Incorporación de un nuevo certificado SSL para aplicaciones integradas con Notific@

Desarrollo CJAP

Caducidad certificados ssl ws031 CJAP

Sevilla, Octubre 2009

Motivo

Caducidad del certificado@ ssl de los servicios web de la Plataforma Notific@ Desarrollo de la Consejería de Justicia y Administración Pública.

Colectivo implicado

Todas las aplicaciones pertenecientes a Consejerías y Organismos públicos integrados con la Plataforma Notific@ Desarrollo, en concreto con sus servicios web (ws031.juntadeandalucia.es)

Fecha del cambio del certificado en la Plataforma Notific@ Desarrollo CJAP

22 de Octubre de 2009.

Procedimiento

Importar la clave pública del certificado raíz fntm.cer en el almacén de certificados o keystore de la aplicación integrada con Notific@ (fichero con extensión "cer" adjunto).

Es importante destacar, que dicho cambio en cada aplicación es independiente de la fecha en que se realice, siempre que se haga efectivo antes de la fecha límite del 22 de Octubre. La modificación a realizar es transparente para el correcto funcionamiento de la aplicación en cada organismo concreto.

NOTA: La clave pública del certificado que va a caducar (ws031.cer) y la nueva (fichero fnmt.cer adjunto) pueden convivir sin problemas en el almacén de certificados, no siendo necesario borrar la antigua.

Método 1 <En la línea de comandos, usando el programa keytool de java>

>keytool -import –alias fnmtraiz -file fnmt.cer -keystore

$rutaAlKeystoreDeLaAplicacion/nombreAlmacenDeCertificados

IMPORTANTE: Es necesario asegurarse del keystore que usa la aplicación, a fin de que tome la aplicación la nueva clave pública incluida.

Ejemplo de importación en un servidor Windows 2003 Server usando jdk1.6, suponiendo que el keystore de la aplicación es el fichero cacerts. La contraseña por defecto del fichero cacerts es changeit

C:\Archivos de programa\Java\jdk1.6.0_15\jre\lib\security>keytool -import -alias

fnmtraiz -file fnmt.cer -keystore cacerts

Escriba la contraseña del almacén de claves:

Propietario: OU=FNMT Clase 2 CA, O=FNMT, C=ES

Emisor: OU=FNMT Clase 2 CA, O=FNMT, C=ES

Número de serie: 36f11b19

Válido desde: Thu Mar 18 15:56:19 CET 1999 hasta: Mon Mar 18 16:26:19 CET 2019

Huellas digitales del certificado:

MD5: 25:9D:CF:5E:B3:25:9D:95:B9:3F:00:86:5F:47:94:3D

SHA1: 43:F9:B1:10:D5:BA:FD:48:22:52:31:B0:D0:08:2B:37:2F:EF:9A:54

Nombre del algoritmo de firma: SHA1withRSA

Versión: 3

Extensiones:

#1: ObjectId: 2.5.29.16 Criticality=false

PrivateKeyUsage: [

From: Thu Mar 18 15:56:19 CET 1999, To: Mon Mar 18 15:56:19 CET 2019]

#2: ObjectId: 2.5.29.15 Criticality=false

KeyUsage [

Key_CertSign

Crl_Sign

]

#3: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

0000: 40 9A 76 44 97 74 07 C4 AC 14 CB 1E 8D 4F 3A 45 @.vD.t.....O:E

0010: 7C 30 D7 61   .0.a

]

]

#4: ObjectId: 1.2.840.113533.7.65.0 Criticality=false

#5: ObjectId: 2.5.29.31 Criticality=false

CRLDistributionPoints [

[DistributionPoint:

[CN=CRL1, OU=FNMT Clase 2 CA, O=FNMT, C=ES]

]]

#6: ObjectId: 2.5.29.19 Criticality=false

BasicConstraints:[

CA:true

PathLen:2147483647

]

#7: ObjectId: 2.16.840.1.113730.1.1 Criticality=false

NetscapeCertType [

SSL CA

S/MIME CA

Object Signing CA]

#8: ObjectId: 2.5.29.35 Criticality=false

AuthorityKeyIdentifier [

KeyIdentifier [

0000: 40 9A 76 44 97 74 07 C4 AC 14 CB 1E 8D 4F 3A 45 @.vD.t.....O:E

0010: 7C 30 D7 61 .0.a

]

┐ Confiar en este certificado? [no]: si (Debemos responder si)

Se ha añadido el certificado al almacén de claves

Ya la tenemos incluida, verificamos que se ha incluido correctamente la clave pública en el keystore:

C:\Archivos de programa\Java\jdk1.6.0_15\jre\lib\security>keytool -list -keystore cacerts

Escriba la contraseña del almacén de claves:

Tipo de almacén de claves: JKS

Proveedor de almacén de claves: SUN

Su almacén de claves contiene 72 entradas

——digicertassuredidrootca, 07-ene-2008, trustedCertEntry,

Huella digital de certificado (MD5): 87:CE:0B:7B:2A:0E:49:00:E1:58:71:9B:37:A8:9

3:72

trustcenterclass2caii, 07-ene-2008, trustedCertEntry,

Huella digital de certificado (MD5): CE:78:33:5C:59:78:01:6E:18:EA:B9:36:A0:B9:2

E:23

thawtepremiumserverca, 12-feb-1999, trustedCertEntry,

Huella digital de certificado (MD5): 06:9F:69:79:16:66:90:02:1B:8C:8C:A2:C3:07:6

F:3A

swisssignsilverg2ca, 13-ago-2008, trustedCertEntry,

Huella digital de certificado (MD5): E0:06:A1:C9:7D:CF:C9:FC:0D:C0:56:75:96:D8:6

2:13

swisssignplatinumg2ca, 13-ago-2008, trustedCertEntry,

Huella digital de certificado (MD5): C9:98:27:77:28:1E:3D:0E:15:3C:84:00:B8:85:0

3:E6

equifaxsecureebusinessca2, 18-jul-2003, trustedCertEntry,

Huella digital de certificado (MD5): AA:BF:BF:64:97:DA:98:1D:6F:C6:08:3A:95:70:3

3:CA

equifaxsecureebusinessca1, 18-jul-2003, trustedCertEntry,

Huella digital de certificado (MD5): 64:9C:EF:2E:44:FC:C6:8F:52:07:D0:51:73:8F:C

B:3D

thawteserverca, 12-feb-1999, trustedCertEntry,

Huella digital de certificado (MD5): C5:70:C4:A2:ED:53:78:0C:C8:10:53:81:64:CB:D
0:1D

utnuserfirstclientauthemailca, 02-may-2006, trustedCertEntry,

Huella digital de certificado (MD5): D7:34:3D:EF:1D:27:09:28:E1:31:02:5B:13:2B:D
D:F7

thawtepersonalfreemailca, 12-feb-1999, trustedCertEntry,

Huella digital de certificado (MD5): 1E:74:C3:86:3C:0C:35:C5:3E:C2:7F:EF:3C:AA:3
C:D9

utnuserfirsthardwareca, 02-may-2006, trustedCertEntry,

Huella digital de certificado (MD5): 4C:56:41:E5:0D:BB:2B:E8:CA:A3:ED:18:08:AD:4
3:39

entrustevca, 28-abr-2009, trustedCertEntry,

Huella digital de certificado (MD5): D6:A5:C3:ED:5D:DD:3E:00:C1:3D:87:92:1F:1D:3
F:E4

certumca, 10-feb-2009, trustedCertEntry,

Huella digital de certificado (MD5): 2C:8F:9F:66:1D:18:90:B1:47:26:9D:8E:86:82:8
C:A9

addtrustclass1ca, 02-may-2006, trustedCertEntry,

Huella digital de certificado (MD5): 1E:42:95:02:33:92:6B:B9:5F:C0:7F:DA:D6:B2:4
B:FC

equifaxsecureca, 18-jul-2003, trustedCertEntry,

Huella digital de certificado (MD5): 67:CB:9D:C0:13:24:8A:82:9B:B2:17:1E:D1:1B:E

C:D4

quovadisrootca3, 09-jun-2009, trustedCertEntry,

Huella digital de certificado (MD5): 31:85:3C:62:94:97:63:B9:AA:FD:89:4E:AF:6F:E

0:CF

quovadisrootca2, 09-jun-2009, trustedCertEntry,

Huella digital de certificado (MD5): 5E:39:7B:DD:F8:BA:EC:82:E9:AC:62:BA:0C:54:0

0:2B

digicerthighassuranceevrootca, 07-ene-2008, trustedCertEntry,

Huella digital de certificado (MD5): D4:74:DE:57:5C:39:B2:D3:9C:85:83:C5:C0:65:4

9:8A

secomvalicertclass1ca, 01-may-2008, trustedCertEntry,

Huella digital de certificado (MD5): 65:58:AB:15:AD:57:6C:1E:A8:A7:B5:69:AC:BF:F

F:EB

equifaxsecureglobalebusinessca1, 18-jul-2003, trustedCertEntry,

Huella digital de certificado (MD5): 8F:5D:77:06:27:C4:98:3C:5B:93:78:E7:D7:7D:9

B:CC

verisignclass3ca, 27-oct-2003, trustedCertEntry,

Huella digital de certificado (MD5): 10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:6

7:67

deutschetelekomrootca2, 06-nov-2008, trustedCertEntry,

Huella digital de certificado (MD5): 74:01:4A:91:B1:08:C4:58:CE:47:CD:F0:DD:11:5

3:08

verisignclass2ca, 27-oct-2003, trustedCertEntry,

Huella digital de certificado (MD5): B3:9C:25:B1:C3:2E:32:53:80:15:30:9D:4D:02:7

7:3E

utnuserfirstobjectca, 02-may-2006, trustedCertEntry,

Huella digital de certificado (MD5): A7:F2:E4:16:06:41:11:50:30:6B:9C:E3:B4:9C:B

0:C9

fnmtraiz, 05-oct-2009, trustedCertEntry,

Huella digital de certificado (MD5): 25:9D:CF:5E:B3:25:9D:95:B9:3F:00:86:5F:47:9

(…) Continua …

Método 2

A través de cualquier interfaz gráfica existente de keytool.

En ambos métodos, posteriormente es imprescindible reiniciar el servidor de aplicaciones concreto, para que tomen efecto los cambios realizados.

Posibles Incidencias

- Es importante destacar, que el cambio es independiente de la fecha en que se realice, siempre antes de la fecha límite de cambio de los servidores de Notific@ Desarrollo CJAP, y transparente para el correcto funcionamiento de la aplicación en el organismo concreto.
- *Cualquier aplicación que no realice dicha modificación antes de la fecha en la que se realice el cambio de certificado en la Plataforma no podría hacer uso de los servicios webs de Notific@ Desarrollo CJAP.*
- Es necesario asegurarse del keystore que usa la aplicación, y programar el reinicio del servidor/es de aplicaciones tras el cambio, a fin de que la aplicación tome los cambios realizados.