Servicio DMA-WS

Direct Market Access Web Service

Requisitos Mecanismo de Autenticación:

“Client Autenticación con HTTPS”

Indice

Revisión Histórica

Fecha	Revisión	Descripción
8-04-15	1.0.0	Versión inicial
29-05-15	1.1.0	Se modificó la sección Formato del Certificado y Archivos a Entregar, agregando la nomenclatura que deberá tener el archivo que contenga el Certificado Cliente. Se modificó la sección Seguridad, mencionando la versión de internet explorer (IE 9).
20-05-16	1.2.0	Se amplió información apartado “Formato del Certificado y Archivo a entregar”. Se agregó apartado “renovación del Certificado” Se aclara restricción campo “issuer”. Se aclara sin restricción campo “subject”.

Pedido del Servicio Productivo

Para DMA un certificado del Back-Office identifica unívocamente a un Agente. Por lo tanto este certificado debe ser registrado en DMA previo a la puesta en marcha del Back-Office. Para ello el Agente debe enviar una Nota al MVBA (en sus oficinas de 25 de Mayo 359 – 10º Piso) manifestando la intensión de contar con el servicio DMA-WS en Ambiente de Producción.

La Nota deberá estar acompañada por el Certificado Cliente que se utilizará en Producción.

El MVBA enviará a CVSA – Sector CAU la documentación y el certificado para que habilitemos el uso del servicio en Producción (alta usuarios, terminales, etc).

Acceso al Servicio Productivo

Para acceder al Servicio SDO el Back-Office cuenta con dos alternativas:

- Acceso por VPN (Virtual Private Network).
- Acceso por Internet.

En ambos casos, el acceso es a través de la siguientes url: https://dma-ws.sba.com.ar

Seguridad

En cuanto a la seguridad la utilización de HTTPS para las comunicaciones entre DMA y el Back-Office garantiza la *privacidad* e *integridad* de toda la información que se intercambia.

En esta sección analizaremos otros aspectos de la seguridad como la *autenticación* y el *no repudio*.

Para la autenticación se ofrecen dos mecanismos alternativos que describiremos en detalle.

1. Autenticación con HTTPS 'Client Authentication'.
2. Autenticación con Firma Digital.

A continuación detallamos las especificaciones del mecanismo de autenticación utilizado, por Uds., durante el período de pruebas: "Client Autenticación" con HTTPS.

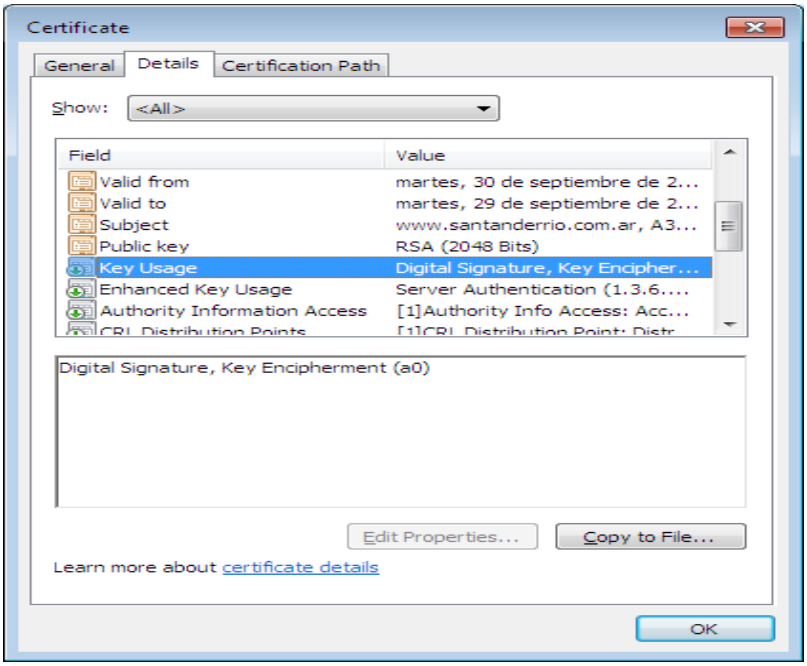
Es importante destacar, que la versión del navegador en el servidor productivo donde se realicen las conexiones deberá ser la IE 9 (Internet Explorer V9).

Autenticación con HTTPS 'Client Authentication'

Una alternativa de autenticación es la utilización de HTTPS con 'Client Authentication'. Esto significa que en cada conexión HTTPS que se establezca, el servidor (DMA) va a requerir al cliente (Back-Office) que envíe un certificado X.509 SSL de tipo cliente, emitidos por una autoridad certificante reconocida y vigentes.

El Back-Office debe contar con uno o más certificados digitales de tipo "X.509v3", SSL de tipo cliente, emitidos por una autoridad certificante reconocida y vigentes.

Es importante destacar, para que el certificado sea apto para SSL con autenticación del Cliente, el 'Key Usage' del certificado (si se especifica) debe incluir 'Key Encipherment'. También debe tener en el propósito cliente ssl.



Cuando se genera el certificado para enviar a la entidad certificante, que en el propósito (propousal) esté definido ssl cliente (sslclient), pueden poner más propósitos si quisieran pero deberán ver con la entidad que no los pise o cambie. Cuando reciban el certificado de la entidad certificadora deberán hacer la verificación de que el propósito de ssl cliente esta seteado en Y tal como lo enviaron al momento de generación.

Se aclara que no hay restricción alguna para el "subject" del Certificado. No obstante, sí hay una restricción particular para el "issuer", en cuyo campo no se deberá incluir el @.

Renovación del Certificado ‘Client Authentication’

Será responsabilidad del Agente gestionar el certificado digital para la autenticación así como también las posteriores renovaciones del mismo. Es decir, que la administración del certificado estará bajo la responsabilidad de cada Agente.

El trámite de renovación deberá presentarse al menos 15 días hábiles con antelación al vencimiento del certificado instalado en producción y ante las oficinas del CAU, situado en Sarmiento 334 – 10º Piso.

Es importante destacar la importancia de la administración y renovación del Certificado, dado que sin dicha conectividad segura, el Agente no podrá contar con el servicio productivo.

Ejemplo de Certificado X.509 SSL de tipo Cliente

A continuación se detalla un ejemplo de comando usando el paquete de Openssl para ver el certificado y sus características.

Openssl x509 -noout -text -purpose -in user.crt

Resultado de la ejecución del commando:

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
3c:3c:5a:24:00:00:00:00:8f:c6
Signature Algorithm: sha1WithRSAEncryption
Issuer: DC=ar, DC=com, DC=xxxxx, DC=xxxxxx, CN=xxxxx
Validity
Not Before: Jan 20 18:27:40 2015 GMT
Not After : Jan 20 18:37:40 2016 GMT
Subject: C=AR, O=XXXXXXXXX, OU=XXXXXX, CN=XXXXXXX
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:b4:df:54:e1:17:93:31:df:f0:85:ae:ff:61:cb:
cc:11:e4:78:a1:7c:03:91:20:f6:32:7c:bc:a1:e0:
1b:bb:03:53:dc:24:cb:8b:eb:82:16:c5:d7:1a:b9:
87:2d:b7:84:fd:54:8b:bc:1b:75:38:ac:55:fc:95:
24:52:3f:c9:78:52:d2:bf:25:2f:0f:9f:8c:41:ac:
7a:00:84:15:9d:d6:f4:2a:af:d3:3e:d8:b3:ec:f3:
dc:46:b3:9c:7a:c7:b6:12:f6:60:45:95:f6:cd:b5:
64:3e:34:22:8d:8e:3a:6f:70:03:b7:01:0f:81:7f:
d8:da:90:b8:bc:73:a2:bc:4e:af:7d:fd:88:93:8d:
36:90:1f:00:2e:a2:6f:46:b1:2d:fb:e0:c1:7a:54:
80:7e:c4:75:a5:20:5a:5d:d0:cd:51:20:cb:62:34:
cd:9b:de:f5:cf:4b:ec:60:a5:84:45:cc:21:49:7d:
7e:9b:1f:c0:f6:78:39:d4:99:42:eb:9d:4a:c3:a3:
54:72:12:0b:ee:ee:86:bc:8a:85:f2:79:1c:e5:89:
23:fc:d0:0b:09:de:ed:24:12:b4:09:67:fc:79:be:
02:5e:79:45:fa:78:20:e5:c0:a2:fe:d2:7d:8f:03:
87:d0:15:bb:be:6f:87:98:67:df:86:51:a4:e4:80:
df:77
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
27:A3:C6:E2:AF:11:57:99:2C:02:99:E2:17:B2:70:25:28:C9:4D:25

X509v3 Authority Key Identifier:
keyid:89:03:17:50:3E:A4:2D:C9:76:6F:95:E5:C7:01:64:E1:DB:21:A2:08

X509v3 CRL Distribution Points:
Full Name:
URI:http://xxxx.xxxx.cajval.com.ar/CertEnroll/xxx.crl
URI:file://\\xxxx.xxxx.cajval.com.ar\CertEnroll\xxx.crl

Authority Information Access:
CA Issuers -
URI:http://xxxx.xxx.cajval.com.ar/CertEnroll/xxxx.xxx.cajval.com.ar_xxx.crt
CA Issuers -
URI:file://\\xxxx.xxx.cajval.com.ar\CertEnroll\xxxx.xxx.cajval.com.ar_xxx.crt
Signature Algorithm: sha1WithRSAEncryption
18:da:26:b8:ed:a4:30:7d:ef:ce:87:f0:5a:98:a0:e5:da:db:
70:35:9b:aa:c3:eb:c5:be:e0:be:2d:5d:14:e6:51:ab:2e:a3:
0a:68:a6:8a:66:53:ba:de:d8:4c:60:c8:c1:87:23:41:b3:c8:
d9:8d:32:34:2e:1d:35:a3:f1:ca:42:5f:b7:eb:98:da:e0:ed:
bc:b3:85:cb:4b:59:44:8f:e5:32:27:c8:66:16:eb:20:1b:f2:
b0:aa:4c:bd:bd:54:06:d0:b9:47:2d:8a:84:f1:92:bb:3d:df:
eb:b6:9a:e5:e7:68:67:44:59:d2:3b:a4:6b:40:7b:f3:43:1a:
fc:ef:73:61:87:87:a4:e3:16:af:2a:2c:11:f4:31:00:d5:76:
8b:6e:f0:ad:61:16:ac:6e:bb:c1:6a:47:2c:c4:2e:ec:8c:c2:
b8:69:c0:d2:e4:51:7f:d7:20:5a:82:4e:86:d8:80:a0:aa:e7:
a9:fe:81:b4:21:b4:86:2c:c7:1c:84:35:1f:c5:59:b1:be:2d:
64:4e:7b:5a:c7:94:f7:23:8c:3f:3b:f3:18:9e:c4:96:e4:04:
92:ae:50:75:2e:26:a1:48:5a:2e:a5:fc:59:09:e7:4f:d2:bc:
3f:21:9f:89:55:89:d4:74:c1:d4:7d:d6:53:1b:84:ff:63:4f:
fc:46:6e:b7:6e:93:cd:50:0f:59:a5:ae:46:c4:6a:da:0d:43:
04:fa:db:6e:fb:cf:56:86:d4:b3:e8:c3:47:31:82:50:64:39:
db:66:71:07:5d:06:6a:1e:a1:01:1e:b0:93:85:54:93:8c:b1:
5a:48:b9:9f:f9:2b:a9:ee:67:45:84:a9:dd:e7:0b:8b:ad:4e:
cc:5d:c2:7b:bd:72:d7:c2:14:19:63:54:92:dd:c0:67:44:35:
67:8d:3b:20:8e:3c:5c:19:f6:76:91:f8:fd:04:91:9e:fa:86:
ba:03:eb:cb:b7:9f:a2:03:52:97:40:c0:3b:26:8e:24:f3:43:
4e:8d:29:c1:60:0b:7d:4a:01:f5:c7:8e:a6:56:d5:01:70:b4:
11:42:a1:13:83:6a:43:51:5e:c5:bf:ca:c0:79:fa:c0:0c:1f:
3d:d8:82:62:c0:04:b0:88:fa:35:78:10:03:d7:29:1f:97:fe:
2b:5c:af:eb:6f:60:39:24:19:51:09:0f:0f:a4:67:7a:a0:e9:
29:28:65:d2:b1:8e:d0:ca:25:f7:18:78:1e:49:3b:a5:b6:c8:
9b:ca:d6:79:94:c2:b5:5f:2a:23:11:e9:97:9f:b1:dc:b4:40:
f3:33:6e:c3:12:97:9a:0a:cd:57:9a:a7:3a:c0:2a:40:5e:19:
8c:1f:b3:30:12:69:12:87

Certificate purposes:
SSL client : Yes
SSL client CA : No
SSL server : Yes
SSL server CA : No
Netscape SSL server : Yes
Netscape SSL server CA : No
S/MIME signing : Yes
S/MIME signing CA : No
S/MIME encryption : Yes
S/MIME encryption CA : No
CRL signing : Yes
CRL signing CA : No
Any Purpose : Yes
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
Time Stamp signing : No
Time Stamp signing CA : No

Formato del Certificado y Archivos a entregar

Formato de los certificados:

Todos los certificados deben ser entregados en formato (encoding) **BASE 64**. Además deben acompañar al certificado cliente, los certificados intermedios de su cadena de certificación (depende de cada entidad certificadora, puede tener ninguno, uno o más certificados intermedios) y el certificado de la CA root. Sin los certificados intermedios, si lo hubiera, y sin la CA root no funcionará la autenticación.

Todos estos certificados (cliente, autoridades intermedias, CA Root) en formato BASE64 = ASCII deben ser incluidos en un archivo ZIP.

El certificado del usuario / agente deberá generarse con un nombre distinto al de la Autoridad Certificante y su cadena.

Formato de archivos y zip:

1. Los certificados de la cadena de certificación (incluyendo el CA root = certificado raíz) deberán figurar teniendo en cuenta la siguiente nomenclatura:

Ejemplo: AG0000_CA_0.crt

AG ➔ Agente.
0000 ➔ Número de Agente dado de alta en los Sistemas Centrales. Ejemplo AG0099.
CA ➔ Cadena de certificación identificada numéricamente con **0 = certificado raíz.**

Este archivo zip deberá contener los certificados con **extensión *.crt ó .cer**

2. Si existiera una cadena de certificación intermedia habría que nombrar el archivo (numeración correlativa) de la siguiente manera:

Ejemplo: AG0000_CA_1.crt

AG ➔ Agente.
0000 ➔ Número de Agente dado de alta en los Sistemas Centrales. Ejemplo AG0099.
CA ➔ Cadena de certificación identificada numéricamente con **1 = intermedio.**

Este archivo zip deberá contener los certificados con **extensión *.crt ó .cer**

3. El Certificado Cliente (es el certificado que se compró o gestionó y recibieron firmado de la Autoridad de Certificación) que instalamos en nuestros servidores deberá figurar teniendo en cuenta la siguiente nomenclatura:

Ejemplo: AG0000_USER.crt

AG ➔ Agente.
0000 ➔ Número de Agente dado de alta en los Sistemas Centrales.
USER ➔ Nombre para identificar al certificado usuario **= comprado y firmado por autoridad certificante.**

Este archivo zip deberá contener los certificados con **extensión *.crt ó .cer**

A continuación se detallan ejemplos para cada caso mencionado.

Ejemplo de Certificado en formato BASE64.

-----BEGIN CERTIFICATE-----
MIIE0zCCA7ugAwIBAgIQGNrRniZ96LtKIVjNzGs7SjANBgkqhkiG9w0BAQUFADCBy
jELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQY
DVQQLExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjA
wNiBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwY
DVQQDEzxWZXJpU2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRp
b24gQXV0aG9yaXR5IC0gRzUwHhcNMDYxMTA4MDAwMDAwWhcNMzYwNzE2Mj
M1OTU5WjCByjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJb
mMuMR8wHQYDVQQLExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQ
LEzEoYykgMjAwNiBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvb
mx5MUUwQwYDVQQDEzxWZXJpU2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IEN
lcnRpZmljYXRpb24gQXV0aG9yaXR5IC0gRzUwggEiMA0GCSqGSIb3DQEBAQUAA4
IBDwAwggEKAoIBAQCvJAgIKXo1nmAMqudLO07cfLw8RRy7K+D+KQL5VwijZIUV
J/XxrcgxiV0i6CqqpkKzj/i5Vbext0uz/o9+B1fs70PbZmIVYc9gDaTY3vjgw2IIPVQT60nK
WVSFJuUrjxuf6/WhkcIzSdhDY2pSS9KP6HBRTdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw
9KIl8q8ckmcY5fQGBO+QueQA5N06tRn/Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxA
y3QkGSGT2RT+rCpSx4/VBEnkjWNHiDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP5
9zuDMKz10/NIeWiu5T6CUVAgMBAAGjgbIwga8wDwYDVR0TAQH/BAUwAwEB/zA
OBgNVHQ8BAf8EBAMCAQYwbQYIKwYBBQUHAQwEYTBfoV2gWzBZMFcwVRY
JaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQUj+XTGoasjY5rw8+AatRIGCx7GS4wJR
YjaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9nby5naWYwHQYDVR0OBBYEF
H/TZafC3ey78DAJ80M5+gKvMzEzMA0GCSqGSIb3DQEBBQUAA4IBAQCTJEowX2L

P2BqYLz3q3JktvXf2pXkiOOzEp6B4Eq1iDkVwZMXnl2YtmAl+X6/WzChl8gGqCBpH3
vn5fJJaCGkgDdk+bW48DW7Y5gaRQBi5+MHt39tBquCWIMnNZBU4gcmU7qKEKQsT
b47bDN0lAtukixlE0kF6BWlKWE9gyn6CagsCqiUXObXbf+eEZSqVir2G3l6BFoMtEMze
/aiCKm0oHw0LxOXnGiYZ4fQRbxC1lfznQgUy286dUV4otp6F01vvpX1FQHKOtw5rDg
b7MzVIcbidJ4vEZV8NhnacRHr2lVz2XTIIM6RUthg/aFzyQkqFOFSDX9HoLPKsEdao7
WNq
-----END CERTIFICATE-----