TB03 Manual de Respuesta Servicio OCSP

1. Información del documento

HISTORIA DEL DOCUMENTO			
Nombre del Documento:	TB03 Manual de Respuesta Servicio OCSP		
Generado por:	Pamela Barría		
Revisado por	Rafael Pérez	**Fecha de Creación:**	10/11/2021
Aprobado por:	Rafael Pérez Osvaldo Martínez	**Fecha de Aprobación:**	10/11/2021
Oficializado por:	Comité de Seguridad y Riesgos	**Entrada en vigencia:**	10/11/2021

CONTROL DE VERSIONES				
Versión:	**Fecha de Publicación:**	**Preparado/ Actualizado por:**	**Aprobado por:**	**Descripción:**
1.0	10/11/2021	Pamela Barría	Rafael Pérez	Creación
2.0	19/05/2023	Nicolás Borbarán	Comité de Seguridad y Riesgos	Revisión Anual. Actualización URL e imágenes de los comandos de OCSP.
2.1	20/08/2024	Nicolás Borbarán	Comité de Seguridad y Riesgos	Revisión anual. Ajuste pie de página. No hay cambios en el documento.

Tabla de contenido

2. Objetivo

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

3. Requisitos

a. OPEN SSL

Para las pruebas se requiere el software OpenSSL (https://www.openssl.org/). En nuestro caso, usaremos una consola del software "Win64 OpenSSL Command Prompt" (descargar de https://linuxhint.com/install-openssl-windows/ y seguir los pasos de instalación).

b. 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.

- Acceder a Marco Legal – Certificación – Certificado CA/Certificado CA intermedia (Descargar archivo)

Adicionalmente se debe obtener el certificado para OCSP en la misma página http://ca.signapis.com/ejbca/publicweb/status/ocsp.

c. CERTIFICADOS DE PRUEBA

Como ejemplo, se usará un certificado en estado vigente y otro certificado con estado revocado.

4. PROCEDIMIENTO

A. 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 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:

```
openssl ocsp -issuer C:/subca.pem -cert  C:/loreto.pem
-CAfile  C:/root.pem -req_text -url
http://ca.signapis.com/ejbca/publicweb/status/ocsp
-no_nonce
```

```
C:\Users\Nicolás>openssl ocsp -issuer C:\Users\Nicolás\Desktop\certificados_signapis_ocsp\AutoridadCertificadora-int.pem
 -cert  C:\Users\Nicolás\Desktop\certificados_signapis_ocsp\josibeth.pem -CAfile  C:\Users\Nicolás\Desktop\certificados_
signapis_ocsp\AutoridadCertificadora.pem -req_text -url http://ca.signapis.com/ejbca/publicweb/status/ocsp -no_nonce
OCSP Request Data:
    Version: 1 (0x0)
    Requestor List:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 40A6B3E650E8D41D08B5AA69947EC25416DFA00D
          Issuer Key Hash: C1BC02F9285C30AF74C30AD2491C95C40C95DCD4
          Serial Number: 1DAC09987F4CD569A33BF7286E0A0480887BDC90
Response verify OK
C:\Users\Nicolßs\Desktop\certificados_signapis_ocsp\josibeth.pem: good
        This Update: May  3 19:48:29 2023 GMT

C:\Users\Nicolás>
```

B. CONSULTA DE UN CERTIFICADO VIGENTE

Utilizando la herramienta Openssl se debe ejecutar:

openssl ocsp -issuer FirmaElectronicaAvanzadaSignapis.pem -serial 0x3CAC4A0707E84B44EDDB77C4AA454881D45FC0EA -cert PedroArayaReyes.pem -CAfile AutoridadCertificadora.pem -req_text -url http://ca.signapis.com/ejbca/publicweb/status/ocsp -no_nonce

Donde cada atributo significa:

-issuer : el certificado de la CA (intermedia) que emitió el certificado a verificar.

-serial: Número serie 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.

-resp_text : específica que muestre la respuesta en texto.

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

```
C:\Users\joseb\Downloads\certificados_signapis_ocsp>openssl ocsp -issuer AutoridadCertificadora-int.pem  -serial 0x1DAC09987F4CD569A3
3BF7286E0A0480887BDC90 -cert josibeth.pem -CAfile AutoridadCertificadora.pem -req_text -url http://ca.signapis.com/ejbca/publicweb/st
atus/ocsp -no_nonce
OCSP Request Data:
    Version: 1 (0x0)
    Requestor List:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 40A6B3E650E8D41D08B5AA69947EC25416DFA00D
          Issuer Key Hash: C1BC02F9285C30AF74C30AD2491C95C40C95DCD4
          Serial Number: 1DAC09987F4CD569A33BF7286E0A0480887BDC90
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 40A6B3E650E8D41D08B5AA69947EC25416DFA00D
          Issuer Key Hash: C1BC02F9285C30AF74C30AD2491C95C40C95DCD4
          Serial Number: 1DAC09987F4CD569A33BF7286E0A0480887BDC90
Response verify OK
0x1DAC09987F4CD569A33BF7286E0A0480887BDC90: good
        This Update: May  3 19:30:54 2023 GMT
josibeth.pem: good
        This Update: May  3 19:30:54 2023 GMT

C:\Users\joseb\Downloads\certificados_signapis_ocsp>
```

Figura 1 – Respuesta 1 OSCP

5. CONSULTA CERTIFICADO REVOCADO

Utilizando la herramienta Openssl se debe ejecutar:

openssl ocsp -issuer FirmaElectronicaAvanzadaSignapis.pem -serial 0x3A76EB1A0870DDE1987C9E7A28F1E0DCDF8B1580 -cert PersonaNatural.pem -CAfile AutoridadCertificadora.pem -req_text -url http://ca.signapis.com/ejbca/publicweb/status/ocsp/ -no_nonce

```
C:\Users\joseb\Downloads\certificados_signapis_ocsp>openssl ocsp -issuer AutoridadCertificadora-int.pem  -serial 0x7760DD2FE1D890844E
005C256A26F5C9BE2F3EF6 -cert certb738018a51e84ce898f8ad2dc71e34226e9ebaa5-chain.pem -CAfile AutoridadCertificadora.pem -req_text -url
 http://ca.signapis.com/ejbca/publicweb/status/ocsp/ -no_nonce
OCSP Request Data:
    Version: 1 (0x0)
    Requestor List:
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 40A6B3E650E8D41D08B5AA69947EC25416DFA00D
          Issuer Key Hash: C1BC02F9285C30AF74C30AD2491C95C40C95DCD4
          Serial Number: 7760DD2FE1D890844E005C256A26F5C9BE2F3EF6
        Certificate ID:
          Hash Algorithm: sha1
          Issuer Name Hash: 40A6B3E650E8D41D08B5AA69947EC25416DFA00D
          Issuer Key Hash: C1BC02F9285C30AF74C30AD2491C95C40C95DCD4
          Serial Number: 7760DD2FE1D890844E005C256A26F5C9BE2F3EF6
Response verify OK
0x7760DD2FE1D890844E005C256A26F5C9BE2F3EF6: revoked
        This Update: May  3 19:31:47 2023 GMT
        Reason: keyCompromise
        Revocation Time: Feb  1 16:07:02 2023 GMT
certb738018a51e84ce898f8ad2dc71e34226e9ebaa5-chain.pem: revoked
        This Update: May  3 19:31:47 2023 GMT
        Reason: keyCompromise
        Revocation Time: Feb  1 16:07:02 2023 GMT

C:\Users\joseb\Downloads\certificados_signapis_ocsp>
```

Figura 2 – Respuesta 2 OSCP

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

Fin del documento