



MINISTERIO  
DE INDUSTRIA, TURISMO  
Y COMERCIO

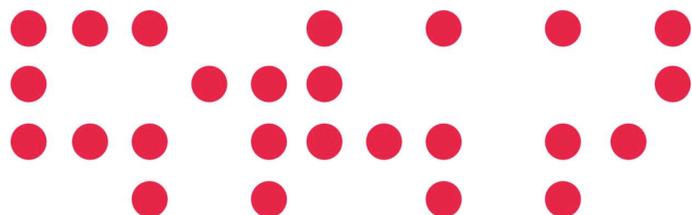
red.es

# SCS: servicio de certificados de servidor

Daniel García - Javi Masa  
19 noviembre 2007 - gt2007 -  
Mieres



- 1** Actualidad
- 2 Errores Comunes
- 3 Procedimiento SMIME
- 4 Piloto con UPCNet
- 5 Más Información





- **Números del servicio**
  - Identidades digitales certificada: 1268
  - Certificados emitidos: 1012
    - Válidos: 962
    - Expirados: 9
    - Revocados 53

- Más de 50

144 upc

137 uc3m

83 upv

63 csic

54 url

- 50 a 25

50 ulpgc

48 uam

43 uma

41 uvigo

36 upf

35 uclm

- 24 a 10

24 urjc, unizar, cesga

22 unileon, uib

21 unirioja, upm, upct

19 usc, udc, ucm,

18 uco

16 uah

15 um, icfo

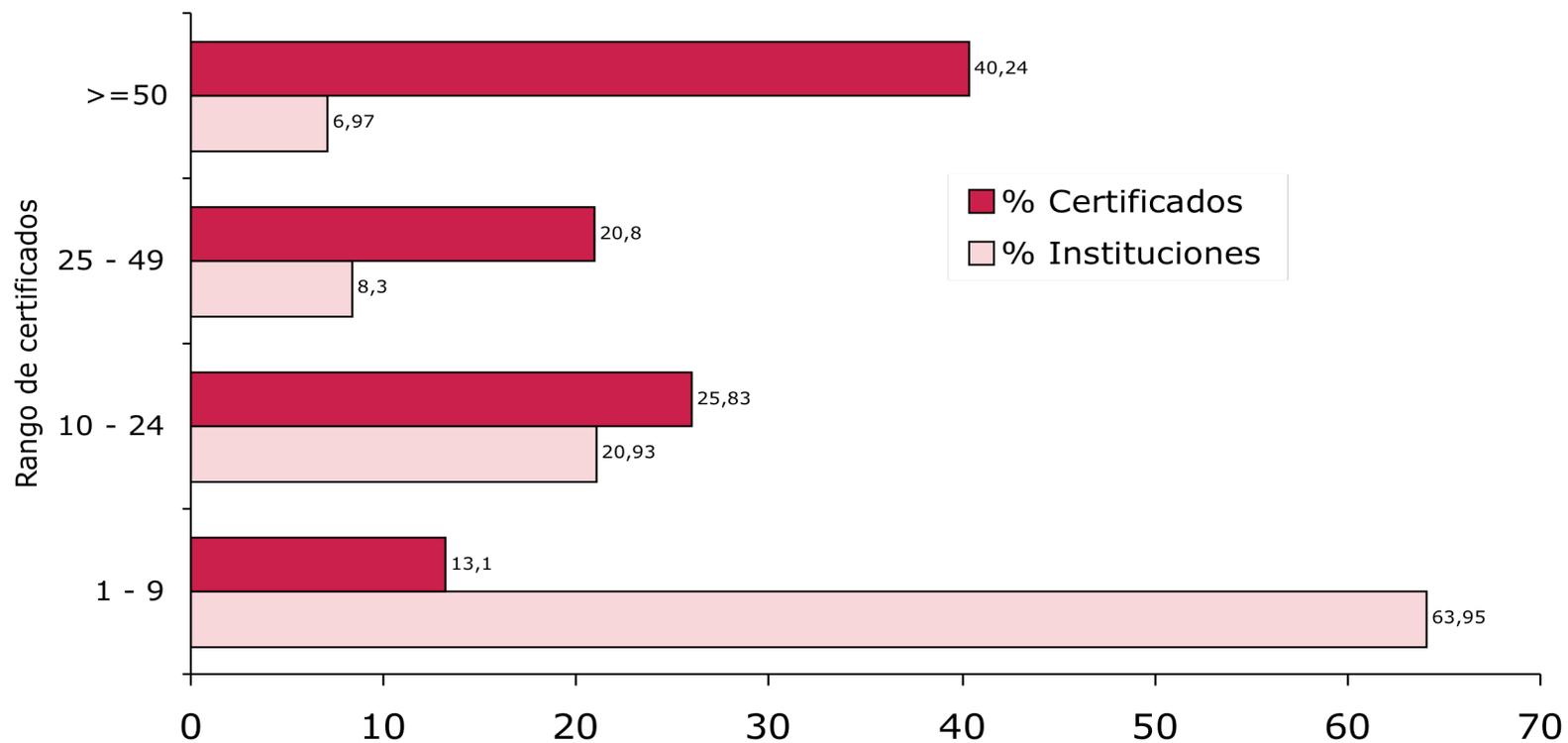
14 unavarra, bsc

11 ubu

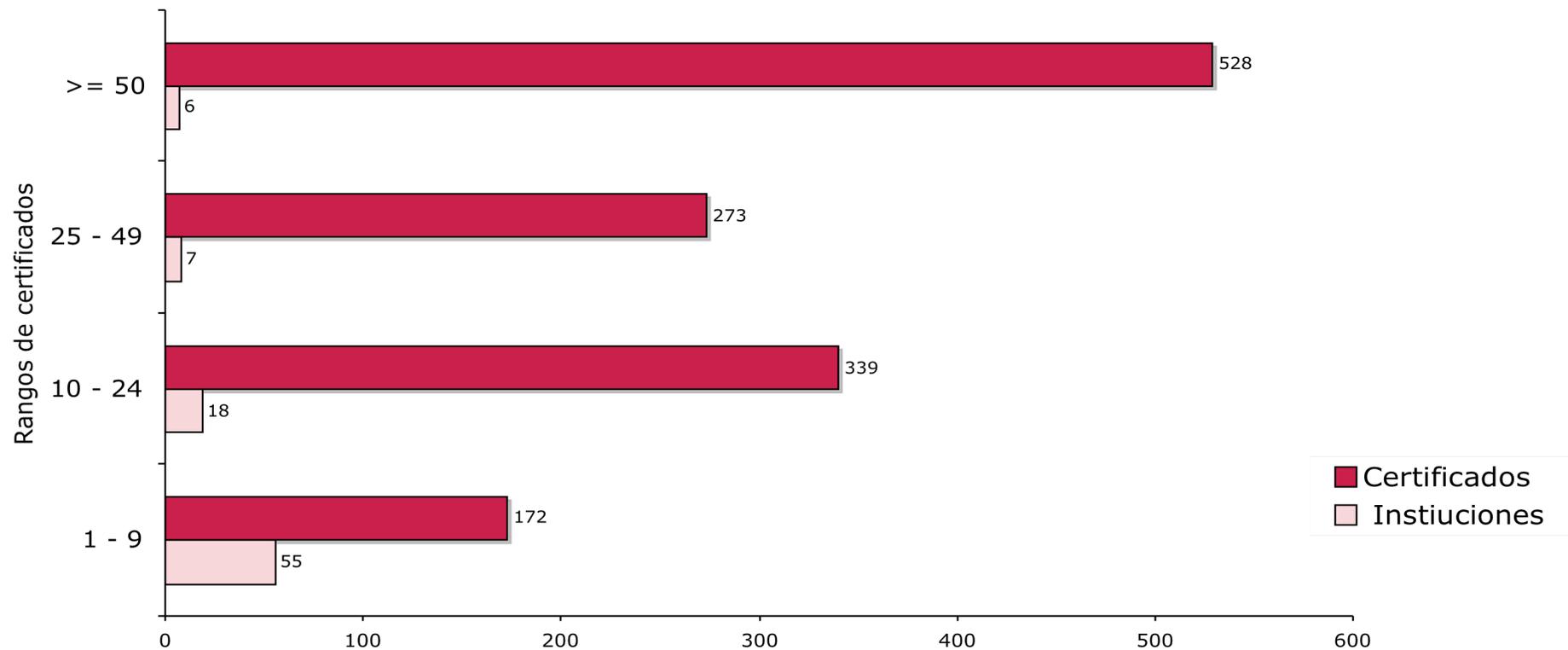
- Menos de 10

Más de 35 instituciones

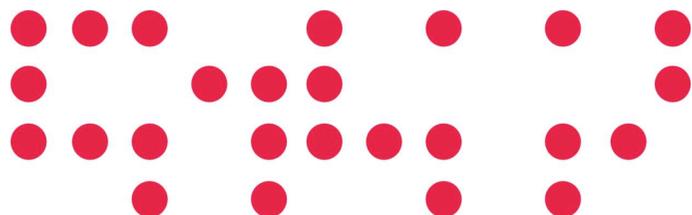
## Distribución de certificados por instituciones



## Distribución de certificados por instituciones

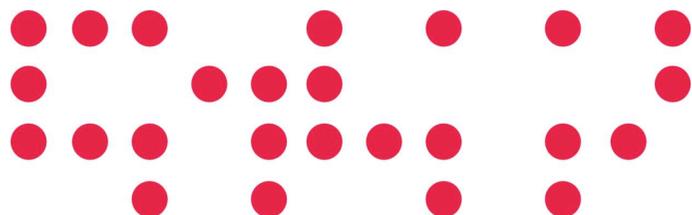


- 1 Actualidad
- 2 Errores Comunes**
- 3 Procedimiento SMIME
- 4 Piloto con UPCNet
- 5 Más Información



- Faltan las Firmas del PER o del solicitante
  - Ya sea en una o en todas las caras de las hojas
- No se han firmado todas las caras de todas las hojas
- Errores en los dominios
  - Prevalidarlos
  - No es el titular
- Falta documentación o mal cumplimentada
- Faltan caras de las hojas en los faxes recibidos
- Si se recibe el correo electrónico de [ra@globalsign.net](mailto:ra@globalsign.net)
  - Comprobar filtros anti-spam

- 1 Actualidad
- 2 Errores Comunes
- 3 Procedimiento SMIME**
- 4 Piloto con UPCNet
- 5 Más Información



- **Objetivo**

- Agilizar la comunicación entre:
  - Solicitantes
  - PERs
  - Operadores de SCS
- Permitir la delegación del PER en otras personas
  - Por medio del Documento de Delegación de Responsabilidad
- Eliminar el FAX del procedimiento
- **El procedimiento clásico no desaparece**
  - Quien quiera puede seguir usándolo

- Requisitos para las instituciones

- Cumplir con el Doc. de Condiciones de Uso versión SMIME [CUSO-smime]
- Complimentar el Doc. de Delegación de Responsabilidad [DResp]
  - No es obligatorio que el PER delegue
  - Basta con que aparezca en el Doc. de Delegación de Responsabilidad

- El solicitante genera la CSR y la pega en el interfaz Web
- Rellena el formulario Web con
  - Sus datos para el contacto técnico
  - Los datos del PER para los datos de la organización
- Envía los datos
- Realiza la captura de pantalla
- Confirma los datos en el interfaz de Web
- El solicitante recibe un correo de [ra@globalsign.net](mailto:ra@globalsign.net)
  - Cuidado con los artefactos anti-spam

- El solicitante rellena el Doc. de Condiciones de Uso [CUSO]
- Imprime toda la documentación
  - El Doc. de Condiciones de Uso
  - La captura de pantalla
  - El correo electrónico recibido de [ra@globalsign.net](mailto:ra@globalsign.net)
- **Firma en todas las caras de todas las páginas de todos los documentos**
- El solicitante hace llegar la documentación al PER



- El PER recibe toda la documentación
- **Realiza las verificaciones a las cuales se compromete en el [CUSO]**
- **Firma en todas las caras de todas las páginas de todos los documentos**
- El PER envía la documentación vía FAX a
  - A/A: Servicio SCS
  - N°: 955056627

- Documento de Condiciones de Uso versión SMIME [CUSO-smime]
  - Cambios mínimos respecto al clásico
    - La mayoría de formato

Aceptación del Solicitante			
En <i>ciudad</i>	a <i>0</i>	de <i>mes</i>	de 200
Firmado D/Dña: <i>Nombre Apellido Apellido</i>			
Con DNI/pasaporte: <i>00000000</i>		Y email: <i>direccionDeCorreo@subdomi.nio</i>	
Validación por el PROXY-PER SCS de la institución			
El PROXY-PER SCS de la institución ha comprobado que el Solicitante es el responsable técnico del servidor o servidores detallados al final del documento para el/los que se ha/n solicitado el/los certificado/s.			
En <i>ciudad</i>	a <i>0</i>	de <i>mes</i>	de 2007
FIRMADO S/MIME			
Firmado D/Dña: <i>Nombre Apellido Apellido</i>			
Con DNI/pasaporte: <i>00000000</i>		Y email: <i>direccionDeCorreo@subdomi.nio</i>	

- Documento de Delegación de Responsabilidad [DResp]
  - El PER al firmarlo autoriza a otras personas a **validar** las solicitudes en su nombre
  - La delegación **sólo** es en el **ámbito** de **SCS**
  - El conjunto de personas sobre el que se delega es **finito**
    - 4 personas de momento
  - Las personas sobre las que se delega son PROXY-SCS
  - **Necesitan certificados digitales**

Reconocidos de acuerdo con lo que establece el artículo 11.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, 18, y 20 de dicha Ley

- Documento de Delegación de Responsabilidad [DResp]

Proxy1	Nombre <b>José</b>	Apellidos <b>Pérez Pérez</b>
	DNI <b>00000000X</b>	Email <b>jose.perez@insti.tucion.es</b>
	Subject DN <b>C=ES, O=FNMT, OU=FNMT Clase 2 CA, OU=500051361, CN=NOMBRE PEREZ PEREZ JOSE - NIF 00000000X</b>	
	Autoridad de Certificación <b>Issuer: C=ES, O=FNMT, OU=FNMT Clase 2 CA</b> <b>X509v3 Authority Key Identifier:</b> <b>keyid:40:9A:76:44:97:74:07:C4:AC:14:CB:1E:8D:4F:3A:45:7C:30:D7:61</b>	

- Dos modos
  - El solicitante es el PROXY-SCS
    - Una sola persona realiza todo el proceso
  - El solicitante y el PROXY-SCS son personas distintas
    - Una persona realiza la solicitud y el PROXY-SCS la valida

- El solicitante genera la CSR y la pega en el interfaz Web
- Rellena el formulario Web
- **Si el solicitante es también el PROXY-SCS**
  - Sus datos para el contacto técnico
  - Sus datos para la información de la organización
  - **Si el solicitante NO es el PROXY-SCS**
    - Sus datos para el contacto técnico
    - Los datos del PROXY-SCS para la información de la organización
- Envía los datos
- Realiza la captura de pantalla
- Confirma los datos en el interfaz de Web
- El solicitante recibe un correo de ra@globalsign.net

## • Si el solicitante es también el PROXY-SCS

- El solicitante rellena el Doc. de Condiciones de Uso [CUSO-smime]
  - [http://www.rediris.es/pki/scs/doc/scs\\_condiciones\\_uso\\_smime.pdf](http://www.rediris.es/pki/scs/doc/scs_condiciones_uso_smime.pdf)
- El solicitante redacta un correo electrónico donde el asunto debe comenzar por
  - **[SCS\_SMIME][AAAAMMDD.vv]**
  - En el asunto debe aparecer el nombre de la institución o sus siglas
  - Ejemplo: **[SCS\_SMIME][20071114.01] UPC 181.02**
- En el **cuerpo del correo** electrónico deben figurar
  - Lista con los CNs de los certificados solicitados
- El correo debe llevar adjunto (en formato PDF)
  - El Doc. de Condiciones de Uso [CUSO-smime]
  - La captura de pantalla
  - El correo electrónico recibido de [ra@globalsign.net](mailto:ra@globalsign.net)

- **Si el solicitante NO es el PROXY-SCS**

- El solicitante rellena el Doc. de Condiciones de Uso [CUSO-smime]
  - [http://www.rediris.es/pki/scs/doc/scs\\_condiciones\\_uso\\_smime.pdf](http://www.rediris.es/pki/scs/doc/scs_condiciones_uso_smime.pdf)
- Imprime la documentación
  - El Doc. de Condiciones de Uso
  - La captura de pantalla
  - El correo electrónico recibido de [ra@globalsign.net](mailto:ra@globalsign.net)
- **Firma a mano todas las caras de todas las páginas de todos lo documentos**
- El solicitante hace llegar toda la documentación al PER

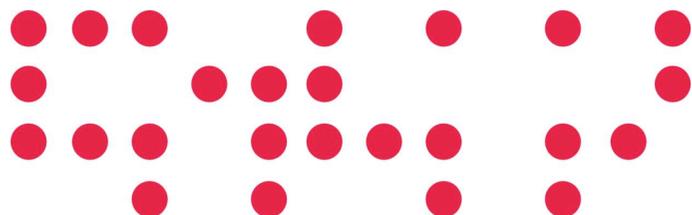
- **Si el solicitante NO es el PROXY-SCS (continuación)**
  - El PROXY-SCS completa el Doc. de Condiciones de Uso [CUSO-smime]
    - No es necesario que lo firme a mano
  - El PROXY-SCS (**nunca el solicitante**) redacta un correo electrónico donde el asunto debe comenzar por
    - **[SCS\_SMIME][AAAAMMDD.vv]**
    - Contener el nombre de la institución o sus siglas
    - Ejemplo: **[SCS\_SMIME][20071114.01] UPC 181.02**
  - En el cuerpo del correo electrónico debe figurar
    - Una lista con los CNs de los certificados solicitados
  - El correo debe llevar adjunto (en formato PDF)
    - El Doc. de Condiciones de Uso [CUSO-smime]
    - La captura de pantalla
    - El correo electrónico recibido de [ra@globalsign.net](mailto:ra@globalsign.net)
    - Todos **firmados a mano** por el **solicitante**



- El correo electrónico debe firmarse digitalmente con SMIME
- Sólo se aceptaran correos electrónicos que
  - Contengan en el **pkcs7** el certificado del firmante
  - Firmados con certificados listados en el Doc. de Delegación de Responsabilidad

- **Cómo enviar los correos para más de una solicitud**
  - Un correo electrónico con el asunto [SCS-SMIME][AAAAMMDD.vv][CUSO]
    - En el cuerpo debe aparecer una lista con **todos** los CNs de las solicitudes
    - Debe llevar adjunto el Doc. de Condiciones de Uso [CUSO-smime]
  - Un correo electrónico **por cada solicitud** con el asunto
    - [SCS-SMIME][AAAMMDD.vv][CN]
    - Ejemplo: [SCS-SMIME][20071114.01][epsc.upc.edu]
    - Debe llevar adjunto
      - La captura de pantalla
      - El correo electrónico enviado por ra@globalsign.net
  - Todos los correos electrónicos deben firmarse digitalmente con SMIME
  - Sólo se aceptaran correos electrónicos que
    - Contengan en el **pkcs7** el certificado del firmante
    - Firmados con certificados listados en el Doc. de Delegación de Responsabilidad

- 1 Actualidad
- 2 Errores Comunes
- 3 Procedimiento SMIME
- 4 Piloto con UPCNet**
- 5 Más Información





- Le toca a Elena Galván

- 1 Actualidad
- 2 Errores Comunes
- 3 Procedimiento SMIME
- 4 Piloto con UPCNet
- 5 Más Información**



- **Página del servicio**
  - <http://www.rediris.es/pki/scs>
- **Documentos para SMIME**
  - [http://www.rediris.es/pki/scs/doc/scs\\_condiciones\\_uso\\_smime-1.0.pdf](http://www.rediris.es/pki/scs/doc/scs_condiciones_uso_smime-1.0.pdf)
  - [http://www.rediris.es/pki/scs/doc/scs\\_delegacion\\_resp\\_smime-1.0.pdf](http://www.rediris.es/pki/scs/doc/scs_delegacion_resp_smime-1.0.pdf)
- **El procedimiento aún no está en la Web**
  - [http://www.rediris.es/pki/scs/doc/scs\\_procedimiento\\_smime-1.0.pdf](http://www.rediris.es/pki/scs/doc/scs_procedimiento_smime-1.0.pdf)
- **Crearemos una guía básica como la actual**
  - <http://www.rediris.es/pki/scs/doc/userguide.es.html>