Normativa del servicio de certificados de servidor.

1.- Introducción.

1.1 Objeto del documento.

El objetivo de este documento es definir el proceso de solicitud y ciclo de vida de certificados digitales de servidor SSL.

Los certificados emitidos deben usarse exclusivamente para el acceso seguro a recursos propios de la institución en tanto en cuanto a sus actividades académicas y de investigación.

Antes de solicitar un certificado se debe conocer el contenido de esta normativa, y es recomendable conocer también la Declaración de Prácticas de Certificación (DPC) del Prestador de Servicios de Certificación (PSC) http://www.terena.org/activities/tcs/repository/cps-server.pdf , con el objeto de conocer los diversos aspectos técnicos sobre todo de seguridad y funcionalidad para prevenir incidencias, los operativos en concreto de gestión y mantenimiento, y legales como las obligaciones y responsabilidades que conlleva la custodia de este tipo de certificados.

El servicio es prestado por CTU-UNED y RedIRIS en términos no comerciales para sus usuarios de la comunidad investigadora y académica, por lo que no cabe reclamar responsabilidad a CTU-UNED, RedIRIS y Terena en relación con la prestación de dichos servicios.

1.2 Comunidad y ámbito de aplicación

El servicio es prestado, por CTU-UNED a través de RedIRIS actuando ambas como AR o Autoridades de Registro de Terena TCS, que actúa como Autoridad de Certificación subordinada de UserTrust, siendo dicha Autoridad de Certificación alojada y operada por Comodo CA Limited.

CTU-UNED

Gestiona la emisión de certificados digitales del prestador de servicios de certificación COMODO http://www.comodo.com/, emitidos a través de un convenio con:

- RedIRIS **http://www.rediris.es/scs/**

- Terena **http://www.terena.org/activities/tcs/repository/**

CTU-UNED actuará como RA o Autoridad de Registro intermedia delegada, ofreciendo el servicio de forma gratuita a la comunidad que conforma el dominio RedUNED.

Para solicitar un certificado, los solicitantes deberán dirigir la petición al servicio CAU del CTU-UNED Utilizando un procedimiento de autenticación, por el que los solicitantes deben identificarse firmando digitalmente el formulario de solicitud de servicio.

Cualquier duda sobre este documento, o en general, con los certificados digitales de servidor pueden resolverse enviando un correo electrónico al CAU.

Solicitantes

Es la persona, física o jurídica, que requiere un certificado de servidor, puede ser también el suscriptor del certificado. Será el principal interlocutor con el CTU y deberá comunicar el mismo cualquier circunstancia que afecte a algún certificado por el solicitado.

Actualmente, CTU-UNED sólo gestiona la emisión de certificados digitales de servidor a departamentos de servicios centrales, facultades, departamentos o centros de investigación que estén dentro del ámbito o vinculados de forma directa con RedUNED.

Suscriptor

El suscriptor es el sujeto, persona física o jurídica, que solicita la emisión de un certificado para un servidor y por tanto asume la responsabilidad última por el uso de la clave privada asociada con el certificado de clave pública.

Por lo general también será el solicitante del certificado.

Aplicabilidad

Los certificados de servidor permiten el aseguramiento de las comunicaciones a través de internet, entablando canales cifrados de comunicación Secure Sockets Layer, en adelante SSL.

Estos certificados no pueden ser utilizados para usos distintos a los previstos, no asumiendo CTU-UNED ninguna responsabilidad en estos casos.

CAU - Detalles de contacto

Las peticiones del servicio así como cualquier sugerencia o duda relacionada con este

Servicio se tramitaran a través del CAU.

2.- Tipos de certificados.

Certificado SSL de servidor que se pueden solicitar, se pueden dividir en 2 sub-perfiles:

- TERENA SSL certificate - Certifica un solo nombre de DNS
- TERENA SSL multi-domain SSL certificate - Certifica hasta 100 nombres de DNS

Certificado de firma de código

- Permiten firmar digitalmente software ejecutable.
- Solicitud pre-validada por el vicerrectorado de tecnología.

2.1. Certificados de servidor SSL

Los certificados emitidos bajo este perfil permiten autenticar servidores y establecer conexiones seguras con los clientes. Este tipo de certificados son X. 509 versión 3.

2.1.1 Certificados SSL

Es un certificado SSL en el que la información que se ha validado está limitada al dominio en el cual el sitio web está localizado. Algunas de sus características son:

- Certificados SSL de servidor con 1 único CN y sin SubjectAltNames
- Sólo sirven para asegurar nombres de dominios completos o FQDNs
- No se deben incluir valores en el SubjectAltName.
- Se verifica únicamente la propiedad del dominio que se está certificando.
- Proporciona una protección de alto nivel de 128/256 bits de encriptación.
- Puede ser utilizado para las transacciones financieras.
- El CN no debe contener el carácter "*"
- Longitud mínima de clave RSA: 2048 b.

2.2.3 Certificados SSL Multi-Domain

Este tipo de certificados tienen las mismas características que los anteriores, pero además del CN principal puede certificar varios nombres alternativos.

Este tipo de certificados tienen las mismas características que los SSL DV Multi-domain, son de la forma: **O=UNED, C=ES, CN=www.org.es., SubjAltName1=www1.uned.es, SubjAltName1=www2.uned.es,…**

- Certificados SSL de servidor para 1 CN y SubjectAltNames
- La CSR no debe incluir el CN entre los valores del SubjectAltName
- CN y SubjectAltNames NO deben contener el carácter "*"

2.2.5 Certificados de firma de código

Este tipo de certificados se utiliza para firmar código ejecutable, como Java Script, evitándose que salten pantallas y alertas al no reconocerse el fabricante del software.

Se piden de forma extraordinaria mediante el proceso normal de solicitud de servicios al CAU, pero la petición debe:

- Solicitarla el director o jefe del departamento o grupo de investigación.
- La solicitud debe venir acompañada de una memoria explicativa que justifique la necesidad de dicho certificado.
- La solicitud debe ser aprobada por el vicerrectorado de tecnología.

- El uso y custodia de este tipo de certificados deben ser especialmente cuidadoso y estar restringido a un único operario o suscriptor.

2.3 Raíces de confianza

Comodo proporciona una CA específica para cada perfil de certificado, bajo el servicio de certificados digitales que ofrece RedIRIS. Cada CAs ha sido emitida a su vez por una CA autofirmada que están ampliamente distribuida entre los clientes web más comunes.

2.3.1Certificados para servidor

Después del 08/10/2014, cadena de certificados: TERENA SSL2 PATH. Sólo se incluyen los certificados marcados con (*).

```
End Entity SSL (serial number = x,
|  expiry = 1, 2, 3 years from issuance)
|
+- TERENA SSL CA 2 [DER|PEM] (*)
   |  (subject = /C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA SSL CA 2
   |   serial number = 00:b0:ff:cf:3a:1d:82:44:98:15:62:9d:64:88:6a:41:65,
   |   expiry = 8 Oct 2024)
   |
   +- USERTrust RSA Certification Authority [DER|PEM] (*)
      |  (serial number = 13:ea:28:70:5b:f4:ec:ed:0c:36:63:09:80:61:43:36,
      |   expiry 30 May 2020)
      |
      +- AddTrust External CA Root [DER|PEM]
         (serial number = 1,
          expiry = 30 May 2020)
```

2.3.2 Certificados para firma de código

Los certificados emitidos bajo este perfil permiten autenticar software distribuido por Internet.

Desde el 08/10/2014, cadena de certificados: TERENA Code Signing 2 PATH. Sólo se incluyen los certificados marcados con (*).

```
End Entity SSL (serial number = x,
|  expiry = 1, 2, 3 years from issuance)
|
+- TERENA Code Signing CA 2 [DER|PEM] (*)
   |   (subject = /C=NL/ST=Noord-Holland/L=Amsterdam/O=TERENA/CN=TERENA
Code Signing CA 2
   |   serial number = c9:25:e1:df:fb:e3:36:6d:5c:e4:f5:15:c4:76:63:09,
   |   expiry = 8 Oct 2024)
```

```
   |
   +- USERTrust RSA Certification Authority [DER|PEM] (*)
      |                          (serial              number              =
13:ea:28:70:5b:f4:ec:ed:0c:36:63:09:80:61:43:36,
      |   expiry = 30 May 2020)
      |
      +- AddTrust External CA Root [DER|PEM]
         (serial number = 1,
          expiry = 30 May 2020)
```

3. Solicitud de Certificados

La solicitud de certificados SCS se realiza a través del sistema de petición de servicios del CAU. Existiendo dos protocolos de solicitud, según quien genere el CSR*, el CTU-UNED o el solicitante, en ambos casos deberá rellenar y enviar al CAU el formulario de solicitud.

http://portal.uned.es/pls/portal/url/ITEM/DF6C3F5A27D00C42E040660A33700964

CTU-UNED y RedIRIS, en la tramitación de las diferentes actuaciones relativas a la emisión de los certificados de servidor SCS, actuará tomando en consideración los datos comunicados por el Solicitante. Cualquier falsedad o error en los datos consignados en la solicitud podrá ser causa de desestimación de la misma.

CTU-UNED y RedIRIS (Red.es) observará en el tratamiento de los datos personales de las personas y entidades mencionadas lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y normativa de desarrollo, en relación con la solicitud y emisión de certificados de servidor SCS.

Los derechos de acceso y rectificación podrán ejercerse de acuerdo con lo dispuesto en la normativa de protección de datos de carácter personal. Los derechos de cancelación y oposición únicamente podrán ejercerse previa revocación del certificado de servidor SCS correspondiente, dado que el tratamiento de los datos personales por parte de Red.es es necesario para la emisión de certificados de servidor SCS.

*** CSR:** Certificate Signing Request, certificado aún no firmado por la autoridad de certificación.

3.1. El CTU genera CSR

En este caso únicamente deberá hacer llegar al CAU el PDF de la petición de servicios firmada y cumplimentada marcando la casilla **'Clave privada',**

Si desea que la clave privada vaya protegida por contraseña, deberá marcar la casilla 'Contraseña', indicando así su deseo de que dicha clave vaya protegida por una contraseña.

Si en la solicitud expresa su deseo de que dicha clave este protegida por contraseña, tenga en cuenta que algunos sistemas por razones de automatismos desaconsejan el uso de dicha protección, ya que deberá introducirse manualmente cada vez que se vaya a hacer uso de la clave, como por ejemplo al iniciar un servidor web Apache. Dicha clave puede posteriormente deshabilitarse o habilitarse según las instrucciones que al efecto estarán disponibles.

https://descargas.uned.es/intranet/pdf/2015-04-08-CTU-SEGURIDAD-MANUS-Instrucciones_certificado_SSL_x509_V1.pdf

Se le hará llegar de vuelta un fichero de exportación de certificados o PKCS#12 (con extensión PFX en sistemas Windows o P12 en el resto), que contendría las claves del certificado. Dicho archivo obligatoriamente irá protegido por el contraseña, que le será comunicada por un medio diferente al que se utilice para el envío del archivo PKCS#12.

Una vez instalado el certificado en el servidor, y se haya probado que cumple con los propósitos requeridos, el suscriptor deberá comunicarlo al CTU-UNED, que procederá a destruir toda copia del certificado en especial de la clave privada. Se mantendrá únicamente una copia del CSR y de la clave pública.

3.2. El CSR es suministrado por el solicitante

En este caso deberá hacer llegar dos documentos al CAU:

- Solicitud en PDF cumplimentada y firmada digitalmente por el peticionario.

- CSR en formato texto plano.

Generación del par de claves y CSR.

Los pares de claves de los certificados de las entidades finales son generados por los propios solicitantes, quienes envían a continuación el archivo CSR (clave pública sin firmar) al CTU-UNED para que gestione la firma.

El solicitante debe generar el par de claves utilizando cualquier dispositivo criptográfico seguro, como alguno de los módulos criptográficos normalizados integrados en sistemas operativos o aplicaciones informáticas de amplio uso.

La política de certificación del perfil de certificados SSL de la Autoridad de Certificación COMODO, declara como componentes válidos del subjectDN los siguientes RDNs:

- **C** country of the Organization
- **ST** State of the Organization (optional)
- **L** Locality of the Organisation (optional)
- **O** Organisation Name
- **OU** Organisational Unit Name (optional)
- **CN** Contains a domain name
- **unstructuredName** Contains a domain name (optional)

Como se puede observar, algunos RDNs son obligatorios y otros optativos, de forma que si genera una CSR cuyo subjectDN no incluye todos los RDNs obligatorios (**C**, **O**, **CN**), ésta será rechazada.

Consulte las guías sobre como generar el CSR disponibles en www.uned.es/scs. De no existir para su sistema en concreto consulte con el CAU.

3.2.1. Solicitud de certificados SSL.

En este caso los certificados contendrán un único nombre de dominio o FQDN a certificar.

https://descargas.uned.es/intranet/pdf/2015-04-08-CTU-SEGURIDAD-MANUS-Instrucciones_certificado_SSL_x509_V1.pdf

3.2.2 Solicitud de certificados Multidomain

Disponemos de 2 opciones para la generación de la CSR:

- Herramienta de generación o ShellScript (Solo Linux).
- Comandos OpenSSL.

Uso de la herramienta scs-genCSR.sh (Linux).

Para generar las CSR podemos hacerlo mediante un Shell script (Linux). Tiene disponibles diferentes versiones dependiendo del algoritmo que use:

- scs-genCSR.sh - SHA-256 y UTF-8 por defecto)
  http://www.rediris.es/scs/util/scs-genCSR.sh
- scs-genCSR-sha2.sh - SHA-256
  http://www.rediris.es/scs/util/scs-genCSR-sha2.sh

Los cuales de forma automática nos preguntará todos los campos que conforman el DN del certificado, así como los subjectAltName (tantos como deseemos). El mismo programa genera la clave privada y la CSR.

Ambos casos están desarrollados en la guía:

https://descargas.uned.es/intranet/pdf/2015-04-08-CTU-SEGURIDAD-MANUS-Instrucciones_certificado_SSL_x509_multidomain_V1.pdf

4.- Envío de documentación

Deberá enviar la documentación requerida mediante correo electrónico al CAU.

5.- Proceso de entrega

Todos los ficheros que se envíen desde el CTU se harán llegar a los suscriptores mediante correo electrónico firmado, e irán empaquetados en un archivo ZIP o similar protegidos por la contraseña.

Si desea que dicho correo electrónico también vaya cifrado deberá proporcionar en el momento de la solicitud su certificado público personal, enviándolo como adjunto e indicando expresamente dicho deseo.

Una vez lo haya recibido, siga los pasos de las siguientes guías para la correcta configuración:

Linux - Apache: https://descargas.uned.es/intranet/pdf/2015-04-08-CTU-SEGURIDAD-MANUS-instalacion_de_certificado_y_cadena_de_confianza_en_Apache_V2.pdf

MS Windows IIS 7: http://technet.microsoft.com/es-es/library/cc732230(v=ws.10).aspx

MS Cadena de Confianza:

https://descargas.uned.es/intranet/pdf/20150408-CTU-SEGURIDAD-MANUS-Configuracion_cadena_confianza_IIS.pdf

Una vez haya sido instalado y este probado el buen funcionamiento del certificado deberá comunicarlo mediante correo electrónico. Principalmente si ha solicitado que el CTU le genere la clave privada, para que se proceda a su destrucción.

6.- Proceso de renovación

Los certificados solicitados se emiten por defecto con un tiempo de **vigencia de 36 meses o 3 años.**

Se recomienda generar nuevas claves privadas y una nueva solicitud a los 24 meses.

El servicio de certificación del CTU-UNED contactara no obstante con el suscriptor cuando queden 3 meses para la expiración de la vigencia del certificado. Y de forma urgente a un mes de la expiración.

Si se emite un certificado nuevo para el mismo FQDN ambos serian perfectamente válidos, mientras no hayan caducado ni hayan sido revocados expresamente, por lo que tendrá un tiempo para probar el nuevo certificado renovado. Una vez haya hecho las pruebas pertinentes es recomendable borrarlo del sistema y de cualquier copia de seguridad que pudiera existir y solicitar la revocación del certificado desechado.

7.- Proceso de revocación

Si por algún motivo necesitara revocar un certificado deberá ponerse en contacto con el CAU que le guiara sobre los pasos a seguir.

De necesitarse la revocación de forma urgente, como p.ej. que sospeche que las claves han sido comprometidas, se puede mandar al mismo tiempo que se avisa al CAU un mail a la cuenta: admin.caroot@csi.uned.es.

Igualmente si el servidor o el/los FQDN a certificar dejaran de existir, se deberá avisar al CTU-UNED de dicha circunstancia.

En caso de grave negligencia técnica, los certificados de servidor pueden ser revocados.

Los certificados no serán utilizados de manera alguna en caso de revocación de los mismos, recomendándose eliminarlos una vez revocados.

Glosario de términos

Vocablo	Significado
AR	**Autoridad de Registro. Es una entidad que no firma certificados ni CRL, pero tiene la responsabilidad de registrar y/o verificar, total o parcialmente, la información que necesita un PSC para emitir certificados y CRL. También puede realizar otras funciones.**
Certificado digital	**Documento electrónico que vincula unos datos de verificación de firma a un signatario y confirma su identidad.**
Clave privada	**En un criptosistema asimétrico, es aquella que se utiliza para firmar digitalmente.**
Clave pública	**En un criptosistema asimétrico, es aquella que se utiliza para verificar digitalmente.**
Criptosistema asimétrico	**Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar esa firma digital.**
CRL	**Lista de Certificados Revocados (Certificate Revocation List). Lista firmada digitalmente y emitida por PSC para identificar los certificados que han sido revocados pero todavía no han expirado.**
CSR	**Certificate Signing Request, petición de firma de certificado, archivo que una vez firmado por una Autoridad de Certificación se convierte en un Certificado Publico.**
Compromiso clave	**Incidente de seguridad por el que la clave queda expuesta o potencialmente expuesta a un acceso no autorizado.**
DN	**Distinghuised Name. Conjunto de valores que identifican el certificado.**
DPC	**Declaración de Prácticas de Certificación. Documento que describe las prácticas de emisión de certificados empleadas por un PSC.**

Vocablo	Significado
Entidad final	**Persona, física o jurídica, titular de un certificado digital que no puede emitir otros certificados, es decir, que no es un PSC.**
Firma electrónica	**Conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recibe.**
Jerarquía PKI	**Conjunto de PSC cuyas funciones están organizadas de forma común, conforme al principio de delegación de autoridad del PSC de nivel superior al inferior y así sucesivamente.**
OID	**Identificador Digital de Objetos (Object Identifier Digital). Valor numérico (distinguible de cualquier otro valor) asociado con un objeto.**
Par de claves	**Clave privada y su correspondiente clave pública en un criptosistema asimétrico, tal que la clave pública puede verificar una firma digital creada por la clave privada.**
PKCS#10	**Public Key Cryptograpy Standard. Estándar que define la estructura de las solicitudes de emisión de certificados.**
PKI	**Public Key Infrastructure. Conjunto de productos, políticas y procedimientos para crear, gestionar, distribuir, almacenar y revocar certificados digitales.**
Política de Certificados	**Conjunto de normas que indican la aplicabilidad de un certificado a una comunidad de usuarios determinada y/o los tipos de aplicación o uso de certificados con requisitos comunes de seguridad.**
PSC	**Prestador Servicios Certificación. Entidad que emite certificados digitales (especialmente en formato X.509) y garantiza la veracidad de los datos del certificado.**
Revocación	**Acción de dejar sin efecto en forma permanente un certificado a partir de una fecha cierta, publicándolo en la CRL.**
SCD	**Signature Creation Device. Dispositivo de creación de firma.**

Vocablo	Significado
SSCD	**Secure Signature Creation Device. Dispositivo seguro de creación de firma.**
Suscriptor	**Entidad que suscribe un certificado con un PSC en nombre de uno o más sujetos (personas físicas o jurídicas).**
Titular del certificado	**Persona, física o jurídica, ligada a los datos en un certificado digital, en particular, a una clave privada asociada a un certificado de clave pública. Cuando no es un PSC coincide con una entidad final. Puede ser un suscriptor actuando en su propio nombre.**