

TB02 Evidencia

Respuesta a consulta de estado de Certificado al servicio OCSP



 e-Digital PKI <small>Una gestión simple y digital</small>	Resolución de acreditación	USO EXTERNO
Versión: 1.0	Propiedad de E-Digital PKI	Pág. 2 de 29

Tabla de contenido

1. Objetivo	3
2. Requisitos	3
2.1. OPENSLL	3
2.2. CADENA DE CERTIFICACIÓN Y CERTIFICADO OCSP	3
2.3. CERTIFICADOS DE PRUEBA	3
3. Procedimiento	3
3.1. TRANSFORMACIÓN DE CERTIFICADOS	3
3.2. CONSULTA DE UN CERTIFICADO VIGENTE	4
4. CONSULTA DE UN CERTIFICADO REVOCADO	6



 e-Digital PKI <small>Una gestión simple y digital</small>	Resolución de acreditación	USO EXTERNO
Versión: 1.0	Propiedad de E-Digital PKI	Pág. 3 de 29

1. OBJETIVO

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

2. REQUISITOS

2.1. OPENSLL

Para las pruebas se requiere el software OpenSSL (<https://www.openssl.org/>). En nuestro caso, usaremos una consola del software MinGW (<https://www.mingw-w64.org/>) que es una versión minimalista de GNU para entornos Windows.

2.2. CADENA DE CERTIFICACIÓN Y CERTIFICADO OCSP

Para poder realizar la verificación de los certificados de pruebas, vamos a requerir los certificados de la cadena, AC raíz y AC intermedio desde el sitio Signapis.com.

Adicionalmente se debe obtener el certificado para OCSP en la misma página <https://ec2-18-216-190-21.us-east-2.compute.amazonaws.com:8443/ejbca/public/web/status/ocsp>.


2.3. CERTIFICADOS DE PRUEBA

Se usará un certificado en estado vigente y otro certificado con estado revocado.

3. PROCEDIMIENTO

3.1. TRANSFORMACIÓN DE CERTIFICADOS



 e-Digital PKI <small>Una gestión simple y digital</small>	Resolución de acreditación	USO EXTERNO
Versión: 1.0	Propiedad de E-Digital PKI	Pág. 4 de 29

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 en 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.

El Comando general para consultar validez de los certificados en OCSP es:

```
comando openssl ocsf: openssl ocsf -issuer <emisor.pem>
-serial <numero_serie_cert_a_verificar> -cert
<cert_a_verificar.pem> -CAfile <ca_root.pem> -url
http://ec2-18-223-136-129.us-east-2.compute.amazonaws.com/ejbca/publicweb/status/ocsp -no_nonce
```

3.2. CONSULTA DE UN CERTIFICADO VIGENTE

Utilizando la herramienta Openssl se debe ejecutar:

```
openssl ocsf -issuer FirmaElectronicaAvanzadaSignapis.pem -serial
0x3CAC4A0707E84B44EDDB77C4AA454881D45FC0EA -cert PedroArayaReyes.pem
-CAfile AutoridadCertificadora.pem -req_text -url
http://ec2-18-216-190-21.us-east-2.compute.amazonaws.com:8080/ejbca/publicweb/status/ocsp -no_nonce
```

Donde 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.

-req_text : se refiere a que mostrará en texto la solicitud.




 e-Digital PKI Una gestión simple y digital	Resolución de acreditación	USO EXTERNO
Versión: 1.0	Propiedad de E-Digital PKI	Pág. 5 de 29

-resp_text : específica que muestre la respuesta en texto.

-url : la URL del servicio OCSP El resultado obtenido es el siguiente:

```
C:\Users\ceden>openssl ocsp -issuer C:\Users\ceden\Downloads\FirmaElectronicaAvanzadaSignapis.pem -serial 0x3CAC4A0707E84B44ED0B77C4AA454881D45FC0EA -cert C:\Users\ceden\Downloads\PedroArayaReyes.pem -CAfile C:\Users\ceden\Downloads\AutoridadCertificadora.pem -req_text -url http://ec2-18-216-190-21.us-east-2.compute.amazonaws.com:8080/ejbca/publicweb/status/ocsp -no_nonce
OCSP Request Data:
  Version: 1 (0x0)
  Requestor List:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: F167A4CAF90F702B4B22F89D0B846A872FE13547
      Issuer Key Hash: 7D5583CD67AB77BDC61D4870C438F37DE63FE862
      Serial Number: 3CAC4A0707E84B44ED0B77C4AA454881D45FC0EA
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: F167A4CAF90F702B4B22F89D0B846A872FE13547
      Issuer Key Hash: 7D5583CD67AB77BDC61D4870C438F37DE63FE862
      Serial Number: 3CAC4A0707E84B44ED0B77C4AA454881D45FC0EA
Response verify OK
0x3CAC4A0707E84B44ED0B77C4AA454881D45FC0EA: good
  This Update: Dec 1 19:25:45 2021 GMT
C:\Users\ceden\Downloads\PedroArayaReyes.pem: good
  This Update: Dec 1 19:25:45 2021 GMT
```

Figura 1 – Respuesta 1 OSCP

 e-Digital PKI Una gestión simple y digital	Resolución de acreditación	USO EXTERNO
Versión: 1.0	Propiedad de E-Digital PKI	Pág. 6 de 29

4. CONSULTA DE UN CERTIFICADO REVOCADO

Utilizando la herramienta Openssl se debe ejecutar:

```
openssl ocsf -issuer FirmaElectronicaAvanzadaSignapis.pem -serial
0x3A76EB1A0870DDE1987C9E7A28F1E0DCDF8B1580 -cert PersonaNatural.pem -CAfile
AutoridadCertificadora.pem -req_text -url
http://ec2-18-216-190-21.us-east-2.compute.amazonaws.com:8080/ejbca/publicweb/status/ocsp/
-no_nonce
```

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

```
C:\Users\ceden>openssl ocsf -issuer C:\Users\ceden\Downloads\FirmaElectronicaAvanzadaSignapis.pem -serial 0x3A76EB1A0870DDE1987C9E7A28F1E0DCDF8B1580 -cert C:\Users\ceden\Downloads\PersonaNatural.pem -CAfile C:\Users\ceden\Downloads\AutoridadCertificadora.pem -req_text -url http://ec2-18-216-190-21.us-east-2.compute.amazonaws.com:8080/ejbca/publicweb/status/ocsp/ -no_nonce
OCSP Request Data:
Version: 1 (0x0)
Requestor List:
Certificate ID:
Hash Algorithm: sha1
Issuer Name Hash: F167A4CAF90F702B4B22F89D08846AB72FE13547
Issuer Key Hash: 7D5583CD67AB77BDC61D4870C438F37DE63FE862
Serial Number: 3A76EB1A0870DDE1987C9E7A28F1E0DCDF8B1580
Certificate ID:
Hash Algorithm: sha1
Issuer Name Hash: F167A4CAF90F702B4B22F89D08846AB72FE13547
Issuer Key Hash: 7D5583CD67AB77BDC61D4870C438F37DE63FE862
Serial Number: 3A76EB1A0870DDE1987C9E7A28F1E0DCDF8B1580
Response verify OK
0x3A76EB1A0870DDE1987C9E7A28F1E0DCDF8B1580: revoked
This Update: Dec 1 19:13:00 2021 GMT
Revocation Time: Nov 25 20:42:30 2021 GMT
C:\Users\ceden\Downloads\PersonaNatural.pem: revoked
This Update: Dec 1 19:13:00 2021 GMT
Revocation Time: Nov 25 20:42:30 2021 GMT
C:\Users\ceden>
```

Figura 2 – Respuesta 2 OSCF