

MANUAL USO OCSP

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

1.	Obj	etivo	3
2.	Rec	uisitos	3
1	L.1.	OpenSSL	3
1	L.2.	Cadena de Certificación y certificado OCSP	3
1	L.3.	Certificados de prueba	3
3.	Pro	cedimiento	3
3	3.1.	Transformación de Certificados	3
3	8.2.	Consulta de un certificado vigente	3
3	3.3.	Consulta de un certificado Revocado	6

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 (<u>https://www.openssl.org/</u>). En nuestro caso, usaremos una consola del software MinGW (<u>http://www.mingw.org/</u>) 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 (<u>https://psc.idok.cl/</u>), 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 <u>http://pki.idok.cl:8080/ejbca/publicweb/status/ocsp</u>

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:

♦ MINGW32/c/Ukes/Santiago/ocsp	-	×
		^
openssl		
penSSL> 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		
CSP 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		
CSP Response Data:		
OCSP Response Status: successful (0x0)		
Response Type: Basic OCSP Response		
Version: 1 (0x0)		
Responder_113: C1C1484EBB6500(43)33062AC//D1EA000E30/E03		
Produced At: Uct 2 10:06:27 2017 GMI		
Kesponses:		
Lertificate ID:		
Hash Algoritami shal		
155UEP Waller Hash: 030FLAT/0EF/2105306/029022252222535		
LSSUEF KEY RASH: /Co/9F0EFEF/04U00/DEE/EFEAUDAA420FCAC6F Soafa Numbers /26/37256Ef604ED		
Serial Number, JOAN/ALAPOSOBJU		
This Undate: 0rt 2 18:06:27 2017 GMT		
Response Extensions:		
OCSP Nonce:		
04103AD36005098E928E5629D5FD2D09BC88		
Signature Algorithm: Sha250wiIntKAlencrypTion		
2b:b2:c1:9d:44:83:12:44:78:b7:c3:36:56:56:76:74:44:48:8b:21:		
a):81:C):da12/100:13):C2:08:83:68:09:104:39:133:40:42:50:		
D9:E0:91:33:04:/0:D0:4C:/0:93:E3:5E:01:90:/3:19:40:62: C=:04:15:E0:C=:C=:04:06:CE::05:E0:04:E0:04:E0:05:E0:05:E0:04:E0:05:E0:05:E0:04:E0:05:E0:04:E0:05:E0:04:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:05:E0:		
04:94:15:01:30:41:42:40:41:10:32:20:04:90:90:100:100:100:100:		
70.04.11.00.00.01.30.47.60.00.00.00.00.00.00.00.00.00.00.00.00.		
J, / J, UL, JJ, JO, EJ, CU, UJ, JJ, AU, 10, JA, P/, OJ, HA, HI, YE, OV. A7, A7, 21, 41, 11, 42, -07, 20, 47, 46, 16, 17, 46, 56, 17, 46, 48, 17, 47, 40, 16, 16, 16, 16, 16, 16, 16, 16		
a ³ + 6, 7a - ai + 1a - 94 - 71 - 73 - 54 - 55 - 56 - 54 - 54 - 54 - 58 - 56 - 58 - 56 - 58 - 56 - 58 - 58		
26-13-78-10-14.14.67-10-13.76-04-13-02-77-76-18-27-07-16-66-		
d_{r+1} , a_{r} , d_{r+1} , a_{r} , d_{r+1} , d		
b5 36 58 74 99 41 14 a0 44 43 93 54 11 37 ab 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:		
57.8h.46.ee.42.4e.cd.ff.9f.8e.fe.52.73.18.h7.68.4d.2e.		- U

MINGW32/c/Users/Santiago/ocsp	-	×
Cert Status: good		~
This Update: 0ct 2 10:06:27 2017 GMT		
Response Extensions.		
ACR None:		a
2 Signature Auguri Itimi, Sinz Jowini, Santini Sa		32
20.02.11.70.41.01.12.44.70.07.04.90.02.14.20.02.17.44.40.00.21.		n
b) ob (94) 5 - (64) 5		
6, (d) 15, (d), (d), (d), (d), (d), (d), (d), (d)		
70 + 10 + 10 + 10 + 10 + 10 + 10 + 10 +		
50, / 3, 40, 10 , 30, 621, 60, 60, 51, 51, 60, 70, 51, 40, 61, 76, 70, 77, 70, 70, 70, 70, 70, 70, 70, 70		
a3 · b5 · 7a · a4 · fa · da · fa · 17 · r3 · ba · b5 · b5 · 55 · b5 · 52 · b5 · b5 · b5		
26.3 - 18 - 60.1 (h) - 51.1 - 31 32 03.1 - 27 03 03.1 - 27 03.1 - 03.1		
b5-36-58-72-9b-41-14-a0-41-41-32-3b-141-72-90-		
$d_1 + f_1 + c_1 + h_1 + d_2 + d_3 + h_1 + f_3 $		
30 (a) 37 (b) 47 (c) 131 (c) (c) 121 (c)		
$f_0, f_1, g_2, m_3, g_1, g_2, g_1, g_2, g_1, g_1, g_2, g_1, g_2, g_3, f_2, g_3, g_4, g_1, g_2, g_1, g_1, g_2, g_1, g_1, g_1, g_1, g_1, g_1, g_1, g_1$		
a6-a6-6f-2d-ab-25-3-66-8d-db-7f-78-d8-aa-7d-15-6f-68-		
f_{2}^{-} , h_{1}^{-} , f_{2}^{-} , g_{1}^{-} , g_{1}^{-} , f_{2}^{-} , f_{2}^{-} , g_{2}^{-} , d_{1}^{-} , f_{2}^{-} , g_{2}^{-} , d_{1}^{-} , f_{2}^{-} , $f_{$		
76-5a-ca-32-6F-43-FF-68-c1-4a-3a-36-19-c2-75-18-ba-		
93-18-55-26-75-13-09-47-18-35-41-91-60-37-44-55-57-		
73 · 2a · 84 · 52 · h1 · 46 · 56 · 76 · 77 · h8 · 2a · 52 · 83 · 5a · 76 · 2a · 52 · 41 · 2a · 52 · 41 · 46 · 56 · 76 · 76 · 76 · 76 · 76 · 76 · 7		
f5 - ca - 5a - 1d - c5 - i - 3a - 5c - i - 3a - 5c - i - 2a		
57-0h-46-0a-(7)-0a-(7)-0a-(5)-(7)-18-(7)-(8-(4)-7)-		
c2 · 25 · 3a · 55 · 39 · c0 · 71 · ch · 60 · ha · 18 · 56 · 1d · d2 · 79 · 01 · 0d · h8 ·		
hh 58 49 - 6 - 36 - 76 - 11 - 6 - 73 - 72 - 10 - 87 - 46 - 73 - 72 - 74 -		
0: f7: 5: 32 fc: 14: 15: dc: 0a: 10: 37: 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+1e+56+e8+55+5e+5e+a0+70+a0+		
83·6r·f1·fa·f1·9r·32·12·6a·dr·9r·90·77·5d·e0·a3·fa·rd·		
42·88·16·37·14·07·81·33		
Response verify OK		
test.new god		
This Indate: Oct 2 10:06:27 2017 GMT		
		-
		~

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 <u>http://pki.idok.cl:8080/ejbca/publicweb/status/ocsp</u>

El resultado obtenido es el siguiente:

♦ MINGVI22/c/Users/Santiago/ocsp	- 0	ı ×	<
Santiacos AUTIACO PC //oce			^
antaugugututori c poup			
DoenSSL> ocsp -issuer CA.pem -CAfile ROOT.pem -cert testRev.pem -VAfile OCSP.pem -reg text -resp text -url http://pki.idok.cl:8080/eibca/publicweb/status/ocsp			
OCSP Request Data:			
Version: 1 (0x0)			
Requestor List:			
Certificate ID:			
Hash Algorithm: sha1			
Issuer Name Hash: 698FCA176CF79EB7F21BC3087029629E32223733			
Issuer Key Hash: 7E879F0EF1F764D687BEE7EF1FADBAA426FCAC8F			
Serial Number: 72BD8C6EAD825811			
Request Extensions:			
OCSP Nonce:			
0410F61514A1656B9FFBF8D928546EE15A25			
OCSP Response Data:			
OCSP Response Status: successful (0x0)			
Kesponse Type: Basic OCSP Kesponse			
Responder 10: LILudadebosod(43)03002AL/UILA000E50/E03			
Produced AL: UCL 2 10:10:07 2017 GM			
Castificate ID:			
Hesh Japonither chai			
1631 ALBOY LUM: 5164 Tecing Name Hach: 648Ef176/E79ER75218C3087029629E322233			
Toscian Kayi Hashi 758704765175267142050507420526522753			
Secial Number: 7280866F40825811			
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:			
81:3a:83:69:7/e:22:90:e9:23:65:65:65:65:65:65:65:65:65:65:65:65:65:			
C8:9C:31:88:C0:22:32:3C:34:85:C0:22:3C:34:10:01:12:35:09:C3: b72(C:40:44:40:02) 20:4(C:72:32:24:45:C6:34:02) 20:4(C:72:02) 20:4			
D/10C/40110160122/4116//231011C31101001051001931C/1001 Halon F8/402 - 4/47_0214-454/40_50-4/40_231-6-1-40_2			
DUL19:30:40:41:40:27:40:405:C1:90:001:C3:00:C01:40:300:001 1x:6x:45:65:6x:04:42:40:xx:7:00:xx:7:00:300:C01:40:300:001			
10.00-01-01-00-54-47-C0-04-55-52-17-04-10-C7-75-20-04- 			
et. at. (J) - 40 - J) - (L - J) - (A - J) - (J)			
59 - 78 - 57 - 13 - 94 - 65 - 94 - 37 - 74 - 35 - 28 - r.e. 96 - f6 - 74 - ar			
h7:95:3h; 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:			\sim

MINGW32:/c/Users/Santiago/ocsp	\times
OCSP Nonce:	^
0410F61514A165689FFBF80928546EE15A25	
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:t6:44:ad:ab:d5:89:t8:3f:9c:cd:de:55:t0:15:ac:	
/3:19:e0:30:71:10:95:80:55:65:55:42:60:55:83:54:60:55:83:47:22:100:e3:	
81:33:83:197/e:22:391:e97/23:167:63:107:1391:601	
C0:9C:31:00:C0:22:32:3C:34:30:C0:30:10:01:12:35:09:100:01:22:35:09:C0:100:00:12:35:09:100:01:01:01:01:01:01:01:01:01:01:01:01	
b/10/15/8/32/a/1/6/72/a/for/for/a/d/d/d/a/b/	
1 e : fe : df : ff : fe : 94 : a7 : cf : ea : 35 : 92 : 17 : 64 : 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:c2:0b:63:8a:75:c3:1e:c?:a/:20:cc=ce:8/:e4:51:85:	
341361001801011c113910013110013/191100110110181901731	
05:43:53:70:40:47:10:62:90:(3:(0:)):102:40:07: 75:32:4:61:32:10:40:47:10:02:100:41:65:66:40:40:90:	
9d-9a-8f-2a-c8-c3-c9-96-5c-92-87-b1-5c-72-18-10-36-5	
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	
Parana warafidid	
Redson: Unspectrate Reusention: Time: Son 29.21.07.07.2017 CMT	
Nevolation (Time, sep 22 21.0.0) 2017 (MT)	
openance -	
	~

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