



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA
E INNOVACIÓN

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

SECRETARÍA DE ESTADO
DE TELECOMUNICACIONES
Y PARA LA SOCIEDAD DE
LA INFORMACIÓN



Red
IRIS

Nuevo Servicio de Certificado de Servidor

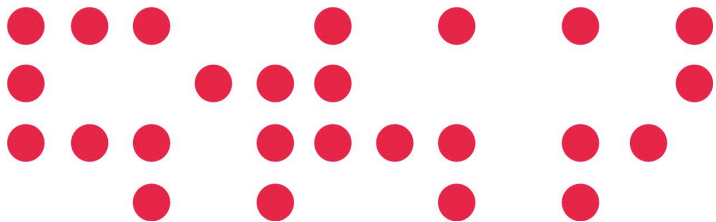
Daniel García

Málaga, 28 de Abril de 2009

Preguntas: <http://backnoise.com/?gt2009-scs>



1. Cambio de proveedor
2. Novedades en el servicio
3. Renovación de certificados
4. Nuevos perfiles de certificados
5. Certificados EV
6. Procedimiento de solicitud



Cambio de proveedor



Finales de Septiembre de 2008 TERENA lanza una convocatoria para renovar el servicio de certificados de servidor.

En Abril de 2009 se firma el acuerdo con
COMODO CA Limited of Manchester, England

<http://www.terena.org/activities/scs/>



Novedades del Servicio



Además de certificados de servidor

- Certificados S/MIME, de cliente
- Certificados para firmar código

Certificados validación extendida (EV)

Online Certificate Status Protocol



Renovación de certificados



¿... y los certificados actuales?

- Solicitar nuevos a COMODO
- Los de GlobalSign serán revocados en Febrero 2010
- Notificaremos a los responsables cuando esté disponible el procedimiento
 - Habrá suficiente tiempo aprox. 6 meses



Nuevos perfiles de certificados



Certificado de servidor TLS Server

Validez: 1, 2 y 3 años

DN:

- C required
- O required
- OU optional
- CN required

extendedKeyUsage: id-pk-serverAuth, id-pk-clientAuth

subjectAltName: hasta 100 dNSName (FQDN)

OCSP: http://ocsp.terena.org/ssl_server



Certificado para personas Personal

Validez: 1, 2 y 3 años

DN:

C required

O required

OU optional

CN required

unstructuredName optional

extendedKeyUsage: id-pk-emailProtection, id-pk-clientAuht

subjectAltName: hasta 10 rfc822Names (email)

OCSP: <http://ocsp.terena.org/personal>



Certificado para código Code Signing

Validez: 1, 2 y 3 años

DN:

C required
O required
OU optional
CN required

extendedKeyUsage: id-pk-codeSigning

OCSP: http://ocsp.terena.org/object_sign





Certificado para grid

eSience TLS Server

Pendiente de aprobación EUGridPMA

Validez: 13 meses

DN:

DC "org"
DC "terena"
DC "scs"
C required
O required
OU optional
CN required

extendedKeyUsage: id-pk-serverAuth, id-pk-clientAuth

subjectAltName: hasta 100 dNSName

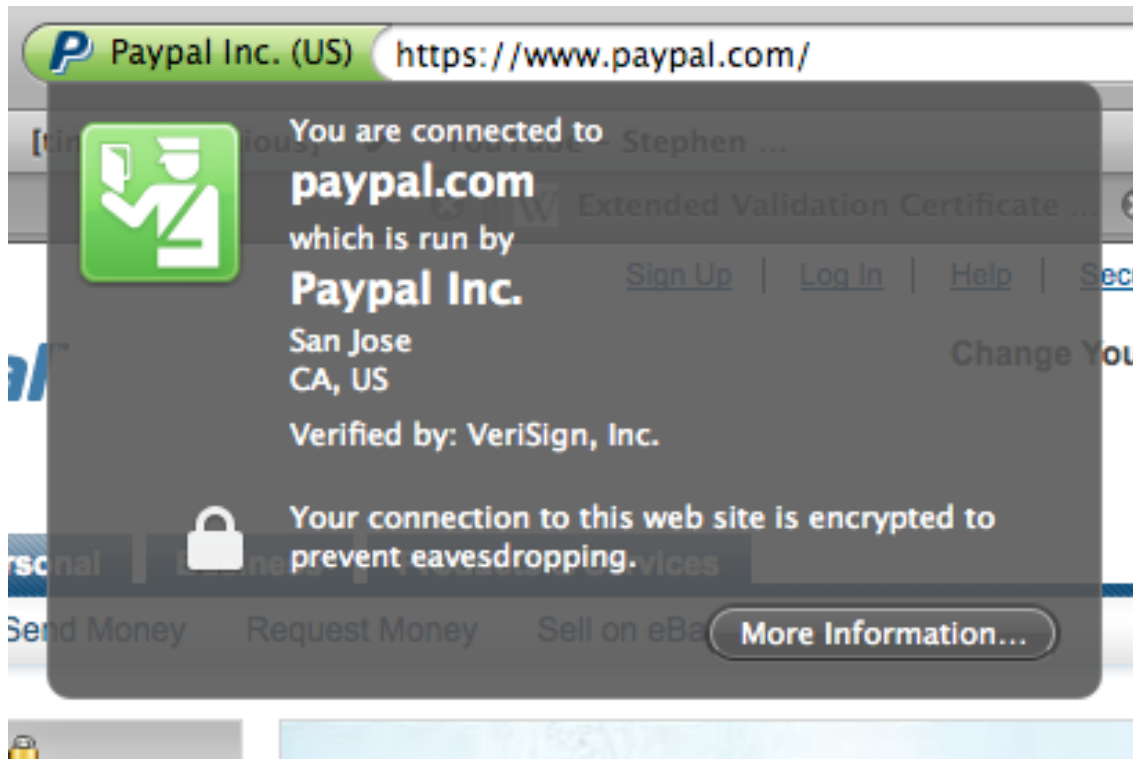
OCSP: http://ocsp.terena.org/eSience_server



Certificados EV



¿Qué es un certificado EV?



EV: Validación extendida



Preguntas: <http://backnoise.com/?gt2009-scs>

Características

- Transacciones económicas
- Proceso de solicitud diferente
- Coste asociado
- No somos RA
 - Actuamos como intermediarios



Proceso de solicitud



El procedimiento de solicitud

- Aún no disponible
- Muy similar al actual
- Incluso más sencillo
- Desterramos el FAX
- Para certificados personales nos apoyaremos en el SIR





XXVII Grupos de Trabajo de RedIRIS



ENCUESTA:

Para nosotros es muy importante tener vuestra opinión para poder adecuar nuestros servicios y eventos a vuestras necesidades. Os agradeceríamos mucho que cumplimentarais la encuesta online que hemos preparado.

¡MUCHAS GRACIAS por vuestra colaboración!

Acceso a la encuesta: <http://www.rediris.es/gt/gt2009/encu/>

Usuario gt2009

Password graciasMalaga

Preguntas: <http://backnoise.com/?gt2009-scs>

