SCS

Servicio de certificados de RedIRIS

Javi Masa - javier.masa@rediris.es

Antonio Pérez - antonio.perez@rediris.es

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
MINISTERIO DE CIENCIA E INNOVACIÓN
Red IRIS

Valladolid, 29/11/2011

Índice

Bienvenida
Acceso a la reunión

- Vídeo
  - Mediante Adobe Connect
    - http://tinyurl.com/czmb3bj
- Material adicional
  - Presentación disponible en
    - http://www.rediris.es/scs/coord/jt2011/

Índice

Escenario actual

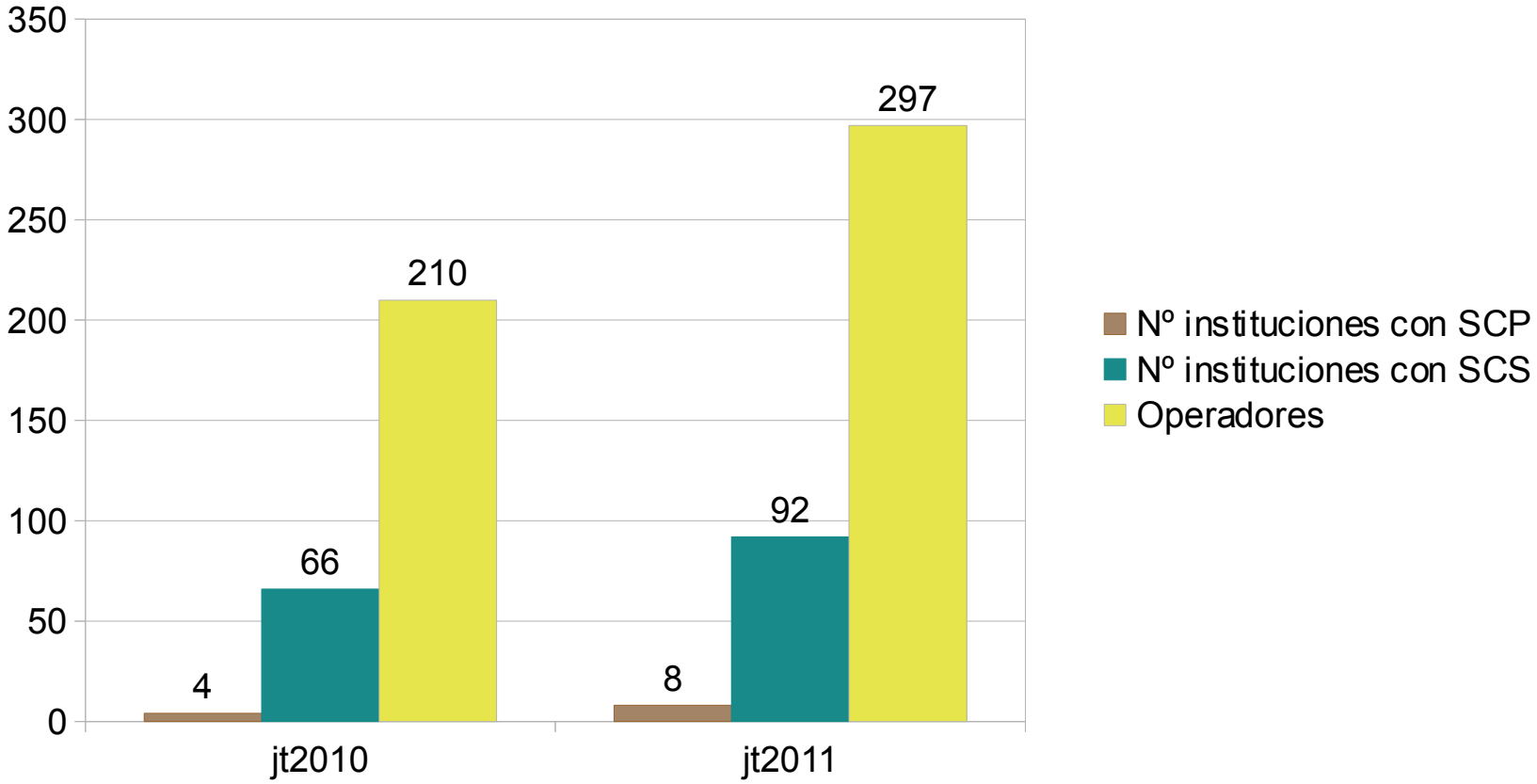
- Aumento de instituciones en el servicio
  - Aumento de solicitantes registrados
  - Aumento de certificados emitidos
- Aumento de perfiles disponibles
  - Certificado SSL de servidor
  - Certificado personal (SCP)
  - Certificados de código (manualmente)
- Disminución del staff
  - Diego dejó RedIRIS en Octubre
- Aumento de carga de trabajo
  - Para los que quedamos

Índice

Estadísticas

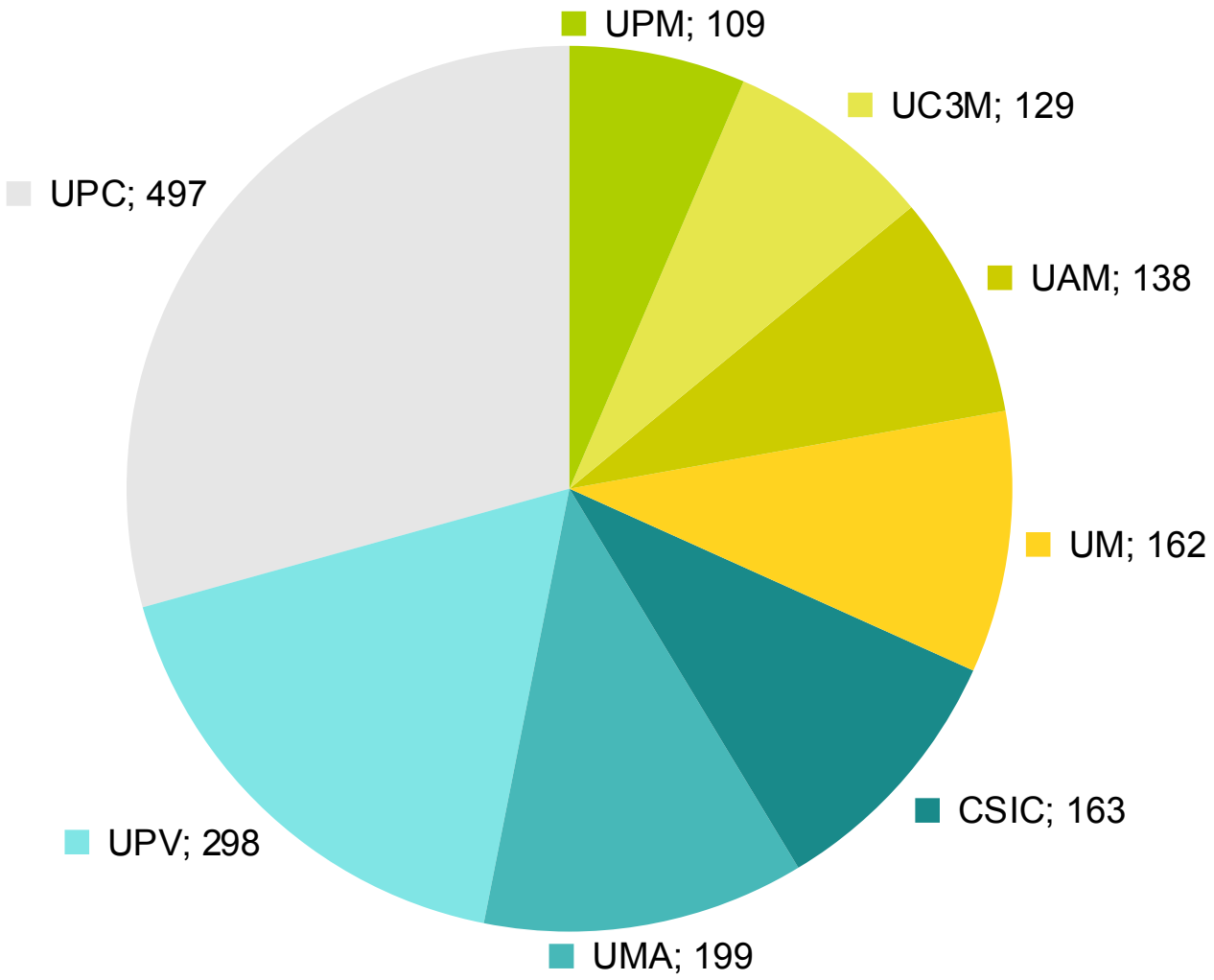
- SSL servidor
  - Instituciones: 92
  - Solicitantes registrados: 297
  - Certificados emitidos: 3703
  - Dominios: 285
- SCP
  - Instituciones: 9
    (BSC, CICA, IVIE, RedIRIS, UC3M, UDC, UPV, URL)
  - Certificados emitidos: 123
- Firma de código
  - Instituciones: 4
    (RedIRIS, UC3M, UPV, UV)
  - Certificados emitidos: 7

Estadísticas
Instituciones y personas participantes



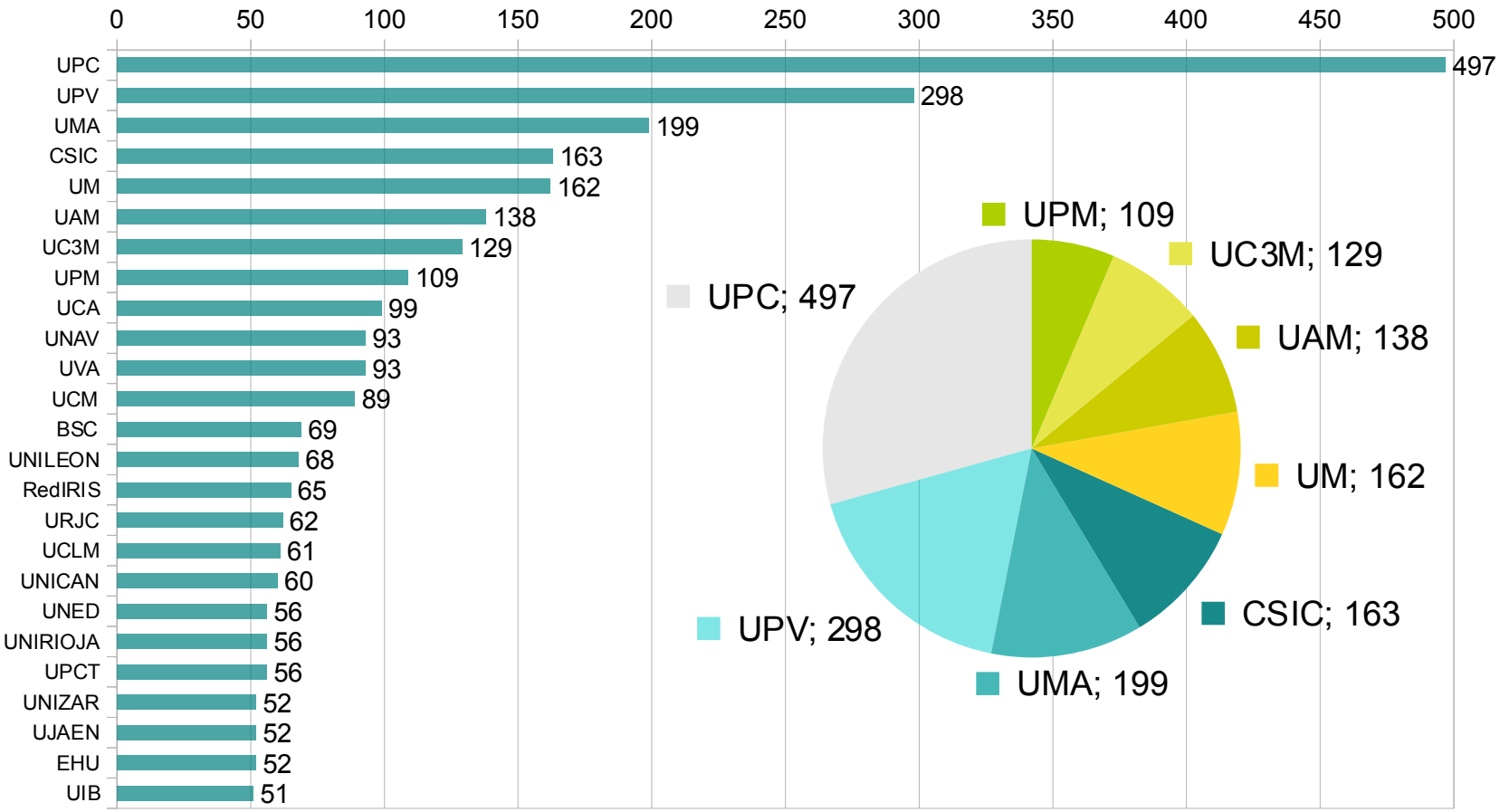
Estadísticas: SCS

Instituciones con más de 100 certificados emitidos



Estadísticas: SCS

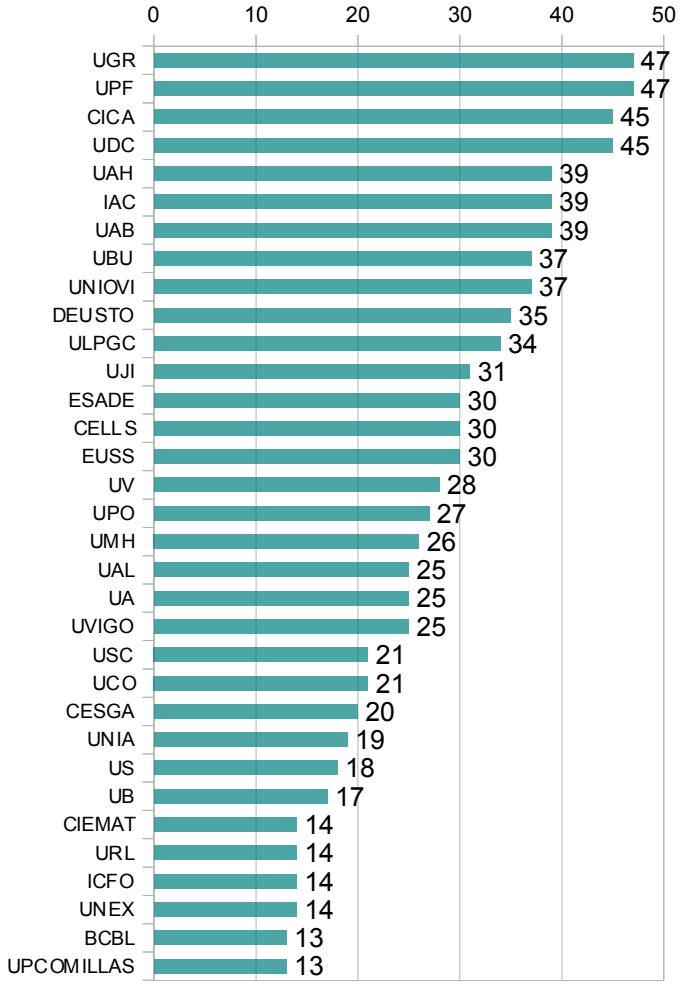
Instituciones con más de 50 certificados emitidos

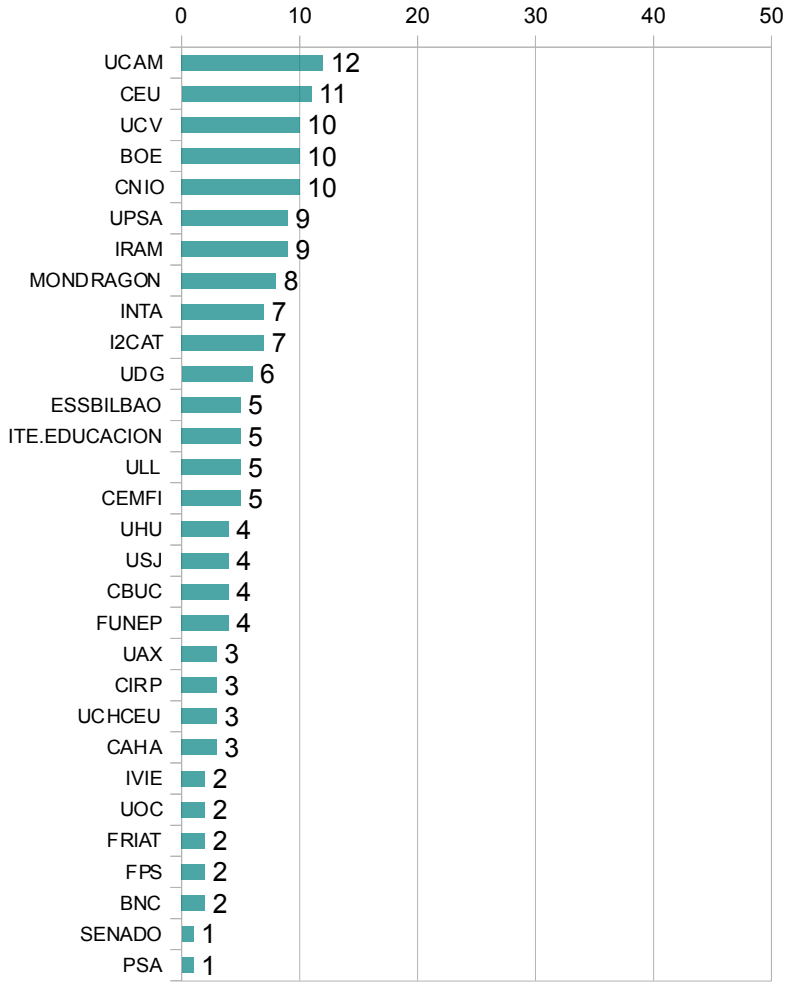


- El resto de instituciones (66) suman 1103 certificados

Estadísticas: SCS

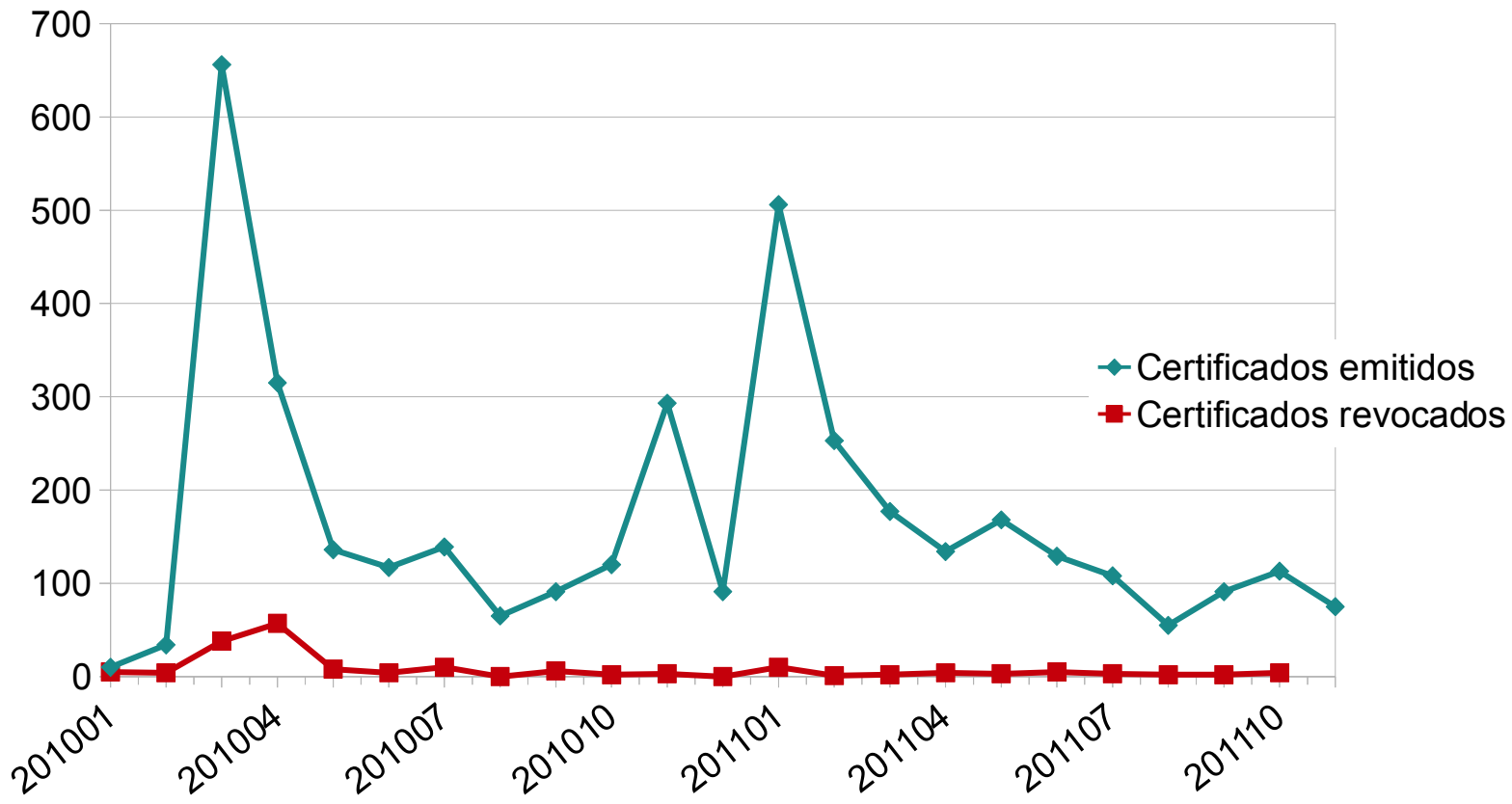
Instituciones con menos de 50 certificados emitidos





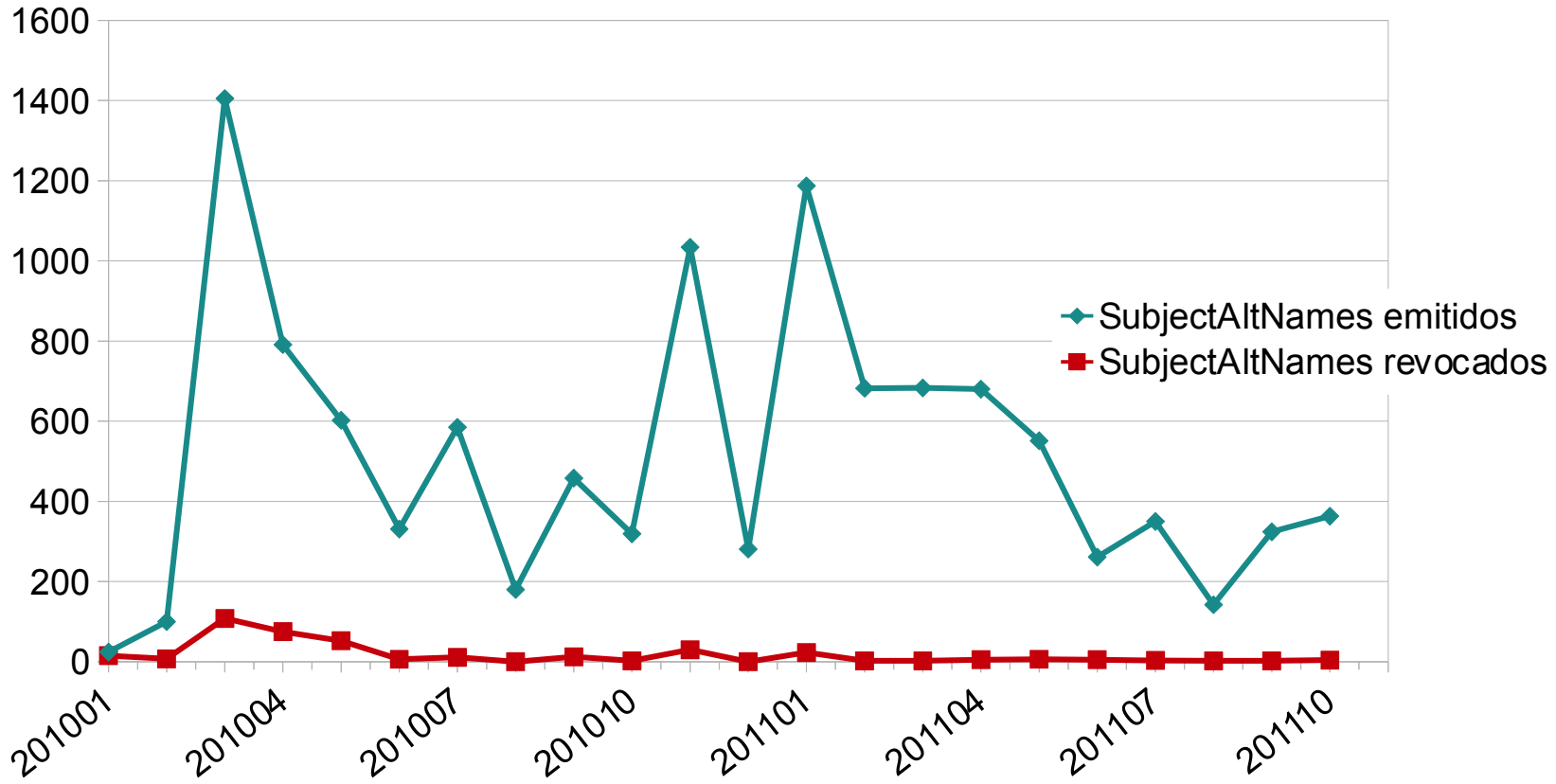
Estadísticas: SSL servidor

Certificados emitidos y revocados (por mes)



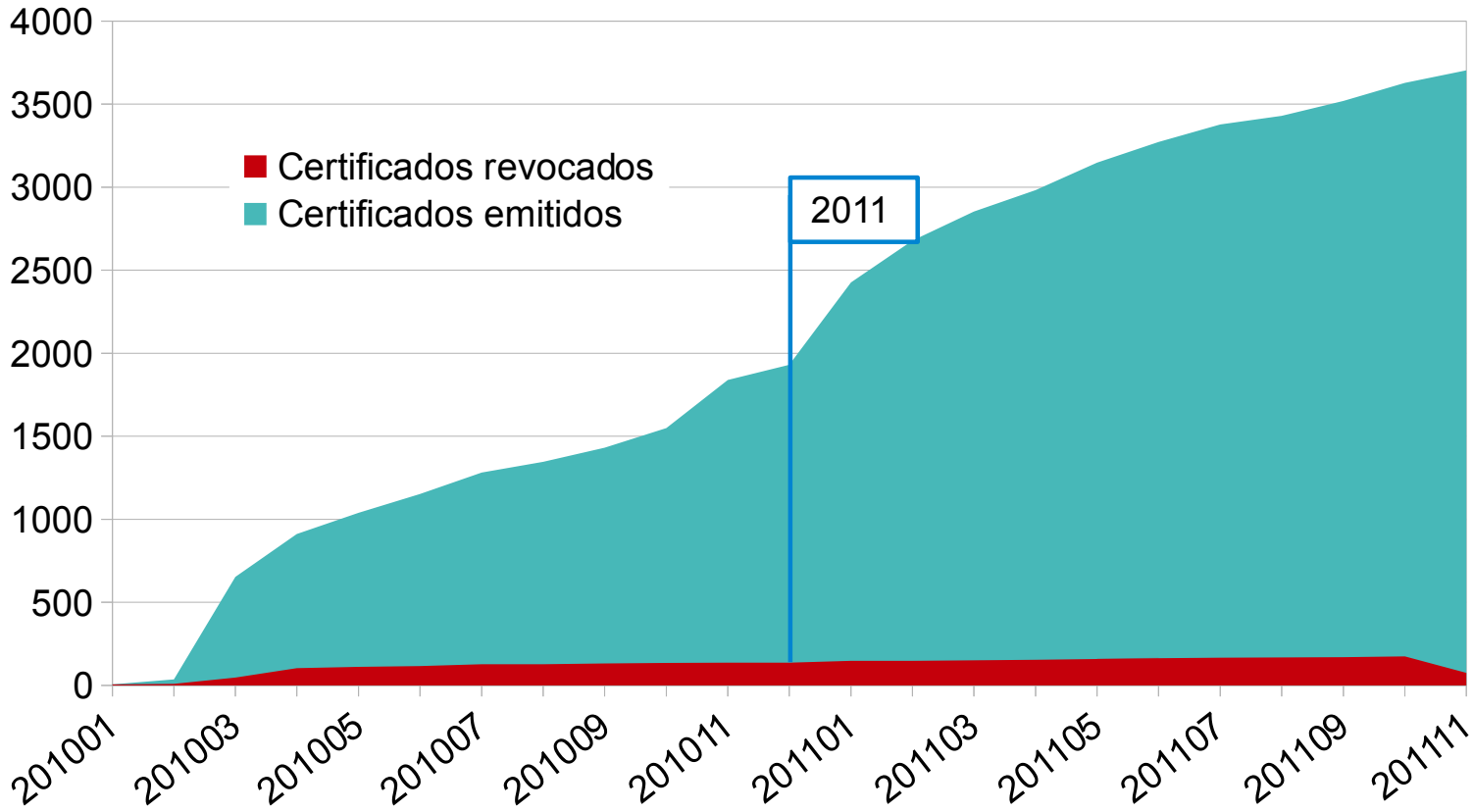
Estadísticas: SSL servidor

SubjectAltNames emitidos y revocados (al mes)



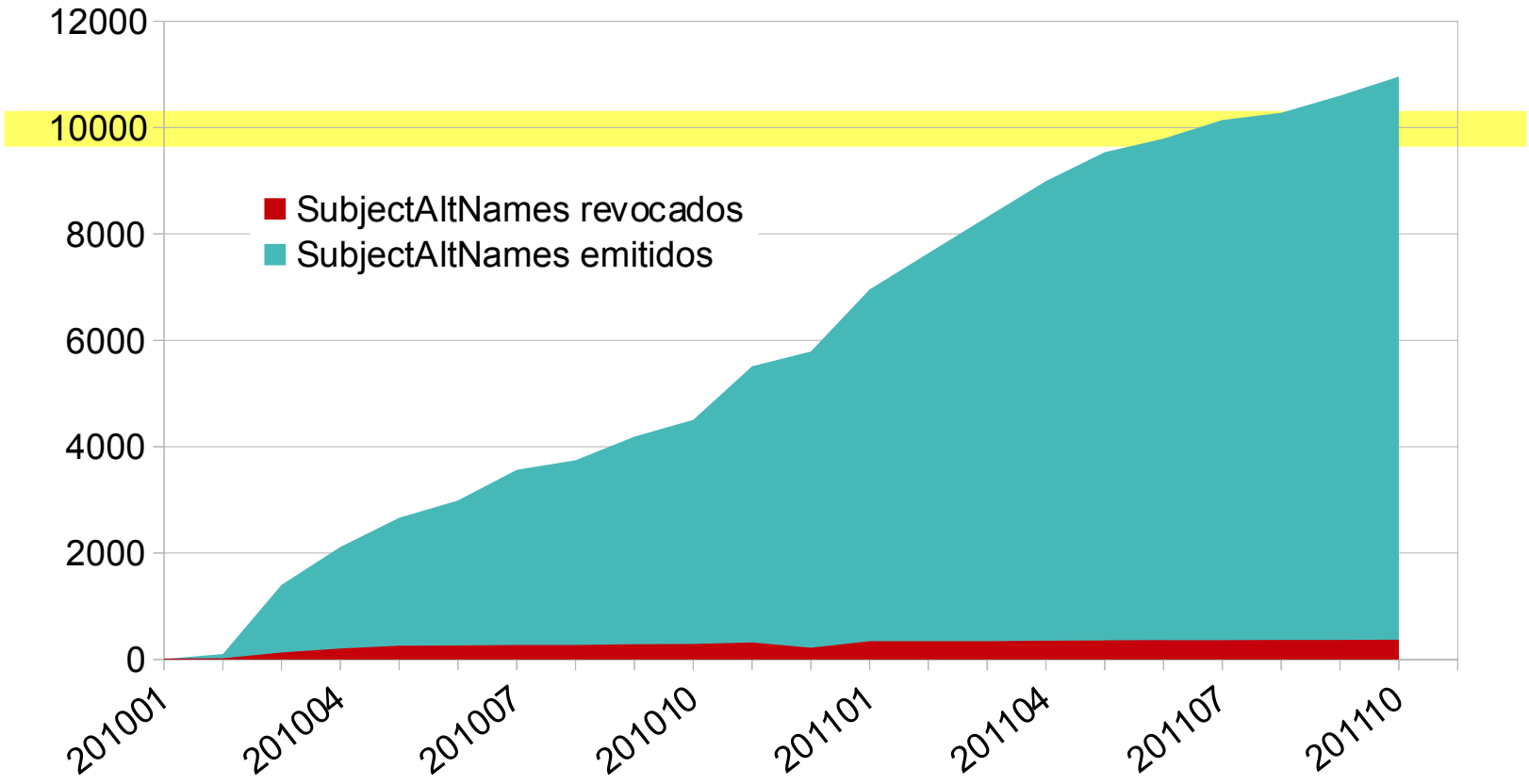
Estadísticas: SSL servidor

Certificados emitidos y revocados (acumulado)

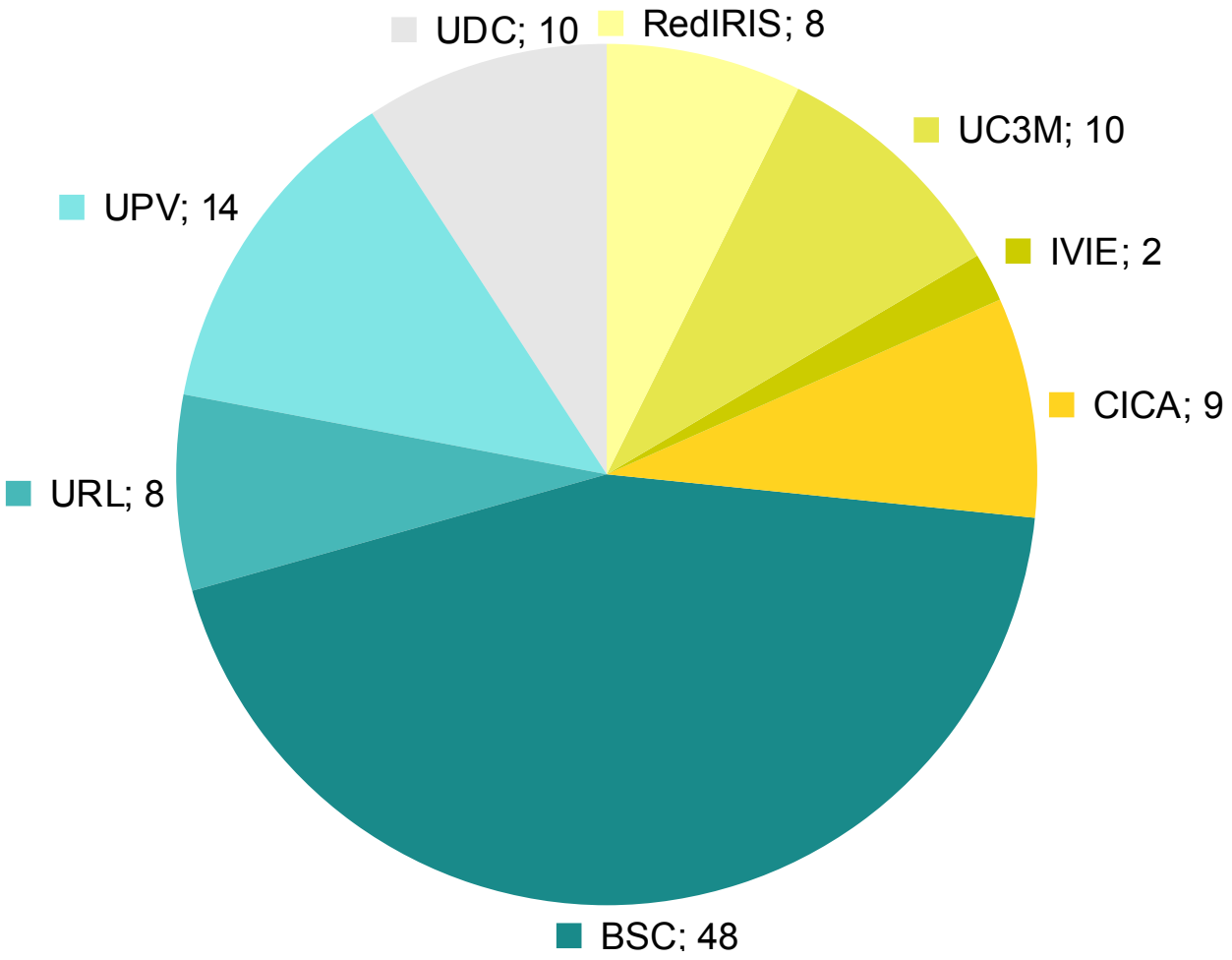


Estadísticas: SSL servidor

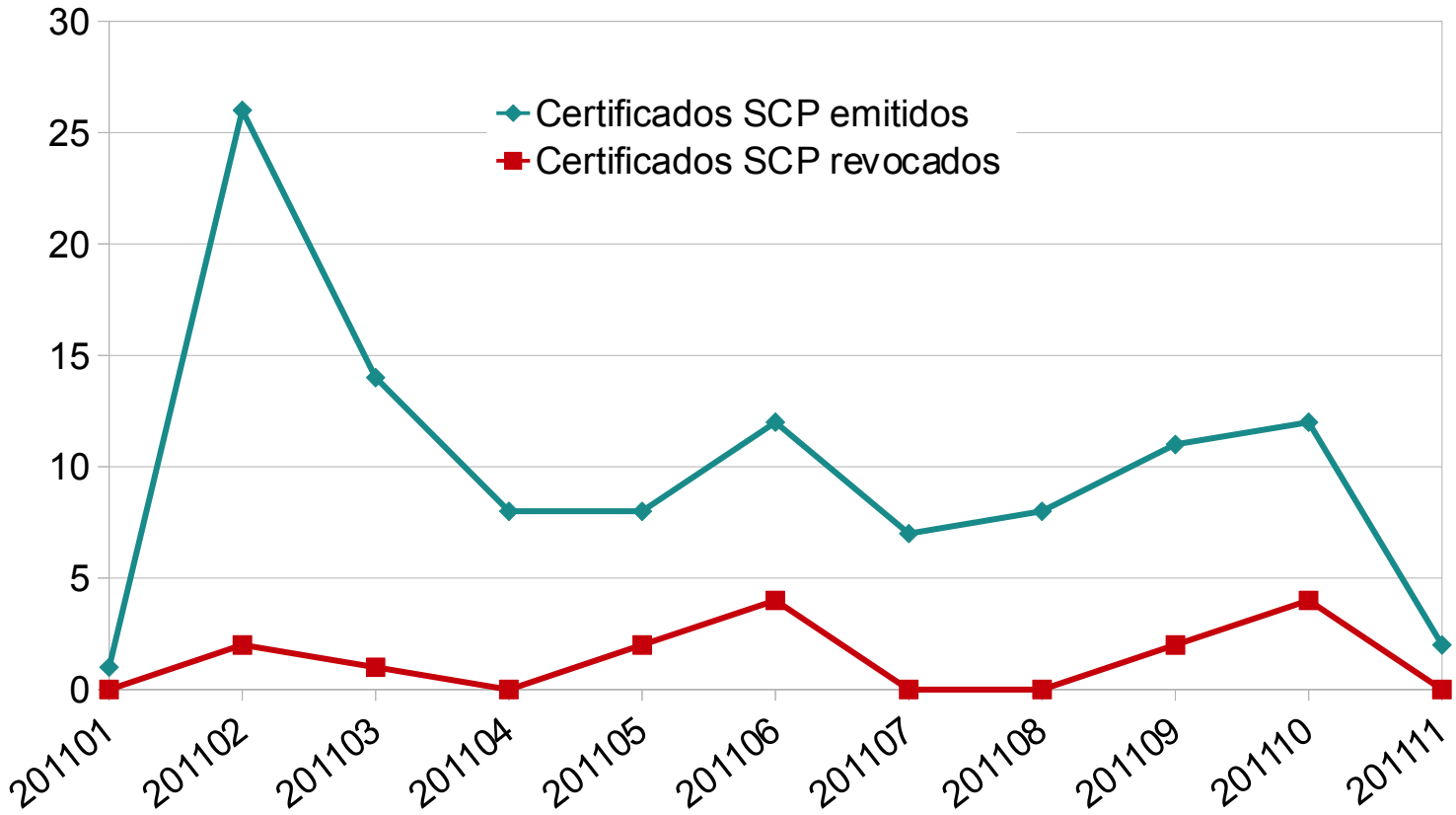
SubjectAltNames emitidos y revocados (acumulado)



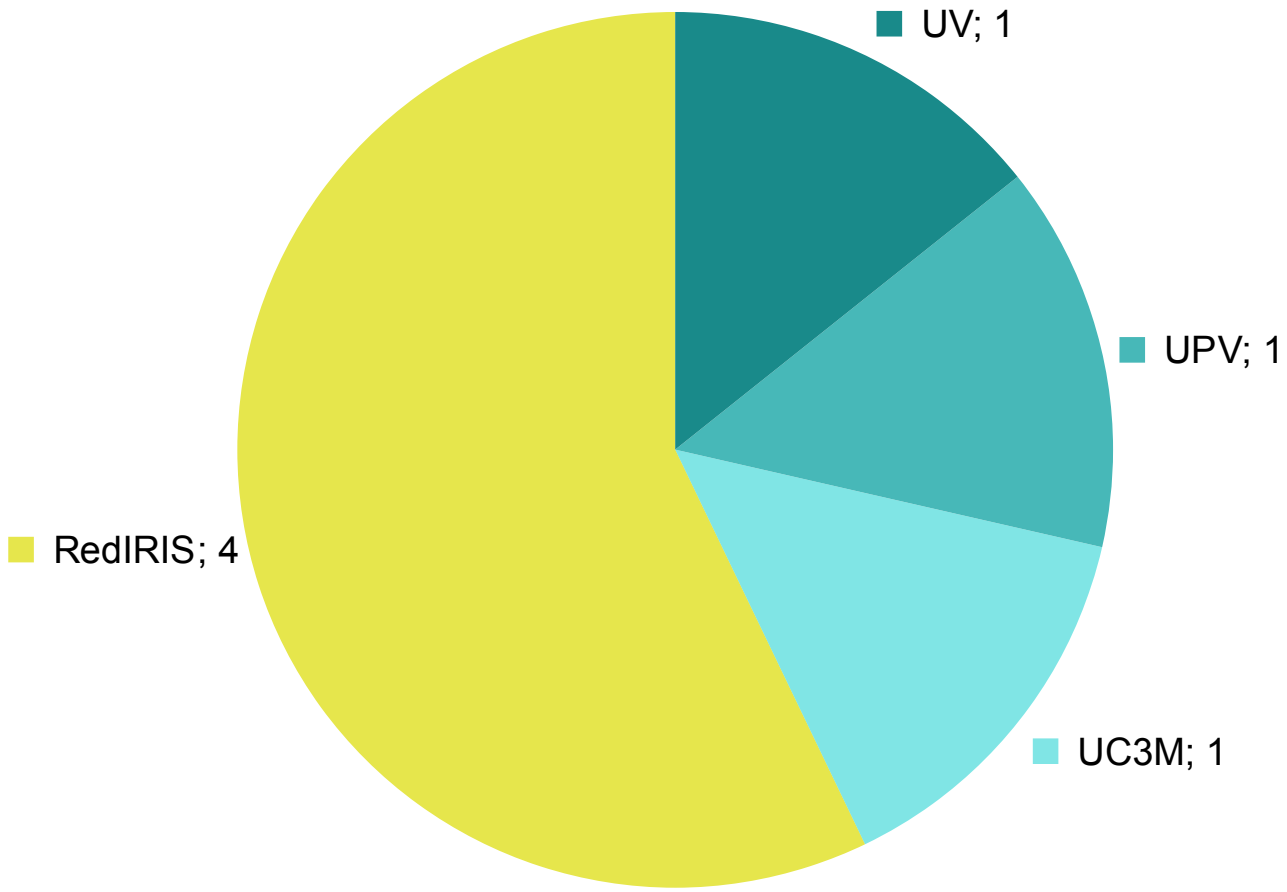
Estadísticas: SCP
Certificados emitidos



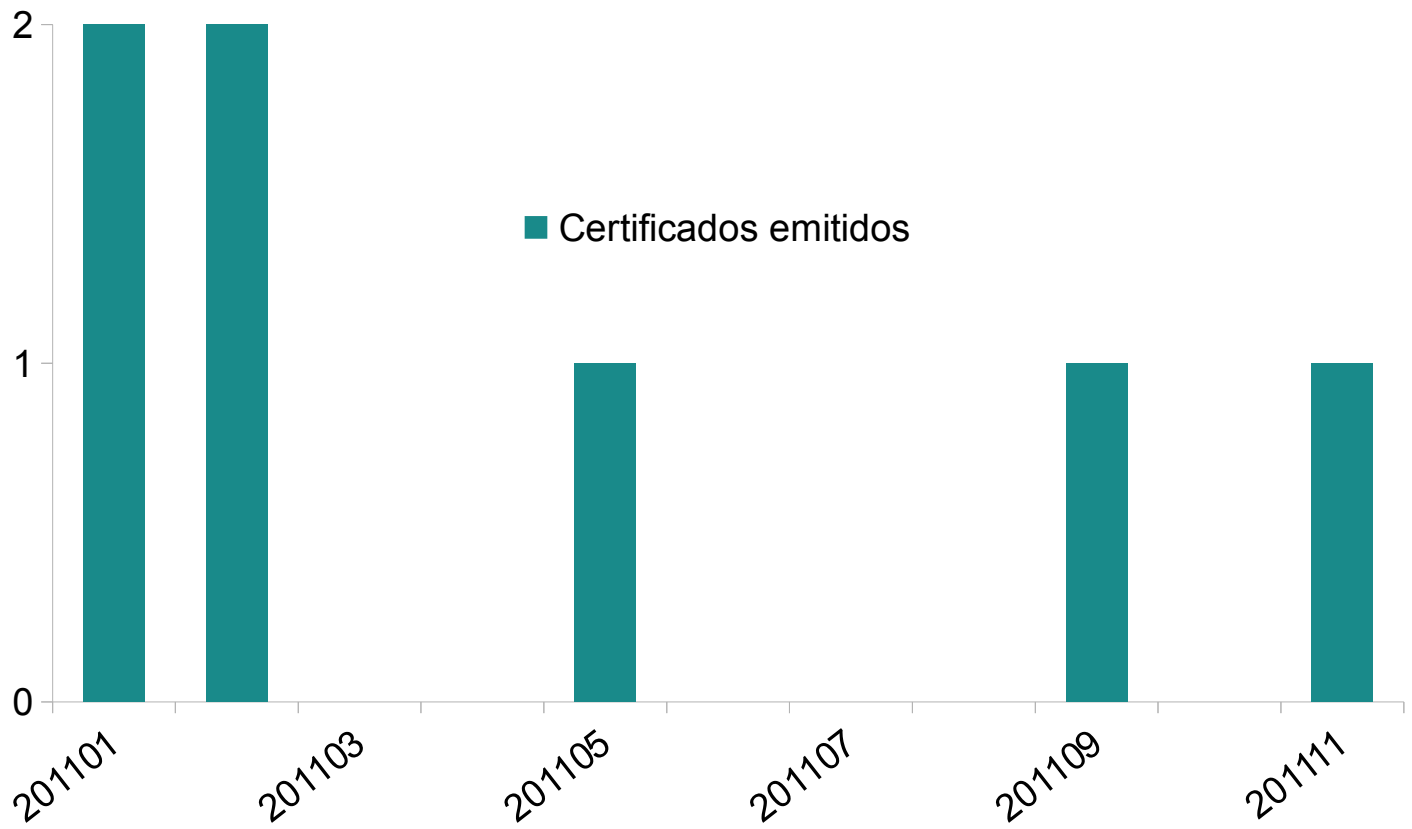
Estadísticas: SCP
Certificados emitidos y revocados (al mes)



Estadísticas: Firma de Código
Certificados emitidos



Estadísticas: Firma de Código
Certificados emitidos (al mes)



Índice

SCS: perfil Personal

- ¿Cómo se da de alta la institución en el servicio SCP?
  - Un operador de SCS debe enviar un mail a scs-ra@rediris.es
    - Identificador del conector SIR
    - Dirección de correo corporativa de la institución dedicada a dar soporte a sus usuarios
    - URL explicativa del servicio para los usuarios finales de la institución.
  - RedIRIS comprueba que esas direcciones funcionan
    - Se activa SCP para la institución

SCS: perfil Personal

- ¿Qué usuarios pueden solicitar certificados?
  - Uso del atributo **ePA** (*eduPersonAffiliation*) en la aserción
  - Este atributo es utilizado para realizar el control de acceso a la solicitud de certificados personales. Los valores aceptados para este atributo son:
    - student: Estudiantes
    - faculty: PDI
    - staff: PAS
    - employee: staff & faculty
    - member: staff, faculty & student
- Guía del servicio
  - http://www.rediris.es/scs/perfiles/personal/guia.html

SCS: perfil Personal

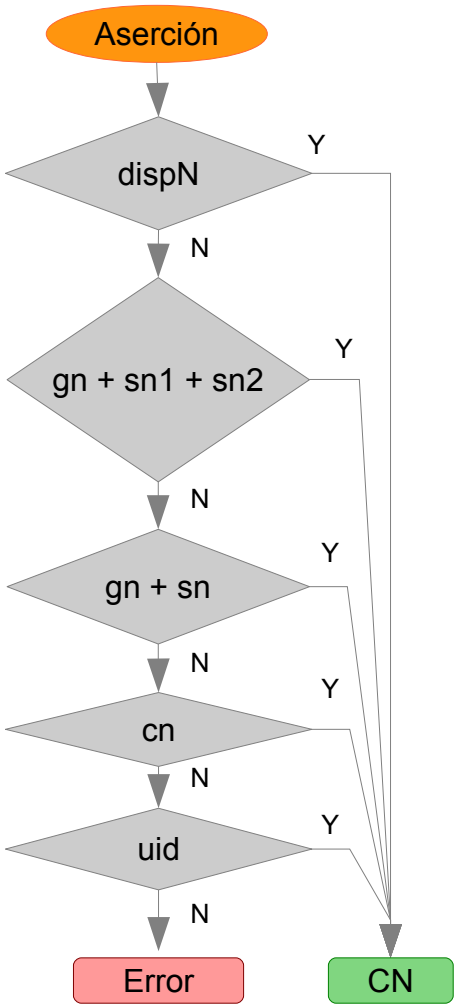
- Formato de un DN
  - **C**=ES, **O**=Inst, **CN**=Name, **unstructuredName**=ID_OpenID

CN	Depende de los atributos que envíe el IdP de la institución a la que pertenece el usuario
unstructuredName	Identificador traceable, único y persistente del propietario del certificado en el ámbito del IdP de la institución a la que pertenece. http://www.rediris.es/sir/howto-openid.html

http://yo.rediris.es/soy/**uid@sHO**/
http://eu.rediris.es/son/**uid@sHO**/
http://jo.rediris.es/soc/**uid@sHO**/
http://ni.rediris.es/**uid@sHO**/naiz/

SCS: perfil Personal

- Composición del CN
  - Se genera a partir de los atributos codificados según SIR
    - dispN, gn, sn1, sn2, sn, cn, uid
      http://www.rediris.es/sir/docs/attr_map.html
  - Usando el proceso de composición
    www.rediris.es/scs/perfiles/personal/guia.html#subjectdn
    1. dispN
    2. gn + sn1 + sn2
    3. gn + sn
    4. cn
    5. uid
- Composición del unstructuredName
  - <prefijo>/**uid@sHO**/<sufijo>



SCS: perfil Personal - Ejemplos

- **cn**=Javier Fariñas Alvariño, **uid**=javier.farinas
  - C=ES, O=upv.es, CN=**Javier Fariñas Alvariño**, unstructuredName=http://yo.rediris.es/soy/javier.farinas@udc.es/
- **cn**=Miguel MacÃ-as EnguÃ-danos, **uid**=mimaen
  - C=ES, O=upv.es, CN=**Miguel MacÃ-as EnguÃ-danos**, unstructuredName=http://yo.rediris.es/soy/mimaen@upv.es/
- **cn**=Observatorio Sie, **uid**=obsersie
  - C=ES, O=ivie.es, CN=**Observatorio Sie**, unstructuredName=http://yo.rediris.es/soy/obsersie@upv.es/
- **cn**= Unidad De Formación Pas Rrhh
  - C=ES, O=upv.es, CN=**Unidad De Formación Pas Rrhh**, unstructuredName=http://yo.rediris.es/soy/rrhh06@upv.es/

SCS: perfil Firma de código

- Por ahora “disponible de forma manual”
  - No integrado en el ISC
- ¿Cómo es el proceso para la obtención?
  - RedIRIS accede a un interface de solicitud que nos da COMODO
  - Introducimos los datos que nos debéis proporcionar
  - Nuestro navegador genera la clave clave privada y envía la CSR
  - COMODO nos envía el certificado
  - Lo instalamos en nuestro navegador y lo exportamos a PKCS #12
  - Os enviamos el PKCS #12 por mail
  - Eliminamos ese certificado de nuestro navegador
    - Hay que “confiar” en RedIRIS

SCS: perfil Firma de código

- ¿Cómo solicitarlo?
  - Datos del certificado
    - Duración del certificado: 1 a 5 años
    - eMail de contacto que aparecerá en el certificado (opcional)
  - Datos de la institución
    - Nombre oficial de la institución
    - Departamento (opcional)
    - Dirección postal
    - Código postal, Ciudad y Provincia
  - Datos del contacto
    - Nombre, Apellidos
    - eMail
    - Teléfono

Índice

Incidencias - ISC de RedIRIS

- Acceso por SIR
  - Cambios en direcciones de correo
  - Compromiso de la clave del usuario en la institución
    - Permite solicitar un certificado desde otra máquina y descargarlo
      - ¿Avisar por mail/SMS cuando se emite un certificado?
- SCS
  - Avisos del alta de usuarios en el ISC a RedIRIS
    - Se automatizará el aviso para agilizar la validación de usuarios
  - Fecha 1970-01-01 en los estados de los certificados
    - Se ha enviado la solicitud validada a COMODO pero todavía no ha sido firmada. Tenemos que arreglar el mensaje mostrado

Incidencias - ISC de RedIRIS

- SCS (continuación)
  - Sede electrónica
    - COMODO no es un prestador reconocido según las leyes 59/2003 y 11/2007 y, por tanto, sus certificados no tienen reconocimiento jurídico.
      - https://www11.mityc.es/prestadores/busquedaPrestadores.jsp
    - Pero COMODO es reconocido por los navegadores
    - Solicitados para: UM (José Fco. Hidalgo), UPV, USAL, URJC
  - Certificados wildcard
    - Actualmente no soportado
    - Futuro: ¿uso para dominios que sigan la regla de los tres puntos?
      - Tipo *.subdomain.domain.tld, por ejemplo *.blog.rediris.es

Incidencias - ISC de RedIRIS

- SCP
  - Los administradores no pueden ver los certificados emitidos bajo sus dominios
  - Cambios de nombre, codificación UTF-8
  - ¿Cómo identificar a un usuario?
    - Diferentes correos para un usuario
      - iMMa (irisMailMainAddress)
      - iMAA (irisMailAlternateAddress)
      - mail
    - Uso de sPUC? http://www.rediris.es/sir/docs/spuc.html

Incidencias - COMODO

- Avisos
  - Avisos de expiración de certificado llegan a RedIRIS
  - No envían avisos de emisión de certificados SCP
- Retrasos en la firma de certificados
  - Validación de control de dominios (DCV)

DCV (Domain Control Validation)
Verificación de la autoridad sobre el FQDN

- Problema
  - Solicitantes no autorizados (por no ser dueños de los FQDNs) consiguieron validar solicitudes y se emitieron los certificados.
- Solución
  - Verificación de la autoridad sobre el FQDN antes de validar la solicitud
  - COMODO exige prueba de que el solicitante es la persona que tiene el control sobre el FQDN que se desea certificar
    - Uso del mecanismo DCV
    - Envío de un correo electrónico con un código necesario para una validación posterior vía web

DCV (Domain Control Validation)
Verificación de la autoridad sobre el FQDN

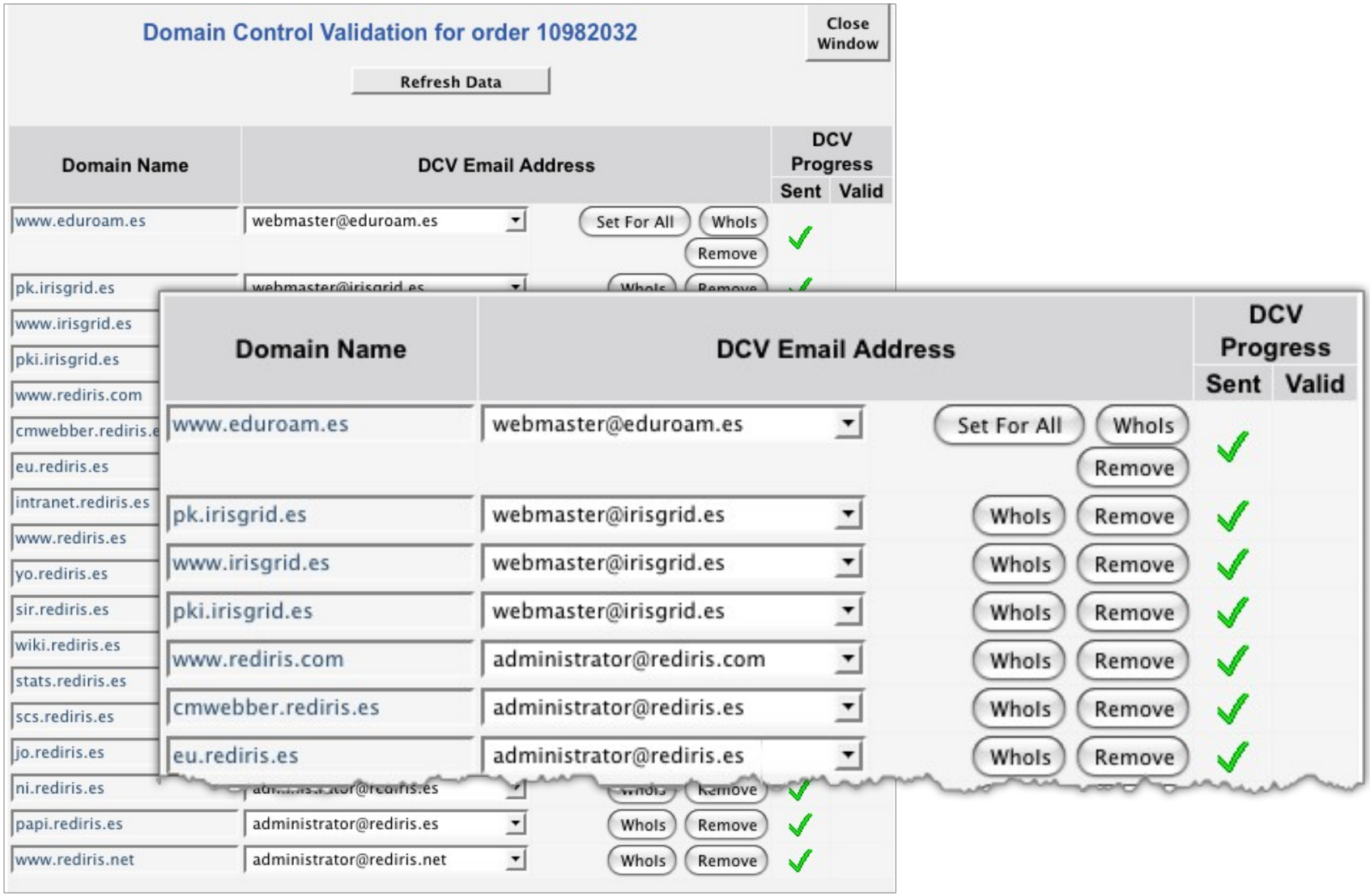
- Descripción del procedimiento DCV
  - De la CSR se extrae el dominio a validar
  - Se presenta una lista de direcciones al usuario para que elija donde recibir el código de validación. La lista se genera en base a
    - Datos obtenidos del Whois +
    - Lista de 5 nombres (decididos por Google, MS y Mozilla) por cada subdominio

      admin@
      administrator@
      hostmaster@
      postmaster@
      webmaster@
  - COMODO envía el código a esa dirección
  - El usuario recibe el código y valida el dominio vía web
  - COMODO valida la solicitud y emite el certificado al instante

DCV y tipos de certificado

- Certificados con un dominio
  - Se usa DCV
    - Se envía un mensaje
- Certificados con varios dominios
  - Se usa DCV para cada dominio
    - Se enviará un mail por cada dominio
    - No se emite el certificado hasta que se han validado todos los dominios
  - Se intentará crear grupos de dominios con el mismo TLD para disminuir el número de mensajes.
    - a1b1.rediris.es, a1b2.rediris.es, a1b3.rediris.es
    - a2b1.rediris.com, a2b2.rediris.com
  - Estamos probando con el interface de COMODO para ver opciones de implementación

DCV para www.rediris.es
Y otros 17 dominios más



DCV para www.rediris.es
Y otros 17 dominios más

De: Comodo Security Services <noreply@trust-provider.com>
Asunto: **Demonstrate domain control and approve 12 domains for SSL/TLS certificate order #10982032**
Fecha: 23 de noviembre de 2011 20:12:01 GMT+01:00
Para: administrator@rediris.es

Dear administrator@rediris.es,

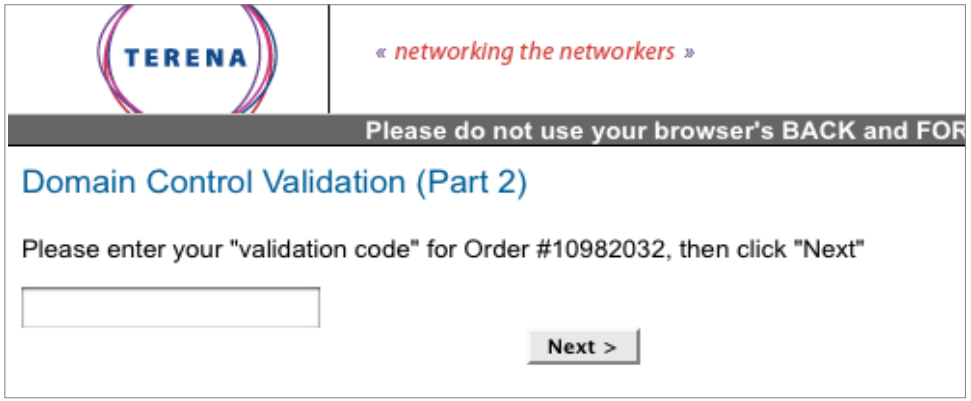
We have received a request to issue an SSL certificate for
cmwebber.rediris.es
eu.rediris.es
intranet.rediris.es
jo.rediris.es
ni.re
is.es
papi.rediris.es
scs.rediris.es
sir.rediris.es
stats.rediris.es
w
.rediris.es
www.rediris.es
yo.rediris.es.

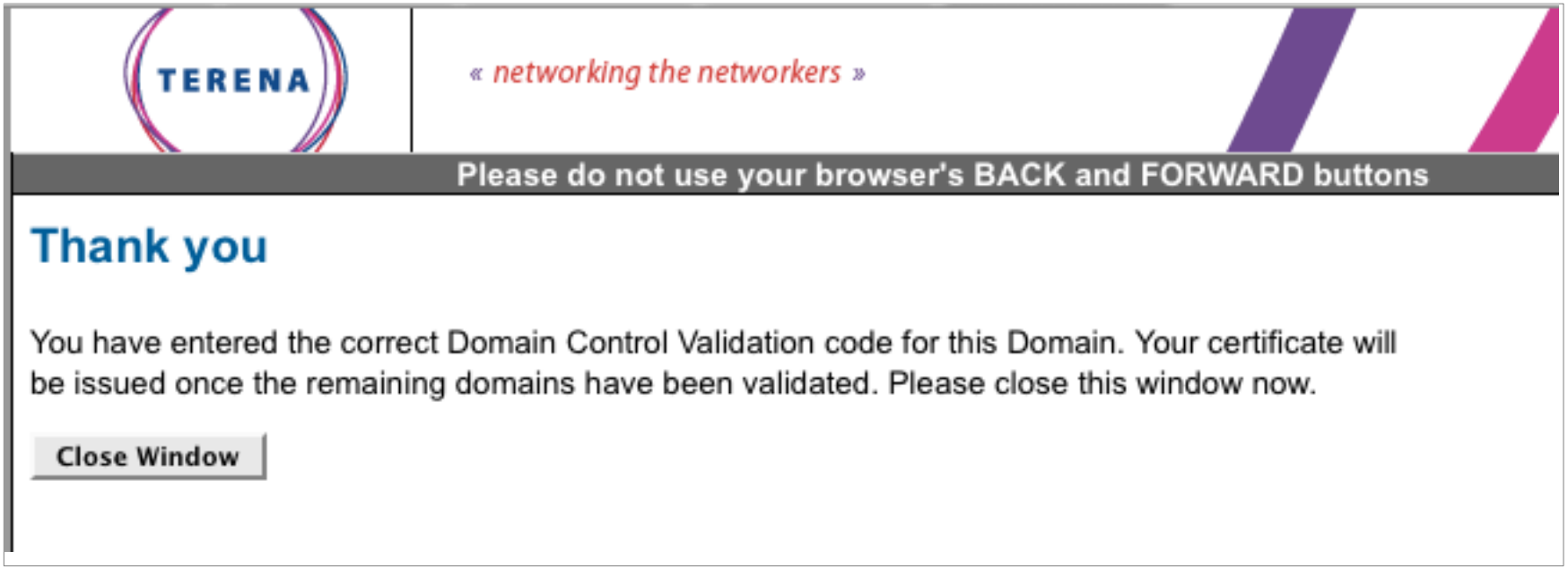
Please ignore this email if neither you nor a trusted colleague made this
request for a certificate.

Otherwise, please browse to
https://secure.comodo.net/products/EnterDCVCode?orderNumber=10982032
and enter the following "validation code":

[redacted]

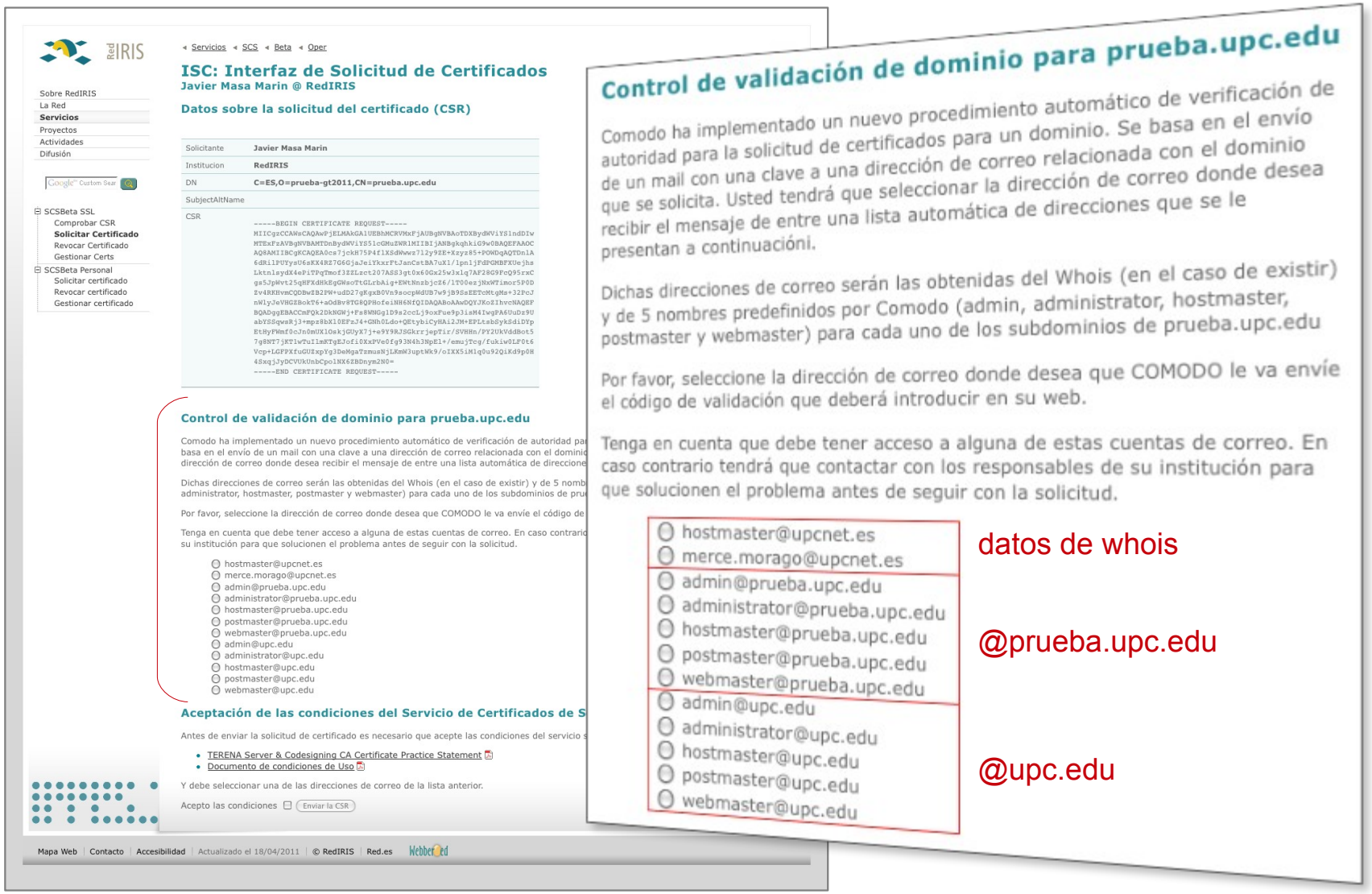
DCV para www.rediris.es
Y otros 17 dominios más





Solicitud de certificado usando DCV
para CN=prueba.upc.edu

Solicitud de certificado usando DCV



Índice

¡Muchas gracias!

Red IRIS

Más de 20 años al servicio de la investigación