

SCS/SCP

Servicio de certificados de RedIRIS

Javi Masa - javier.masa@rediris.es

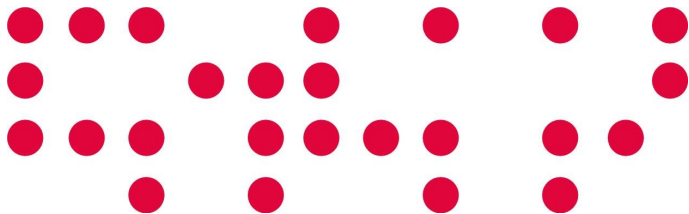


red.es



Barcelona, 02/06/2011

- 1 Bienvenida**
- 2 Escenario actual
- 3 Estadísticas
- 4 Incidencias
- 5 Ruegos y preguntas



- **Vídeo**
 - Mediante Adobe Connect
- **Material adicional**
 - Presentación disponible en
 - <http://www.rediris.es/scs/coord/gt2011/>

- Aumento de instituciones en el servicio
- Aumento de certificados emitidos
- Aumento de perfiles disponibles
 - Certificado SSL de servidor
 - Certificado personal (SCP)
- Disminución del staff
 - Dani dejó RedIRIS en Febrero
- Aumento de carga de trabajo
 - Para mi :(

- Mejoras en el ISC
 - Administración de certificados
 - Búsqueda en la tabla
 - Ordenación de columnas
 - Paginación de resultados

← Servicios ← SCS ← ISC ← Administración

ISC: Interfaz de Solicitud de Certificados

Javier Masa Marin @ RedIRIS como Administrador

Muestra entradas

Buscar:

Subject DN ▲	Estado ▼	orderNumber ▼	Propietario ▼	Institucion ▼	Validez ▼
/C=ES/O=RedIRIS /CN=rediris.es	issued	10382316	Javier Masa Marin	rediris	2011-05-12 02:00 2014-05-12 01:59
/C=ES/O=RedIRIS /CN=stats.rediris.es	issued	10364477	Javier Masa Marin	rediris	2011-05-06 02:00 2014-05-06 01:59
/C=ES/O=RedIRIS /CN=www.rediris.es	issued	10190256	Javier Masa Marin	rediris	2011-03-14 01:00 2014-03-14 00:59
/C=ES/O=RedIRIS /CN=www.rediris.es	issued	10386259	Javier Masa Marin	rediris	2011-05-13 02:00 2014-05-13 01:59

Mostrando 1 de 4 de un total de 4 entradas - filtradas de 56 entradas

Inicio | Anterior | 1 | Siguiente | Final

- **Certificados personales (SCP)**

- Disponible desde el 20/02/2011
- Guía: <http://www.rediris.es/scs/perfiles/personal/guia.html>
- 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/>

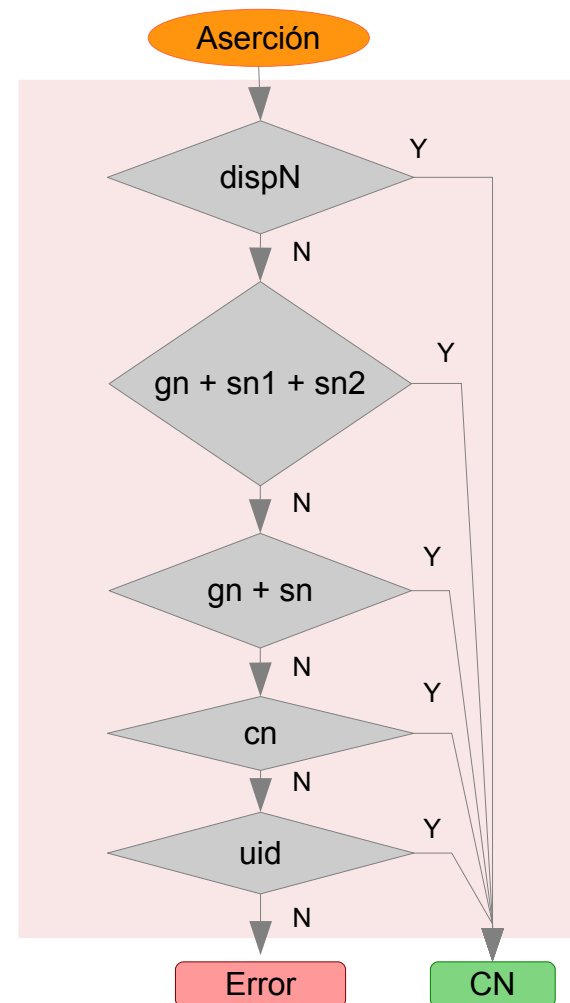
• Composición del CN

- 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>



- **cn=Javier Masa Marin, uid=masa**

- C=ES, O=rediris.es, CN=**Javier Masa Marin**,
unstructuredName= <http://yo.rediris.es/soy/masa@rediris.es/>

- **uid=gelpi / uid=mimaen**

- C=ES, O=bsc.es, CN=**gelpi**,
unstructuredName= <http://jo.rediris.es/soc/gelpi@bsc.es/>
- C=ES, O=upv.es, CN=**mimaen**,
unstructuredName= <http://jo.rediris.es/soc/mimaen@upv.es/>

- **uid=rodrigo.aragon**

- C=ES, O=ivie.es, CN=**rodrigo.aragon**
unstructuredName= <http://yo.rediris.es/soy/rodrigo.aragon@ivie.es/>

- **uid=joaquim.vericat@iqs.url.edu**

- C=ES, O=url.edu, CN=**joaquim.vericat@iqs.url.edu**,
unstructuredName= <http://jo.rediris.es/soc/joaquim.vericat@iqs.url.edu@url.edu/>

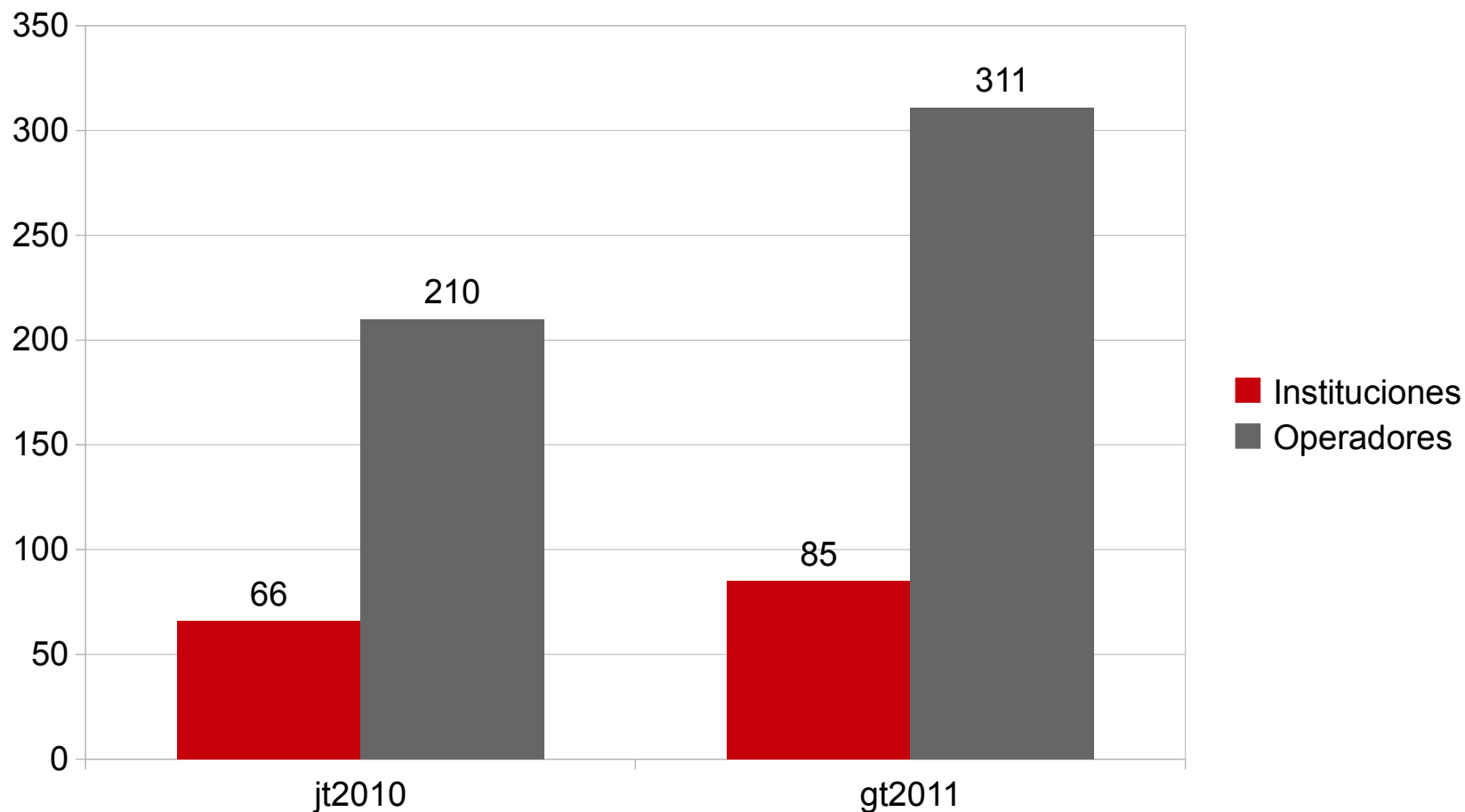
- ¿Cómo se da de alta la institución en el servicio SCP?
 - Un operador de SCS debe enviar un mail a scs-ra@rediris.es
 - Identificador del conector SIR
 - Dirección de correo corporativa de la institución dedicada a dar soporte a sus usuarios
 - URL explicativa del servicio para los usuarios finales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

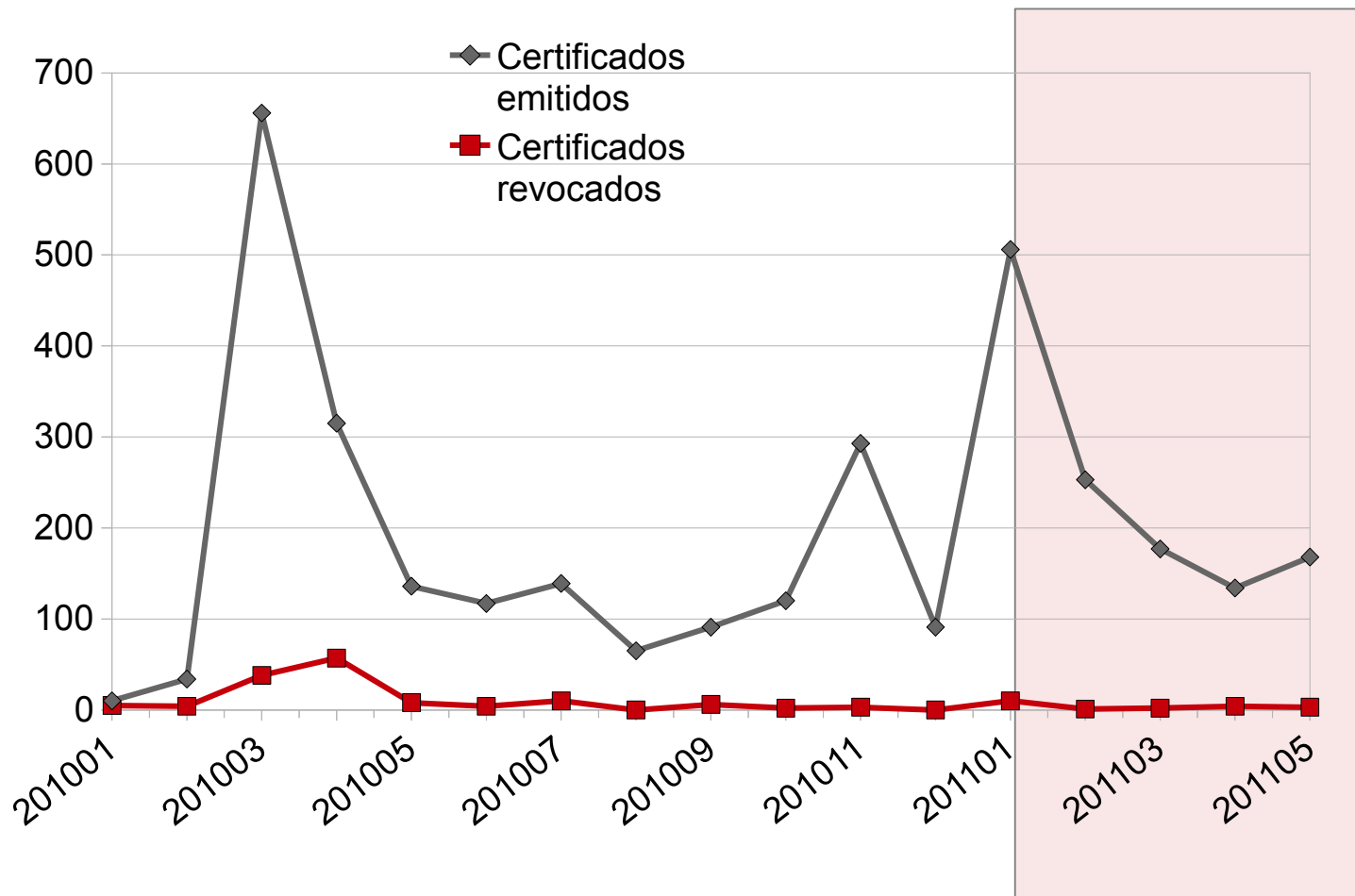
- **SSL servidor**

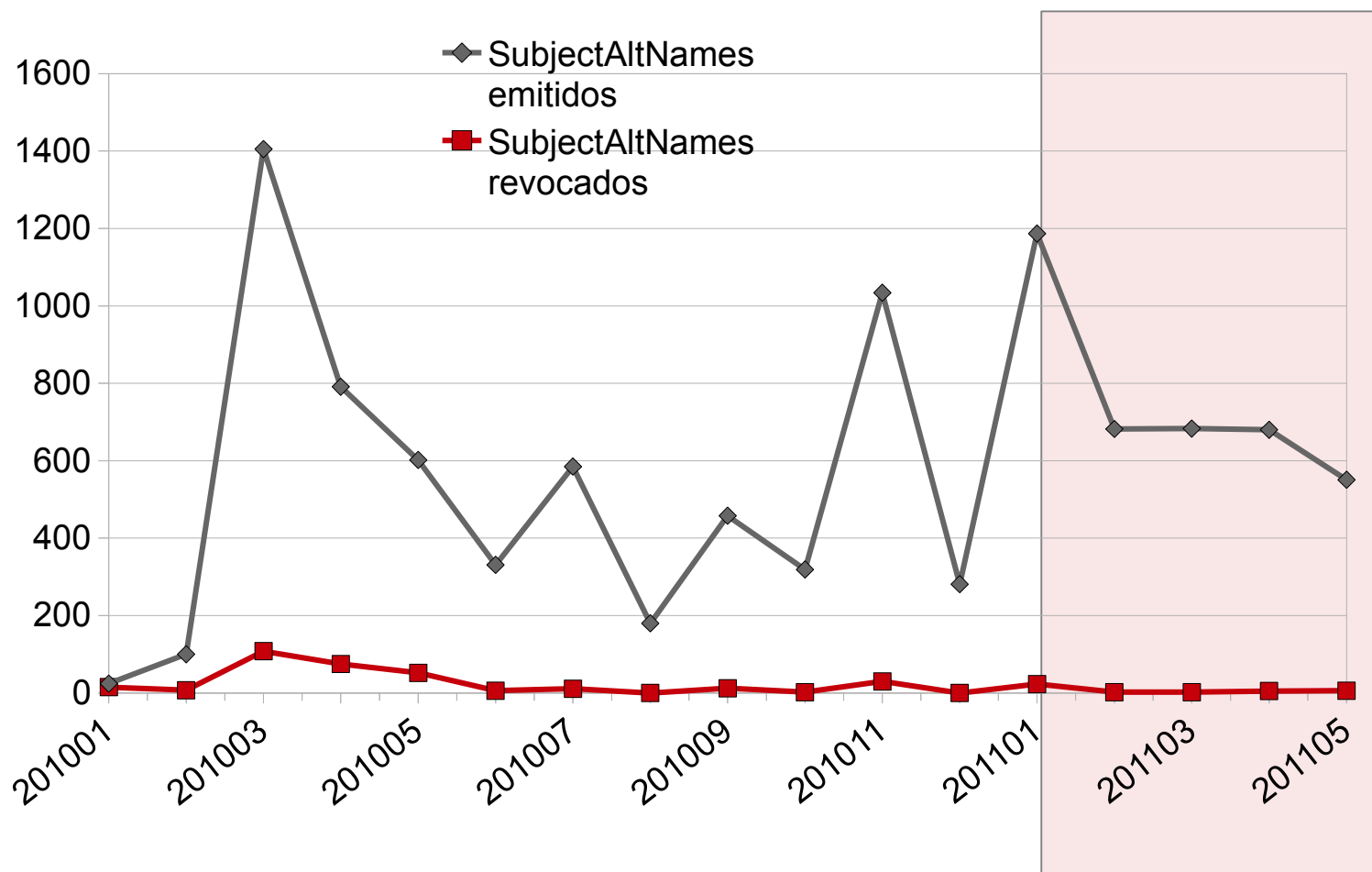
- Instituciones: 85
- Personas registradas: 311
- Certificados emitidos: 3148

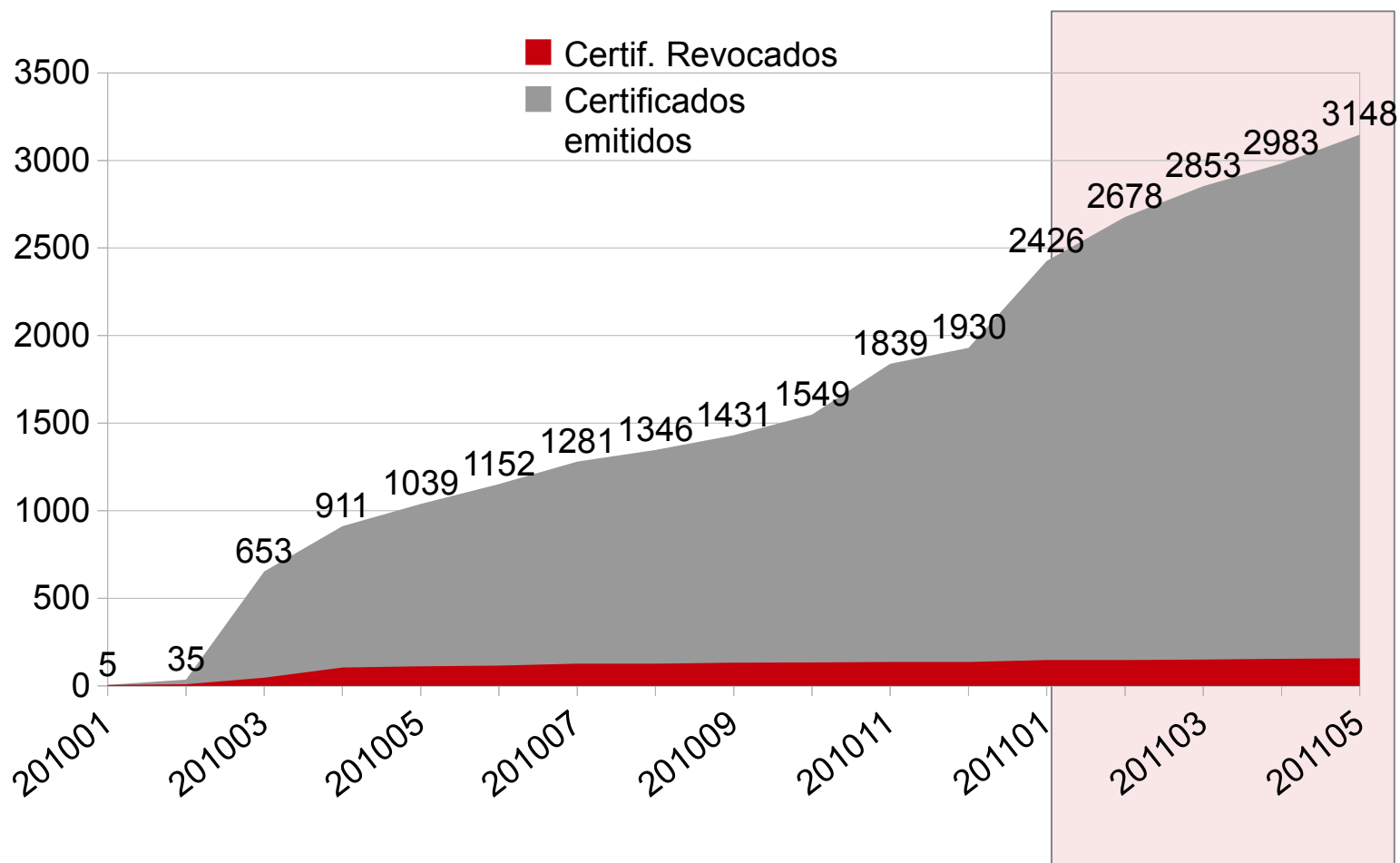
- **SCP**

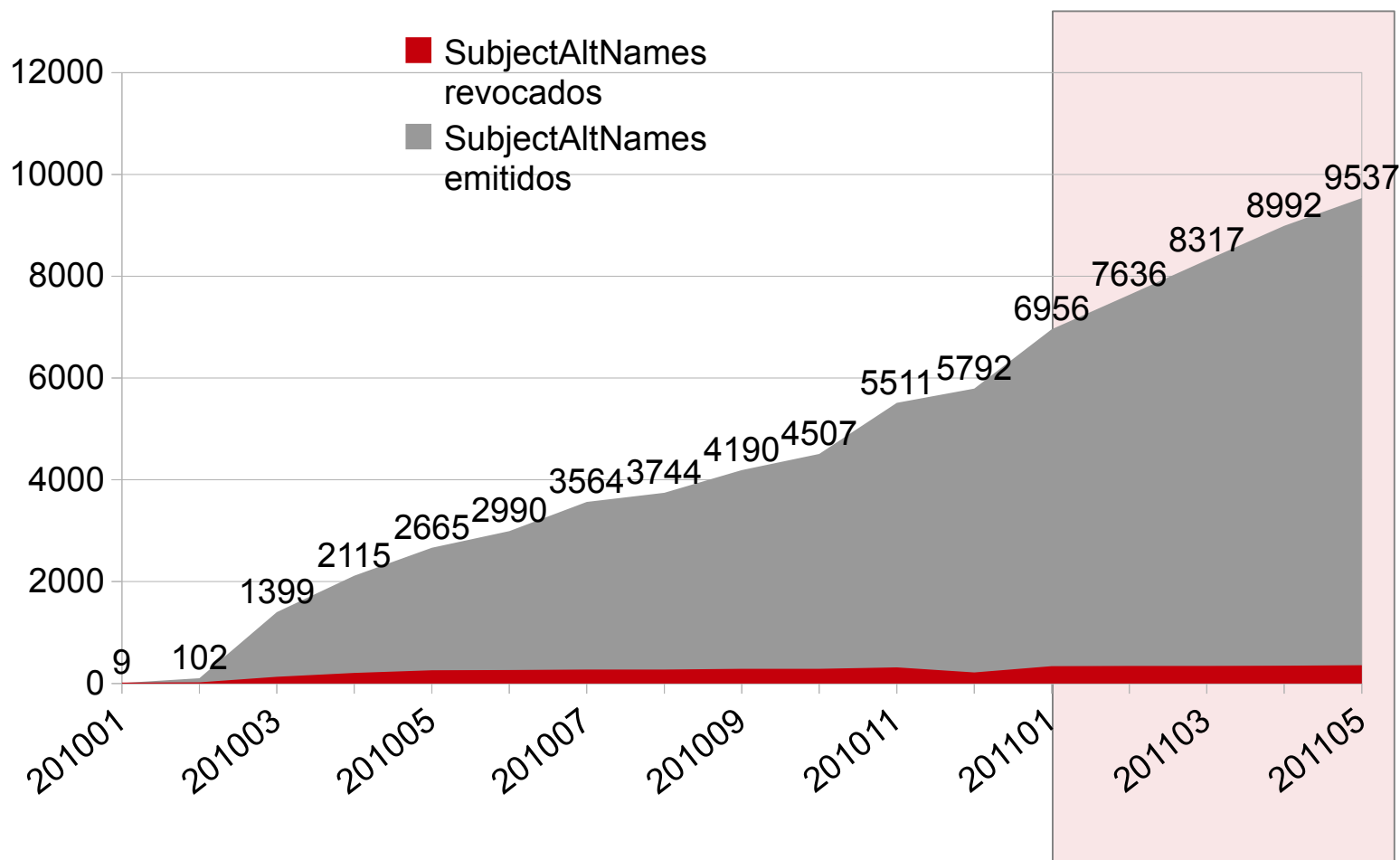
- Instituciones: 6
(BSC, CICA, IVIE, RedIRIS, UPV, URL)
- Certificados emitidos: 65
- UnstructuredName
 - <http://eu.rediris.es/son/uid@inst.domin> 5
 - <http://jo.rediris.es/soc/uid@inst.domain> 9
 - <http://yo.rediris.es/soy/uid@inst.domain> 51











- **RedIRIS - ISC**

- Claves de 1024 bits
- Aserciones que no envían correctamente el correo electrónico
 - Se han registrado de forma incorrecta en el ISC
- Cambios en direcciones de correo
- Certificados donde el FQDN = dominio de la institución
 - Por ejemplo: C=ES, O=UniversIRIS, CN=universiris.es

- **COMODO**

- No están enviando avisos de expiración de certificado
- No están enviando avisos de emisión de certificados SCP
- Emisión de varios certificados fraudulentos

- **Compromiso de una cuenta de operador en una RA**

- Una RA sufre un ataque el 15/03/2011 y el atacante consigue acceso a una cuenta de operación
 - Ataque desde la IP 212.95.136.18 - Teherán (Irán)
 - Según COMODO el ataque podría estar incitado por el gobierno
 - El pirata Iraní dice que no tiene nada que ver con su gobierno
- Uso fraudulento de la cuenta de operador
 - Creación de una cuenta nueva para no llamar la atención
 - Solicitud de 9 certificados
 - Validación de 9 certificados

Incidencias - COMODO

Certificados emitidos de forma fraudulenta



MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

Domain	Serial	Seen live on the internet
mail.google.com	047ECBE9FCA55F7BD09EAE36E10CAE1E	No
www.google.com	00F5C86AF36162F13A64F54F6DC9587C06	No
login.yahoo.com	00D7558FDAF5F1105BB213282B707729A3	Yes
login.yahoo.com	392A434F0E07DF1F8AA305DE34E0C229	No
login.yahoo.com	3E75CED46B693021218830AE86A82A71	No
login.skype.com	00E9028B9578E415DC1A710A2B88154447	No
addons.mozilla.org	009239D5348F40D1695A745470E1F23F43	No
login.live.com	00B0B7133ED096F9B56FAE91C874BD3AC0	No
global trustee	00D8F35F4EB7872B2DAB0692E315382FB0	No

- **Medidas urgentes adoptadas**

- Revocación de los 9 certificados emitidos
- Cuarentena de la RA afectada
- Cuarentena de las solicitudes desde esa RA
- Monitorización del tráfico OSCP
 - No se han intentado usar 8 de los certificados emitidos
 - Se desconoce si el atacante llegó a recibir todos los certificados antes de que fuesen revocados

- **Más información**

- <http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html>
- <http://blogs.comodo.com/category/it-security/>

- Retrasos en la firma de solicitudes
 - Comprobación manual de las solicitudes
- Nuevos procedimientos de verificación
 - Verificación de cuentas de operación de RAs
 - Cambios de clave de operación en 24 horas
 - Caducidad de las claves cada 90 días
 - Cambios cada 3 meses y modificaciones en nuestro software
 - Listas blancas de IPs de acceso a cuentas de operación
 - Listas blancas de IPs de acceso a las APIs
 - Verificación de autoridad sobre FQDNs a certificar
 - DCV (Domain Control Validation)

- **Problema**

- Solicitantes no autorizados (por no ser dueños de los FQDNs) han conseguido validar solicitudes.

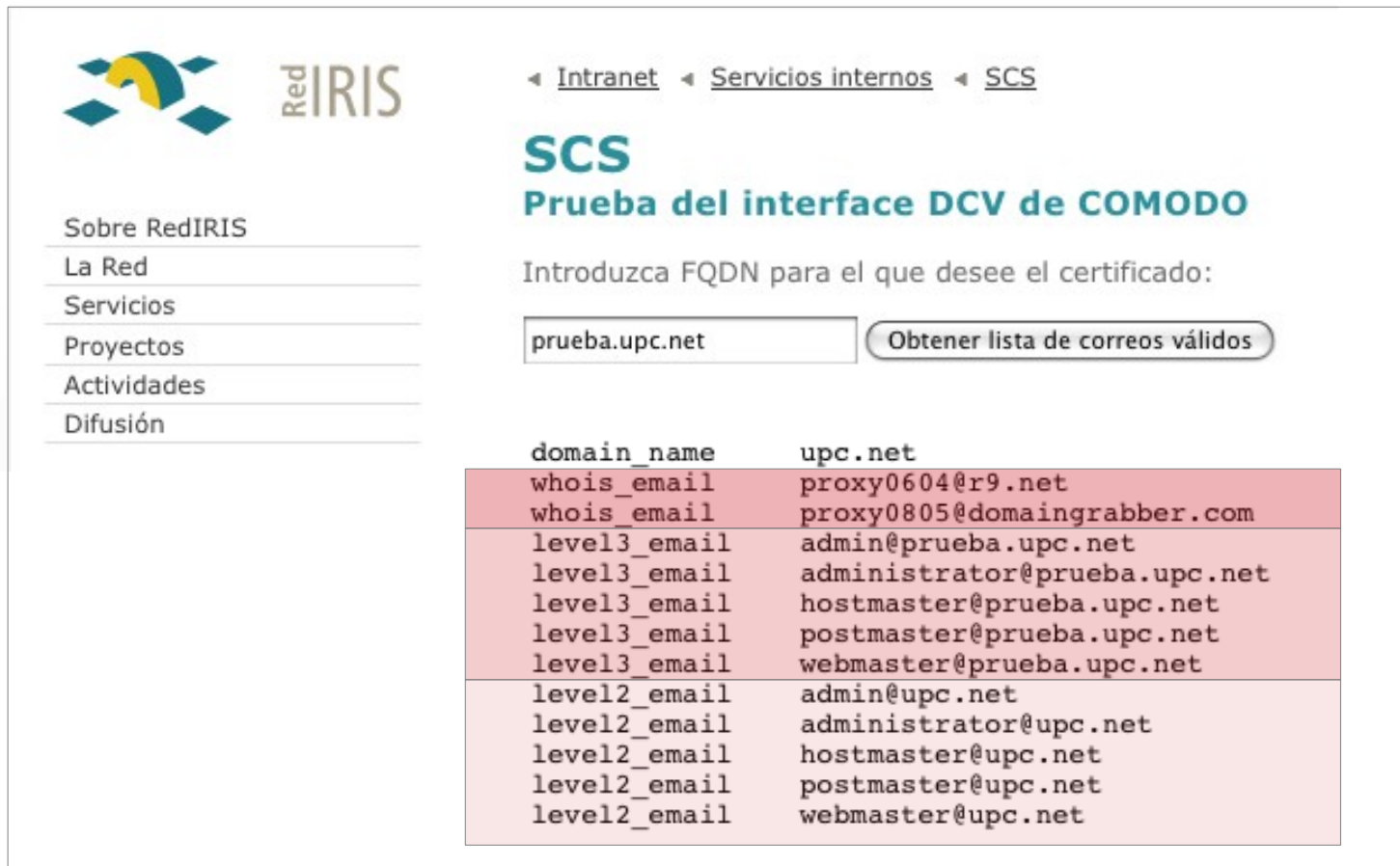
- **Solución**

- Verificación de la autoridad sobre el FQDN antes de validar la solicitud
- COMODO exigirá prueba de que el solicitante es la persona que tiene el control sobre el FQDN que se desea certificar
 - Uso de DCV
 - Envío de un PIN por correo para validación posterior en la web de COMODO

- Descripción del procedimiento DCV

- COMODO obtiene el dominio de la CSR
- Presenta al usuario una lista de direcciones de correo para que elija una donde se enviará el código de validación de la solicitud
 - Usa datos del Whois
 - Usa una lista de 5 nombres para cada subdominio
 - Decididos por Google, MS y Mozilla
 - **admin@** - **administrator@** - **hostmaster@** - **postmaster@** - **webmaster@**
 - El solicitante elige la dirección donde desea recibir el código
- COMODO envía el código a esa dirección
- El solicitante recibe el mensaje
 - Va a una página web a validar la solicitud e introduce el código recibido
- COMODO valida la solicitud y emite el certificado

- DCV para prueba.upc.net



The screenshot shows the RedIRIS SCS interface for DCV testing. On the left is a navigation menu with items: Sobre RedIRIS, La Red, Servicios, Proyectos, Actividades, and Difusión. The main content area has a breadcrumb trail: Intranet > Servicios internos > SCS. Below this is the title 'SCS Prueba del interface DCV de COMODO'. A form prompts the user to 'Introduzca FQDN para el que desee el certificado:' with the input 'prueba.upc.net' and a button 'Obtener lista de correos válidos'. Below the form is a table of email addresses:

domain_name	upc.net
whois_email	proxy0604@r9.net
whois_email	proxy0805@domaingrabber.com
level3_email	admin@prueba.upc.net
level3_email	administrator@prueba.upc.net
level3_email	hostmaster@prueba.upc.net
level3_email	postmaster@prueba.upc.net
level3_email	webmaster@prueba.upc.net
level2_email	admin@upc.net
level2_email	administrator@upc.net
level2_email	hostmaster@upc.net
level2_email	postmaster@upc.net
level2_email	webmaster@upc.net

DCV (Domain Control Validation)

Verificación de la autoridad sobre el FQDN



MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

¿Cómo vamos a implementar DCV en el ISC?



RedIRIS

Servicios < SCS < Beta < Oper

ISC: Interfaz de Solicitud de Certificados

Javier Masa Marin @ RedIRIS

Validez del certificado:

Tipo de servidor:

CSR - Certificate Signing Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0jCCABoCAQAwODELMAkGA1UEBhMCRVVxEDAOBgNVBAoTB1J1ZElSSVMxZAV
BgNVBAMTDnBrLmlyeXNncmlkLmVzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAnOkzwqnown9lmi8d3rDQk1Xdyo3V1rDCD7ANBYWMScwe+jpjyhEZ1H0r
RbiNblZMKELqT0zA7JES/Pogf7kR6+wn5L/fDIS7/YkAkU4WqfDmJNMIa29Vrr17
J3G6khoUwXNk0mqWYJwbamaDz1833bjbjXpcAk/Pec2h88T19+oU90b2pEsFR7EA
8IaHfx0X5RWHpoJgdhT22P++NtxIa+yiXJXs9dqDyMz82b0I6uGY94T0umhOQ4JW
U8eOHg/tFoDY8ebgYu1MT/GkbaTpBtde2A2PA1Kb98f60/tJapmgJ6V0C9SalQOA
6q3kxax5NKNGdfmrWge5Jp4ynyGDwIDAQABOFUwUwYJKoZIhvcNAQkOMUYwRDAJ
BgNVHRMEAjAAMAsGAlUdDwQEAwIFoDaqBgNVHREIzAhgg5way5pcmlzZ3JpZC5l
c4IPcGtpLmlyeXNncmlkLmVzMAOGCSqGSIb3DQEBAQUAA4IBAQCOTOnCnDrfTPmm9
focFKZYWcY4kTb3s3myRIJnDLPE+JoxzvehWwF3WgCtgc+uYPvakG0BrZU2NVabX
pAvh/xLR5ugnJk+q20wGI dwBVcl1EFqrgEQQ9HPWQvCAP8EX0pwvqhXofoKMEbt
6iY6rRtLNh77k7qtRMQ76bsXWdX2uDeM9GNIRAnFT0JX0532bnDXhhOjmaOpJMLM
HP+WEUnVzQKlm+ke3nSZH77heOwH/VfEWAuPyfcU9i6sBDQ780Hr1P923TQGL1f
EmqNfOlxcSBmItU/ZS00zg0aakkP5z9K65pEJk3xo3uC6W+pdwrJ5ge+87PiHTkz
```

Dirección de correo:

SCSBeta SSL

- Comprobar CSR
- Solicitar Certificado**
- Revocar Certificado
- Gestionar Certs

SCSBeta Personal

- Solicitar certificado
- Revocar certificado
- Gestionar certificado

Solicitud de certificado usando DCV

Mail recibido desde COMODO



MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

« [Back to Search Results](#) Archive Report spam Delete Move to Inbox Labels ▾ More actions ▾

ORDER #7872647 - Domain Control Validation for [REDACTED]

★ Comodo Security Services to root

C·O·M·O·D·O

Domain Control Validation for [REDACTED]

Dear [root@\[REDACTED\]](mailto:root@[REDACTED]),

We have received a request to issue an SSL certificate for [REDACTED].

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

Otherwise, please browse [here](#) and enter the following "validation code":

WON68Z6L2iD1IHZ04Cp106sqQf5RyfjJ

Kind Regards,

Comodo Security Services
Support Website: <http://support.comodo.com>
Validation Docs Fax: US +1.866.831.5837 / Canada +1.866.831.5837 / Worldwide +1.801.303.9291

Solicitud de certificado usando DCV

Formulario de control de validación



COMODO

Please do not use your browser's BACK and FORWARD buttons

Domain Control Validation (Part 2)

Please enter your "validation code" for Order #7872647, then click "Next"

Next >

- ¿Alguna pregunta?



red.es

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Fax: 91 212 76 35
www.red.es

RedIRIS. Edificio CICA
Avenida Reina Mercedes s/n
41012. Sevilla. España

Tel: 95 505 66 00
Fax: 95 505 66 27
www.rediris.es