        6d:7f:12:74:94:2e:01:4b:43:2e:26:61:e7:b2:c6:b0:c7:2e:
        43:a1:30:34:c6:58:d2:47:93:74:59:9e:00:a6:58:29:cf:e7:
        94:f6:44:a4:ab:d5:89:f8:3f:9c:cd:de:55:f0:15:0f:f5:ac:
        73:19:e6:30:71:10:95:80:58:55:4c:6b:5c:87:d7:52:d0:e3:
        8f:3a:83:69:7e:22:90:e9:23:67:63:bc:35:c5:7f:67:99:6d:
        c8:9c:31:88:c6:2d:52:3c:34:a5:c8:30:10:01:12:55:d9:ca:
        b7:6c:48:1b:e8:32:4f:e7:23:b1:ca:fd:50:65:00:9a:c7:03:
        bd:19:58:48:a1:45:2f:ad:c5:c1:98:6b:c5:60:cd:43:3b:eb:
        1e:6e:df:6f:6e:94:a7:c0:ea:35:92:17:04:3b:c7:98:20:64:
        e0:a4:d3:46:35:bc:57:fa:5b:47:56:68:5e:b7:a2:41:68:7f:
        e9:6e:df:9e:27:14:80:6a:37:e2:04:59:c1:5c:de:64:15:98:
        59:78:57:1a:0d:65:0f:5c:0d:ac:7f:35:28:ce:96:f6:7d:ac:
        b7:05:3b:c8:99:36:54:54:27:c1:72:6a:ef:54:be:da:9f:40:
        ad:fb:f2:ee:43:f8:61:94:b1:13:cd:98:c4:2f:27:44:56:94:
        74:3e:b0:79:69:63:db:43:cd:5a:73:70:02:d2:af:d1:00:a2:
        4c:6b:03:77:be:52:8f:a6:43:1e:fc:99:28:29:4c:3d:e1:16:
        04:94:4b:b4:41:e3:e1:27:d7:34:33:d2:87:2d:47:cd:20:83:
        8a:0c:e2:0b:63:8a:f5:e3:1e:c7:a7:20:ce:ee:87:e4:61:85:
        34:3e:bd:80:d9:6f:39:0e:31:db:a7:91:00:fb:16:e3:9c:7a:
        65:a3:33:7b:d8:4f:1d:e5:98:c3:ce:3e:74:bb:51:b2:4b:67:
        7a:2d:cd:12:b5:b1:fe:73:04:d4:56:50:d4:5f:66:ed:de:8e:
        9d:9a:8f:43:c8:c3:f9:06:5c:97:87:b1:5c:73:18:10:39:8b:
        64:33:58:a1:0e:58:6b:64:1b:c7:81:92:cd:7b:6d:1c:76:f3:
        eb:44:ac:93:b3:84:ef:c6:2c:e6:ca:c7:bf:21:30:82:81:35:
        37:19:2a:98:bd:9d:33:72:cb:eb:1d:56:ad:fe:4f:f8:89:71:
        6c:fe:82:62:53:12:63:a4:61:c2:80:2a:21:f7:79:4f:98:56:
        5b:b5:80:c5:f9:2d:93:e2:99:a4:88:a7:8c:1a:ca:70:d6:4c:
        80:f7:45:f0:80:e5:a2:02:f6:b2:4e:4b:67:ec:6d:b4:49:a1:
        e1:36:38:84:98:d7:aa:94
Response verify OK
testRev.pem: revoked
        This Update: Oct  2 10:10:07 2017 GMT
        Reason: unspecified
        Revocation Time: Sep 29 21:07:07 2017 GMT
OpenSSL> 
```

De este modo se verifica que el servicio OCSP está operativo.