Preguntas frecuentes servicio SCS.

1. ¿Qué aplicaciones y/o dispositivos soportan los certificados SCS?

Web Browsers *(con soporte EV)*

Apple Safari 3.2+, Google Chome 1.0+, Microsoft Internet Explorer 7.0+. Mozilla Firefox 3.0+, Opera 9.5+

Web Browsers *(sin soporte EV)*

Apple Safari 1.2+, AOL 5.0+. Camino 1.0+, Google Chrome 1.0+, KDE Konqueror, Microsoft Internet Explorer 5.01+, Mozilla Firefox 1.0+, Netscape Communicator 4.77+, Opera 7.0+

Clientes de correo *(S/MIME)*

Apple Mail, Lotus Notes *(6+)*, Microsoft Outlook 99+, Microsoft Outlook Express 5.0+, Microsoft Entourage, Microsoft Windows Mail 1.0+, Mozilla Thunderbird 1.0+, Qualcomm Eudora 6.2+, The Bat 1,0+

PDAs

ACCESS NetFront 3.4+. Apple iPhone 1.0+, KDDI Openwave v6.2.0.12+, Microsoft Windows Mobile 5.0+, Nintendo Wii, NTT DoCoMo, Opera Mini 3.0+, Opera Mobile 6.0+, RIM Blackberry v4.2.1+, Sony Playstation 3, Sony Playstation Portable

Otras aplicaciones

Adobe AIR, Microsoft Authenticode, Microsoft Office, Microsoft Visual Basic for Applications, Mozilla Suite 1.0+, Sea Monkey, Sun Java SE 1.4.2+,
Desafortunadamente, la CA raíz de COMODO no se encuentra pre-instalada en el sistema operativo Symbian usado por muchos dispositivos Nokia y Sony Ericsson. Sin embargo puede ser añadida la CA raíz de comodo, descargándola e instalándola.

2. ¿Se pueden solicitar certificados con longitud de clave de 1024 bits?

No. En diciembre de 2010 Comodo anunció que no emitirá certificados con claves que tengan menos de 2048 bits.

3. ¿Se pueden solicitar certificados wildcard?

Sí, el servicio actual permite la solicitud de certificados wildcard "*".

4. ¿Pueden coexistir dos certificados con el mismo DN?

Sí. No hay ningún problema en que se soliciten varios certificados con el mismo DN.

5. ¿Cómo renuevo un certificado?

No existe un proceso específico para la renovación de certificados ya que es posible solicitar tantos certificados con el mismo DN como se deseen. Recomendamos solicitar certificados cada dos años e ir reemplazando los antiguos.

Puntos a tener en cuenta:

- Solicitar el certificado por un maximo de 3 años pero reemplazarlo cuando transcurran 2 años.
- No reutilizar la misma CSR
- Una vez instalado el nuevo certificado se debe solicitar la revocación del antiguo y eliminar cualquier copia del obsoleto.

6. Ya he recibido el certificado que he solicitado, ¿cómo lo instalo para el servicio?

Existe una Guía Básica de instalación de certificados SCS, que indica como instalar un certificado en los servicios más comunes.

7. Quiero firmar una aplicación Java utilizando el certificado de firma de código. ¿Cómo lo hago?

Si tiene un PKCS12 ya puede utilizarlo como almacén *(*keystore*)* en Java. Quizás sea lo más cómodo.

Para ver el alias de tu certificado:

```
keytool -list -v -storetype PKCS12 -keystore <ficheroPKCS12>
```

Para firmar un JAR:

```
jarsigner -storetype PKCS12 -keystore <ficheroPKCS12> -signedjar
<ficheroFirmado.jar> <ficheroOriginal.jar> <aliasCertificado>
```

Se recomienda no usar certificados que contengan tilde, eñes, ... ya que se han dado casos en los que el jarsigner no los interpreta bien, y tras firmar el applet, los navegadores no consiguen ejecutar el applet por errores de utf8.

8. ¿Qué es el CA/Browser Forum?

CA/Browser Forum es una organización formada por autoridades de certificación *(*CAs*)* y vendedores de software de navegador de Internet y otras aplicaciones.
Los miembros del CA/Browser Forum han colaborado estrechamente en la definición de directrices e implementación de los mecanismos de validación extendida *(*EV*)* de certificados SSL como una manera de proporcionar una mayor seguridad para las transacciones por Internet y la creación de un método más intuitivo de visualizar sitios seguros a los usuarios de Internet.

9. Tengo una duda, pero no está resuelta en este FAQ.

Por favor, envíenosla para que podamos resolvérsela y añadirla a este FAQ.

10. ¿Hay algún otro FAQ en TERENA?

TERENA mantiene un FAQ relativo al servicio TCS que puede consultar.

http://www.terena.org/activities/tcs/faq/