Migración proveedor de certificados de SCS

Migración del proveedor de certificados SCS

1.- Se va a producir un cambio en el proveedor de firma de certificados del servicio SCS, los certificados firmados hasta ahora por Cybertrust pasarán a ser firmados por la CA de COMODO. Estos cambios fueron anunciados en los pasados grupos de trabajo en Málaga:

http://www.rediris.es/gt/gt2009/ponencias/gt2009-gt-scs.pdf

2.- Aunque puede que a priori los certificados firmados por Cybetrust tengan una validez posterior, estos serán revocados en febrero de 2010. Hay por tanto tiempo para hacer la transición hasta dicho momento. Pasada dicha fecha, los certificados pueden seguir siendo 'válidos' hasta su fecha de caducidad si el cliente no hace verificación de la revocación del mismo por medio de la CRL de Cybertrust...

(recomendamos no evitar esta comprobación como 'solución' o apaño en los casos en los que se pueda...).

3.- Este cambio en la autoridad de certificación puede suponer problemas debido a la configuración que tienen los clientes, que podrían dejar de funcionar de una de las siguientes maneras:

- 3.1.- Denegando la conexión entre el cliente y un servidor cuyo certificado haya sido revocado por Cybertrust.
- 3.2.- Pidiendo al usuario (popup) que acepte un certificado que no es válido. El usuario podría aceptar dicho certificado (y conectarse) o rechazarlo (y no conectarse mientras siguiera dicho certificado instalado en el servidor).

4.- Las soluciones pasan por tanto por:

- 4.1.- Solicitar un certificado con tiempo suficiente para poder hacer la transición lo más suavemente posible. Avisaremos del momento en el que se puedan solicitar certificados firmados por la nueva CA de COMODO.
- 4.2.- Introducir en los clientes de los usuarios la nueva autoridad de certificación y fijar una fecha para la realización del cambio en el certificado del servidor.
- 4.3.- Informar a los usuarios en caso de que necesiten actualizar el software de conexión antes de la fecha del cambio (o en la fecha del cambio si no es posible antes).
- 4.4.- Informar a los usuarios del cambio que tendrán que realizar en la configuración de sus clientes cuando no se trate de un kit de instalación desatendida.

Solución del problema para distintos clientes

1.- SecureW2 con kit de instalación

SecureW2 soporta la posibilidad de activar dos autoridades de certificación en la configuración de kits de autoinstalación, lo cual se haría:

```
VerifyServerCertificate = TRUE
```

```
ServerName = uam.es
```

```
; GTE
```

```
TrustedRootCA.0 = 97817950d81c9670cc34d809cf794431367ef474
```

```
; COMODO
```

```
TrustedRootCA.1 = 6631bf9ef74f9eb6c9d5a60cba6abed1f7bdef7b
```

2.- SecureW2 sin kit de instalación.

Es posible también configurar manualmente dos autoridades de certificación en SecureW2 de modo manual:

También es posible no seleccionar ninguna CA en SecureW2:

3.- Cliente de redes de Microsoft.

Por defecto trae ambas CAs, pero en las instrucciones facilitadas a los usuarios suele pedírsele aceptar todas las CAs instaladas, o aceptar la CA de Cybertrust. Estudiar los distintos "sabores" de windows y su situación:

- Windows XP
- Windows Vista
- Otros windows...