SCS

Servicio de certificados de RedIRIS

Javi Masa - javier.masa@rediris.es

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMIA Y COMPETITIVIDAD
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
red.es
RedIRIS

Bilbao, 27/11/2012

Índice de contenidos

DCV

- DCV (Domain Control Validation)
  - Mecanismo de verificación de la autoridad sobre un dominio
- Comodo y DCV
  - DCV en producción desde el 18 de Junio de 2012
  - Comodo exige una prueba de que el solicitante es la persona que tiene el control sobre el dominio del FQDN que se desea certificar
  - Para una solicitud de certificado multidominio se realiza un DCV por cada dominio asociado a los FQDNs que lleve la solicitud
    - Comodo no emitirá el certificado hasta que hayan pasado todas las verificaciones DCV para todos los dominios de la solicitud
- Disponemos de varios métodos DCV

DCV - métodos disponibles

- Basado en mail
  - Envío de un correo electrónico a una dirección determinada con un código necesario para una validación posterior vía web
  - Soportado en ISC
- Basado en HTTP
  - Fichero de texto en el servidor web con información basada en 2 hashes generados a partir de la CSR (MD5 y SHA-1)
  - Soportado en ISC (beta)
- Basado en DNS (registro CNAME)
  - Creación de un CNAME con información basada en 2 hashes generados a partir de la CSR (MD5 y SHA-1)
  - Soportado en ISC (beta)

DCV - Basado en mail

- Descripción del proceso
  - El solicitante vuelca la CSR en el ISC
  - Para cada FQDN de la solicitud
    - Comodo genera una lista de direcciones de correo basada en la CSR y la presenta al usuario para que elija dónde 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, una vez que RedIRIS valida la solicitud, envía el código de verificación al correo seleccionado
    - El solicitante recibe el código y valida el dominio vía web
  - Comodo emite el certificado si todos los dominios han sido validados

DCV - Basado en HTTP

- Descripción del proceso
  - El solicitante vuelca la CSR en el ISC
  - Comodo genera dos hashes basados en la CSR
    - Uno en MD5 y otro en SHA-1
  - Para cada FQDN de la solicitud
    - Crear un fichero cuyo nombre sea el hash en MD5 y “.txt”
    - El contenido del fichero serán 2 líneas, una con el hash en SHA-1 y otra con la cadena "comodoca.com"
    - Poner el fichero en la raíz de la web
  - RedIRIS valida la solicitud y la envía a Comodo
  - Comodo revisa el contenido del fichero cuando le llega la solicitud
    - Valida el dominio
  - Emite el certificado si todos los dominios han sido validados

DCV - Basado en HTTP

- Ejemplo
  - Certificado multidominio con FQDN1 y FQDN2
  - Supongamos que Comodo genera los hashes
    MD5: 9350CE346979601729CCA18EB5E7100 y
    SHA-1: BED81F3B8090D0CD6DD71877879919 5E3C506AA3
  - Crear ficheros
    - http://FQDN1/9350CE346979601729CCA18EB5E7100C.txt
    - http://FQDN2/9350CE346979601729CCA18EB5E7100C.txt
  - Contenido de cada uno de los 2 ficheros:
    - BED81F3B8090D0CD6DD71877879919 5E3C506AA3
      comodoca.com

DCV - Basado en DNS (registro CNAME)

- Descripción del proceso
  - El solicitante vuelca la CSR en el ISC
  - Comodo genera dos hashes basados en la CSR
    - Uno en MD5 y otro en SHA-1
  - Para la validación buscará los registros CNAME de los FQDNs para los que se están solicitando certificados.
  - Los hashes deben ser introducidos de la siguiente manera:
    - <MD5 hash>.FQDN. CNAME <SHA-1 hash>.comodoca.com
  - RedIRIS valida la solicitud y la envía a Comodo
  - Comodo busca en el DNS cuando le llega la solicitud
    - Valida el dominio si encuentra el registro correspondiente
  - Emite el certificado si todos los dominios para esa solicitud de certificado han sido validados

DCV - Basado en DNS (registro CNAME)

- Ejemplo
  - Certificado multidominio con FQDN1 y FQDN2
  - Supongamos que Comodo genera los hashes
    MD5: 9350CE346979601729CCA18EB5E7100 y
    SHA-1: BED81F3B8090D0CD6DD71877879919 5E3C506AA3
  - Añadir al DNS
    - 9350CE346979601729CCA18EB5E7100C.FQDN1. CNAME BED81F3B8090D0CD6DD71877879919 5E3C506AA3.comodoca.com
    - 9350CE346979601729CCA18EB5E7100C.FQDN2. CNAME BED81F3B8090D0CD6DD71877879919 5E3C506AA3.comodoca.com

DCV - Ejemplo de solicitud de certificado

- Solicitud de un certificado con 3 FQDNs
  - pruebaDCV.rediris.es
  - pki.irisgrid.es
  - www.eduroam.es

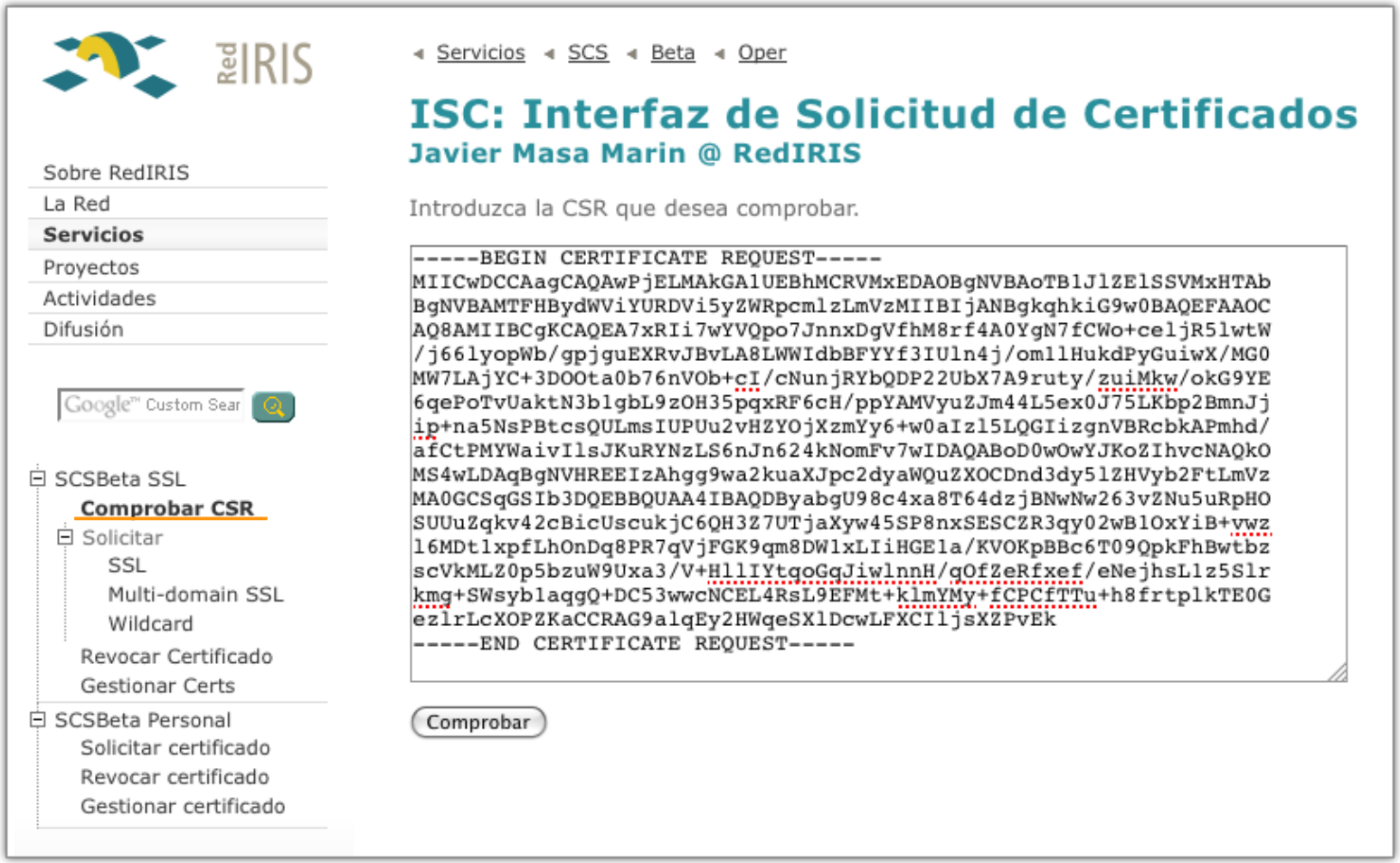
DCV - Ejemplo de solicitud de certificado

- Generar la CSR con la herramienta scs-genCSR.sh

```
$ ./scs-genCSR.sh
Generador de clave privada y CSR (Certificate Signing Request)
-----------------------------------------------------------
¿Para que tipo de certificado desea generar la solicitud?
   1. Certificado simple (sólo CN)
   2. Certificado con múltiples dominios (CN y Subject Alternative Names)
   3. Certificado Wildcard

Seleccione una opcion [1]: 2
Certificado con múltiples dominios (CN y Subject Alternative Names) seleccionado
FQDN/CommonName (p. ej. www.example.com): pruebaDCV.rediris.es
OrganisationName (p. ej. RedIRIS): RedIRIS
...
Introduzca SubjectAltName para el certificado, uno por línea.
Introduzca una línea en blanco para finalizar
SubjectAltName: DNS: pki.irisgrid.es
SubjectAltName: DNS: www.eduroam.es
SubjectAltName: DNS:
Running OpenSSL...
Generating a 2048 bit RSA private key  .....+++ .....
```

DCV - Ejemplo de solicitud de certificado
Comprobación CSR



DCV - Ejemplo de solicitud de certificado
Comprobación CSR - resultado comprobación

Resultado de la comprobación de la CSR

Ok - La CSR está bien formada

Datos de la CSR

CN=pruebaDCV.rediris.es
O=RedIRIS
C=ES
Public
Key=3082010A0282010100EF14488BBC18550A68EC99E7C438157E133CADFE00D1880DEDF096
Key Size=2048
dnsName(s)=pki.irisgrid.es,www.eduroam.es

md5=9350CE346979601729CCA18EB5E7100C
sha1=BED81F3B8090D0CD6DD718778799195E3C506AA3

-----BEGIN CERTIFICATE REQUEST-----
MIICwDCCAagCAQAwPjELMAkGA1UEBhMCRVMxEDAOBgNVBAoTB1JlZElSSVMxHTAb
BgNVBAMTFHBydWViYURDVi5yZWRpcmlzLmVzMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEA7xRIi7wYVQpo7JnnxDgVfhM8rf4A0YgN7fCWo+celjR5lwtW
/j66lyopWb/gpjguFXRvJBvLA8lWWIdbBFYYf3IUln4j/om1lHukdPyGuiwX/MG0
MW7LAiYG+3P6

DCV - Ejemplo de solicitud de certificado
Volcado de la CSR en el ISC

DCV - Ejemplo de solicitud de certificado
Descripción DCV - Mail

DCV - Ejemplo de solicitud de certificado
Descripción DCV - HTTP

...ntactar con los respons... de su ... ...n ... que solu...onen el p... ... ...r con la solicitud.

2. Validación de dominios basado en HTTP

Comodo genera dos hashes basados en la CSR, uno MD5 y otro SHA1, y para la validación buscará, usando sólo HTTP, un fichero de texto plano en la raíz del servidor web que contenga dicha información.

Para cada dominio, el nombre del fichero contiene el hash en MD5 y la cadenta ".txt":

```
http://yourdomain.com/<MD5 hash CSR>.txt
```

y el contenido del fichero serán 2 líneas, una con el hash en SHA1 y otra con la cadena "comodoca.com":

```
<SHA1 hash CSR>
comodoca.com
```

Para cada dominio de la solicitud actual, y utilizando los hashes generados por COMODO (MD5=9350CE346979601729CCA18EB5E7100C y SHA1=BED81F3B8090D0CD6DD718778799195E3C506AA3), el fichero debe llamarse:

```
http://yourdomain.com/9350CE346979601729CCA18EB5E7100C.txt
```

y el contenido debe ser:

```
BED81F3B8090D0CD6DD718778799195E3C506AA3
comodoca.com
```

Nota: Servir el fichero sobre HTTPS o usar una redirección HTTP 302 hacia HTTPS causará un fallo en la verificación. Por favor utilice únicamente HTTP para este procedimiento.

3. Validación de dominios basado en DNS CNAME

DCV - Ejemplo de solicitud de certificado
Descripción DCV - DNS/CNAME

utilice [illegible] para este pro[illegible]

3. Validación de dominios basado en DNS CNAME

Comodo genera dos hashes basados en la CSR, uno MD5 y otro SHA1, y para la validación buscará los registros CNAME de los dominios para los que se están solicitando certificados.

Los hashes deben ser introducidos de la siguiente manera:

```
<MD5 hash CSR>.yourdomain.com. CNAME <SHA1 hash CSR>.comodoca.com
```

Para cada dominio de la solicitud actual, y utilizando los hashes generados por COMODO (MD5=9350CE346979601729CCA18EB5E7100C y SHA1=BED81F3B8090D0CD6DD718778799195E3C506AA3), el registro CNAME debería ser:

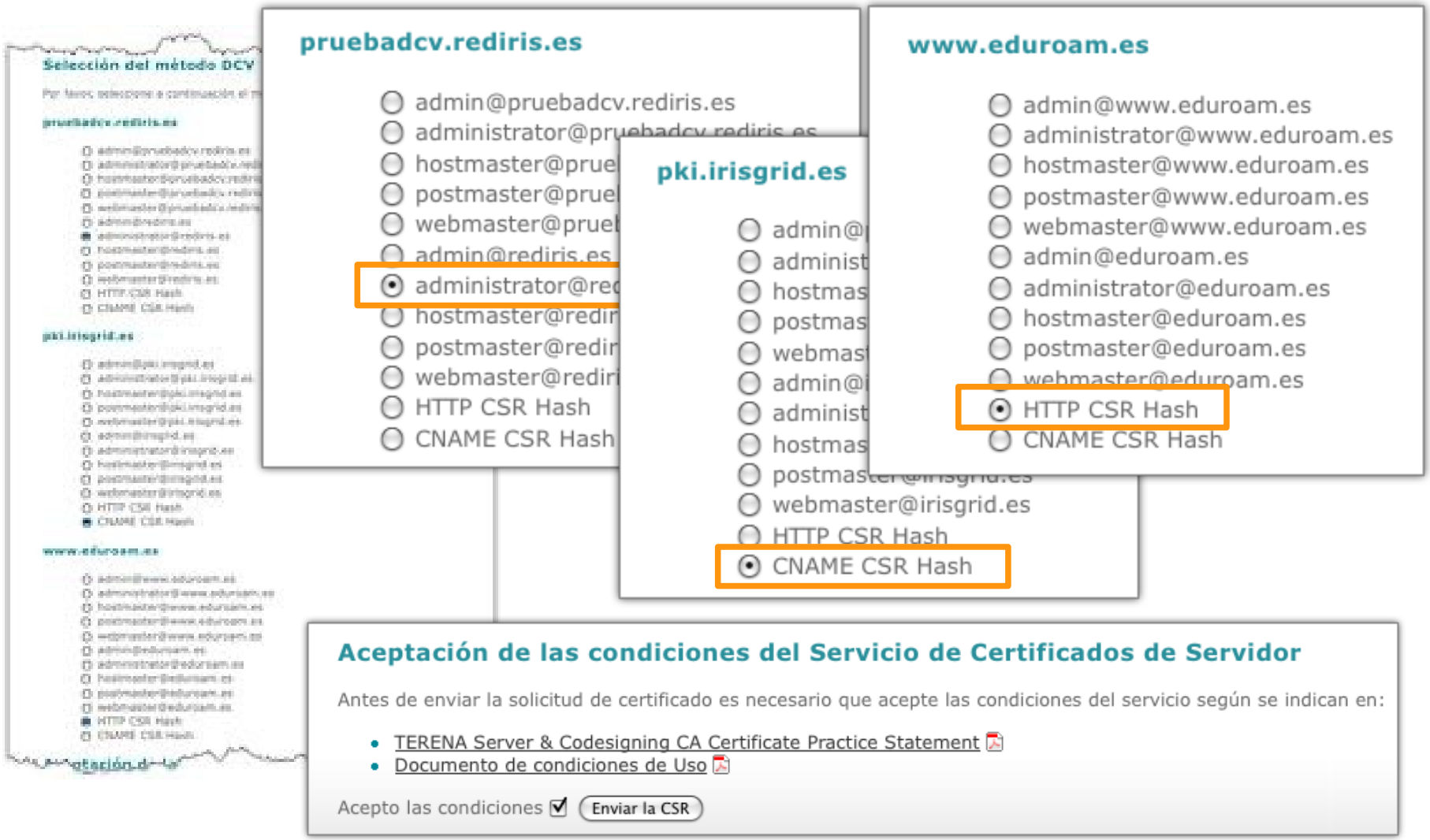
```
9350CE346979601729CCA18EB5E7100C.yourdomain.com. CNAME BED81F3B8090D0CD6DD718778799195E3C506AA3.comodoca.com
```

Nota: Por favor, tome nota del punto al final de cada TLD ya que es requerido para que la entrada sea totalmente cualificada.

Nota 2: Observe que yourdomain.com en el ejemplo anterior hace referencia al FQDN contenido en el certificado. Si usted está solicitando certificados multidominio, se deben crear registros CNAME separados para cada FQDN de la solicitud. Por ejemplo:

```
<MD5 hash CSR>.subdomain1.yourdomain.com. CNAME <SHA1 hash CSR>.comodoca.com
<MD5 hash CSR>.subdomain2.yourdomain.com. CNAME <SHA1 hash CSR>.comodoca.com
```

DCV - Ejemplo de solicitud de certificado
Elección método DCV



DCV - Ejemplo de solicitud de certificado
Envío de la solicitud

DCV - Ejemplo de solicitud de certificado
Aprobación por RedIRIS

ISC: Interfaz de Solicitud de Certificados

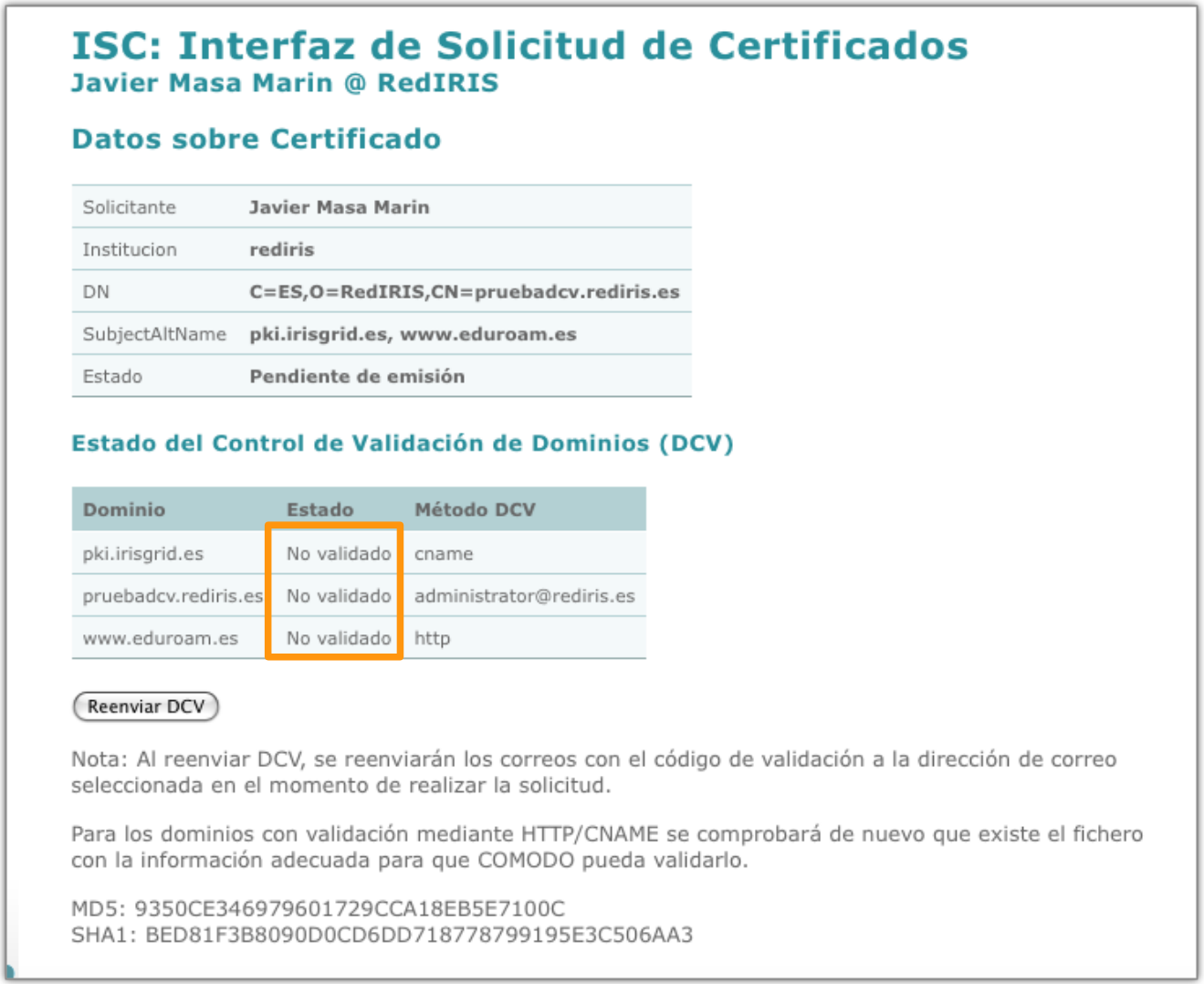
Javier Masa Marin @ RedIRIS

Datos sobre la solicitud del certificado (CSR)

Solicitante	**Javier Masa Marin** - javier.masa@rediris.es
Institucion	**rediris**
DN	**C=ES,O=RedIRIS,CN=pruebaDCV.rediris.es**
SubjectAltName	**pki.irisgrid.es, www.eduroam.es**
CSR	-----BEGIN CERTIFICATE REQUEST----- MIICwDCCAagCAQAwPjELMAkGA1UEBhMCRVMxEDAOBgNVBAoTB1J1ZElSSVMxHTAb BgNVBAMTFHBydWViYURDVi5yZWRpcmlzLmVzMIIBIjANBgkqhkiG9w0BAQEFAAOC AQ8AMIIBCgKCAQEA7xRIi7wYVQpo7JnnxDgVfhM8rf4A0YgN7fCWo+celjR5lwtW /j66lyopWb/gpjguEXRvJBvLA8LWWIdbBFYYf3IUln4j/omllHukdPyGuiwX/MG0 MW7LAjYC+3DOOta0b76nVOb+cI/cNunjRYbQDP22UbX7A9ruty/zuiMkw/okG9YE 6qePoTvUaktN3b1gbL9zOH35pqxRF6cH/ppYAMVyuZJm44L5ex0J75LKbp2BmnJj ip+na5NsPBtcsQULmsIUPUu2vHZYOjXzmYy6+w0aIzl5LQGIizgnVBRcbkAPmhd/ afCtPMYWaivIlsJKuRYNzLS6nJn624kNomFv7wIDAQABoD0wOwYJKoZIhvcNAQkO MS4wLDAqBgNVHREEIzAhgg9wa2kuaXJpc2dyaWQuZXOCDnd3dy5lZHVyb2FtLmVz MA0GCSqGSIb3DQEBBQUAA4IBAQDByabgU98c4xa8T64dzjBNwNw263vZNu5uRpHO SUUuZqkv42cBicUscukjC6QH3Z7UTjaXyw45SP8nxSESCZR3qy02wBlOxYiB+vwz l6MDtlxpfLhOnDq8PR7qVjFGK9qm8DW1xLIiHGEla/KVOKpBBc6T09QpkFhBwtbz scVkMLZ0p5bzuW9Uxa3/V+HllIYtqoGqJiwlnnH/qOfZeRfxef/eNejhsL1z5Slr kmg+SWsyblaqgQ+DC53wwcNCEL4RsL9EFMt+klmYMy+fCPCfTTu+h8frtplkTE0G ezlrLcXOPZKaCCRAG9alqEy2HWqeSXlDcwLFXCIljsXZPvEk -----END CERTIFICATE REQUEST-----

Aprobar | Denegar | Volver

DCV - Ejemplo de solicitud de certificado
Estado del DCV en la solicitud



ISC: Interfaz de Solicitud de Certificados
Javier Masa Marin @ RedIRIS

Datos sobre Certificado

Solicitante	**Javier Masa Marin**
Institucion	**rediris**
DN	**C=ES,O=RedIRIS,CN=pruebadcv.rediris.es**
SubjectAltName	**pki.irisgrid.es, www.eduroam.es**
Estado	**Pendiente de emisión**

Estado del Control de Validación de Dominios (DCV)

Dominio	Estado	Método DCV
pki.irisgrid.es	No validado	cname
pruebadcv.rediris.es	No validado	administrator@rediris.es
www.eduroam.es	No validado	http

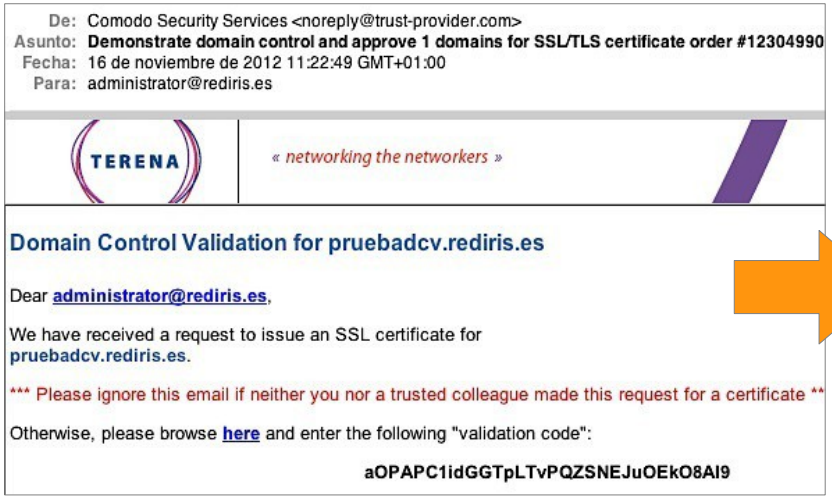
Reenviar DCV

Nota: Al reenviar DCV, se reenviarán los correos con el código de validación a la dirección de correo seleccionada en el momento de realizar la solicitud.

Para los dominios con validación mediante HTTP/CNAME se comprobará de nuevo que existe el fichero con la información adecuada para que COMODO pueda validarlo.

MD5: 9350CE346979601729CCA18EB5E7100C
SHA1: BED81F3B8090D0CD6DD718778799195E3C506AA3

DCV - Ejemplo de solicitud de certificado
Validación DCV - Mail


De: Comodo Security Services <noreply@trust-provider.com>
Asunto: **Demonstrate domain control and approve 1 domains for SSL/TLS certificate order #12304990**
Fecha: 16 de noviembre de 2012 11:22:49 GMT+01:00
Para: administrator@rediris.es

TERENA « networking the networkers »

Domain Control Validation for pruebadcv.rediris.es

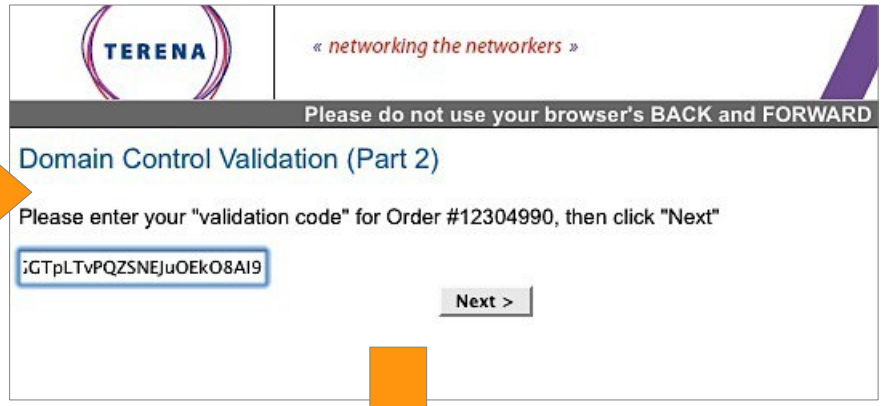
Dear **administrator@rediris.es**,

We have received a request to issue an SSL certificate for **pruebadcv.rediris.es**.

*** 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":

aOPAPC1idGGTpLTvPQZSNEJuOEkO8AI9


TERENA « networking the networkers »

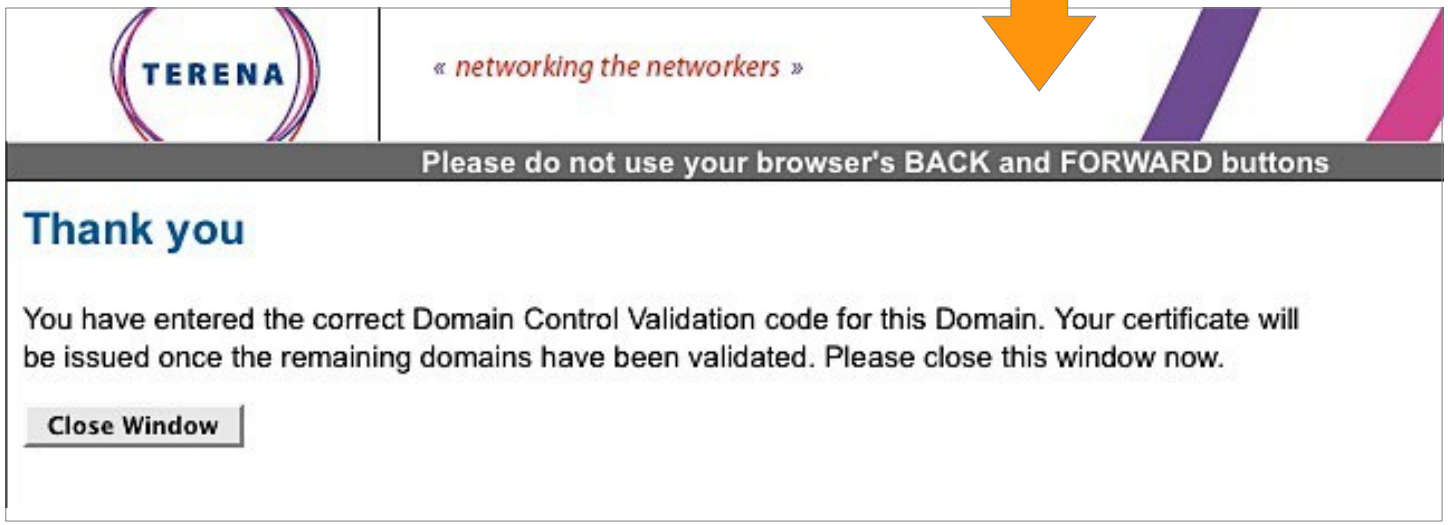
Please do not use your browser's BACK and FORWARD

Domain Control Validation (Part 2)

Please enter your "validation code" for Order #12304990, then click "Next"

;GTpLTvPQZSNEJuOEkO8AI9

Next >


TERENA « networking the networkers »

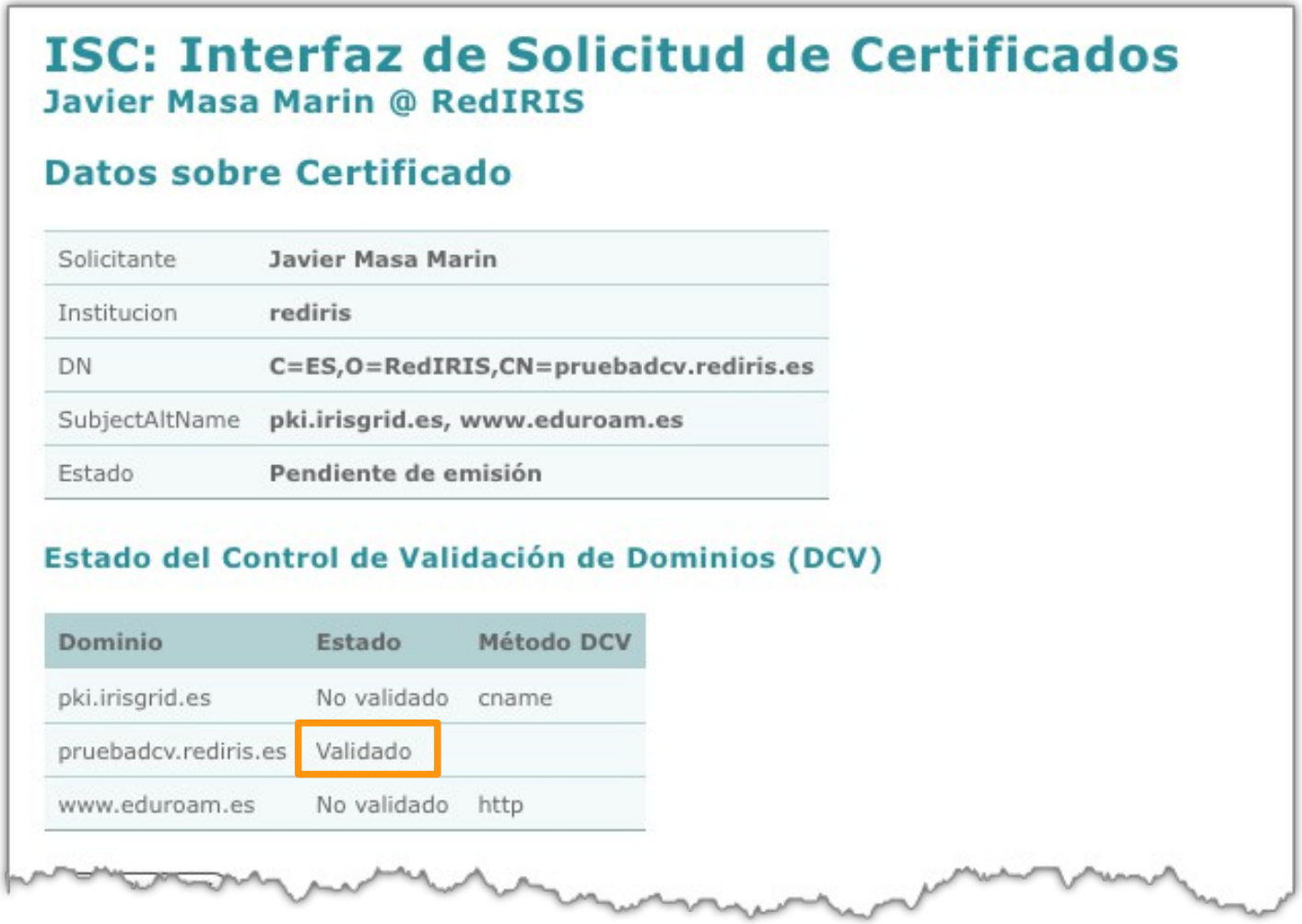
Please do not use your browser's BACK and FORWARD buttons

Thank you

You have entered the correct Domain Control Validation code for this Domain. Your certificate will be issued once the remaining domains have been validated. Please close this window now.

Close Window

DCV - Ejemplo de solicitud de certificado
Estado solicitud - DCV - Mail - OK



ISC: Interfaz de Solicitud de Certificados
Javier Masa Marin @ RedIRIS

Datos sobre Certificado

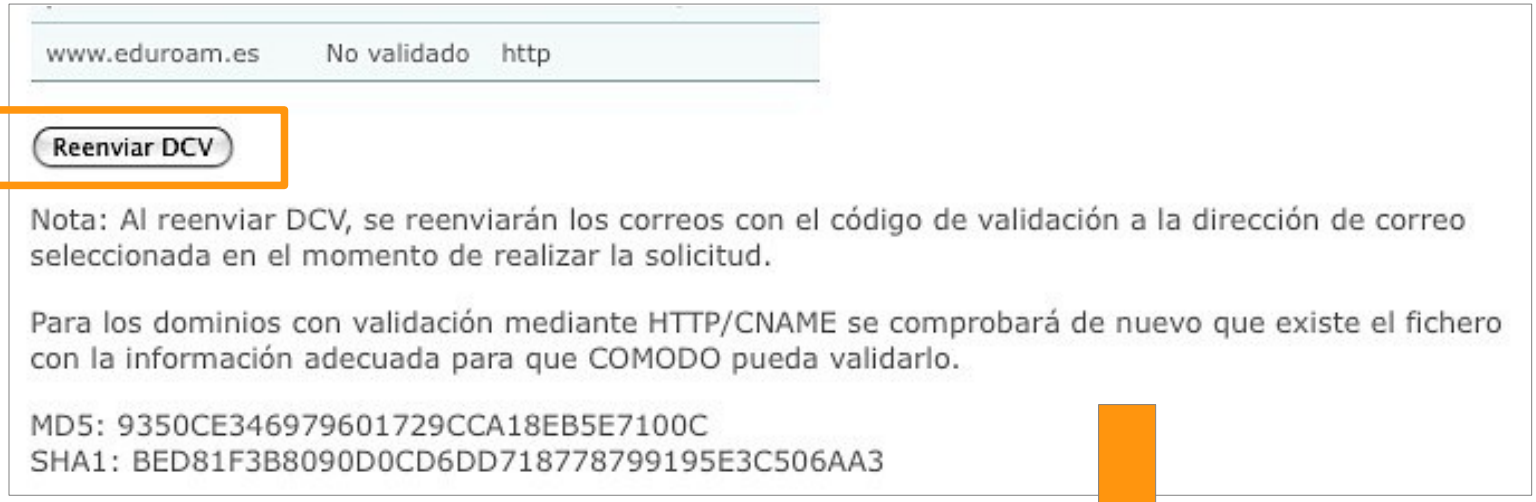
Solicitante	**Javier Masa Marin**
Institucion	**rediris**
DN	**C=ES,O=RedIRIS,CN=pruebadcv.rediris.es**
SubjectAltName	**pki.irisgrid.es, www.eduroam.es**
Estado	**Pendiente de emisión**

Estado del Control de Validación de Dominios (DCV)

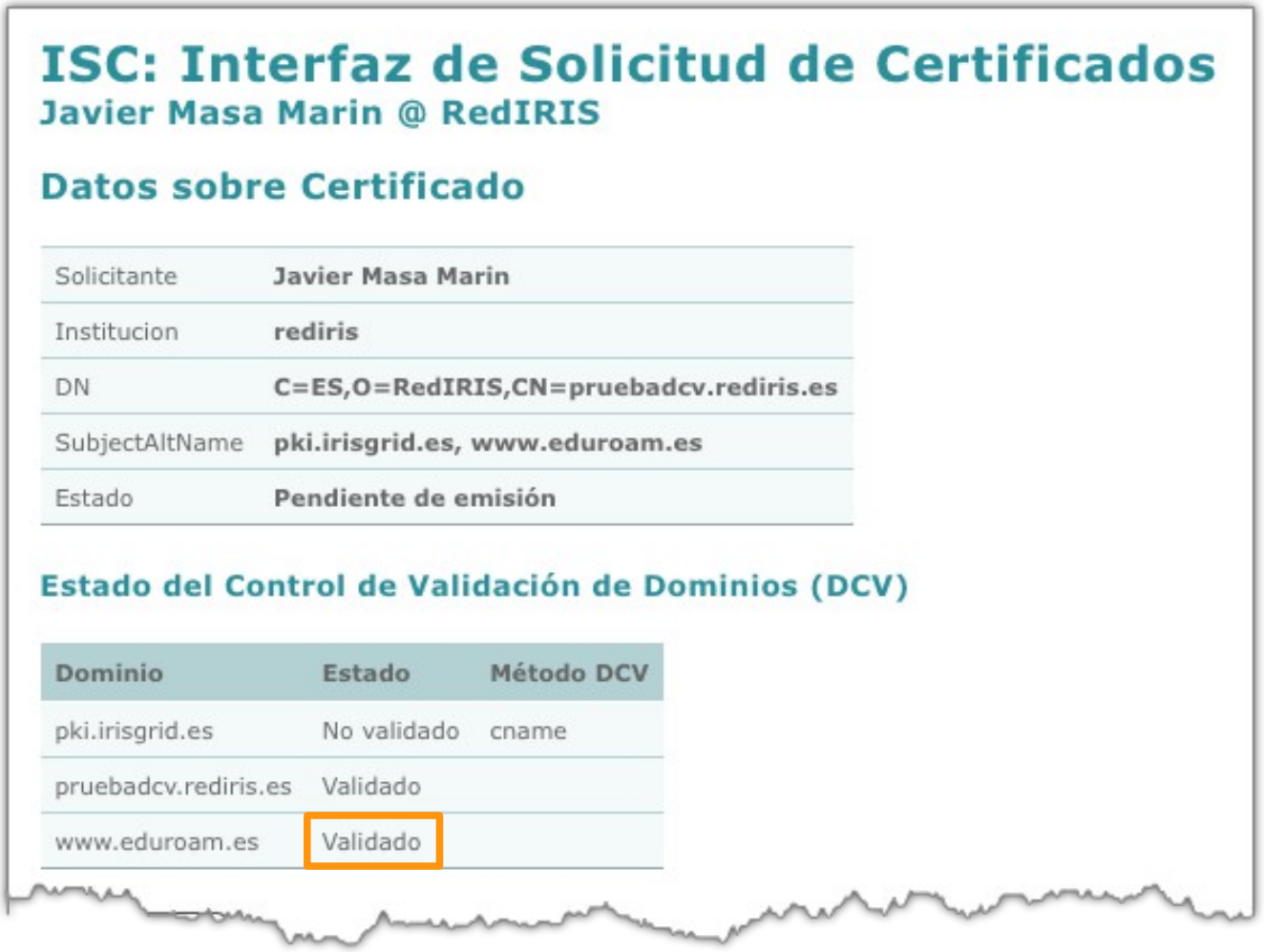
Dominio	Estado	Método DCV
pki.irisgrid.es	No validado	cname
pruebadcv.rediris.es	Validado	
www.eduroam.es	No validado	http

DCV - Ejemplo de solicitud de certificado
Validación DCV - HTTP

DCV - Ejemplo de solicitud de certificado
Reenvío DCV



DCV - Ejemplo de solicitud de certificado
Estado solicitud - DCV - HTTP - OK



ISC: Interfaz de Solicitud de Certificados
Javier Masa Marin @ RedIRIS

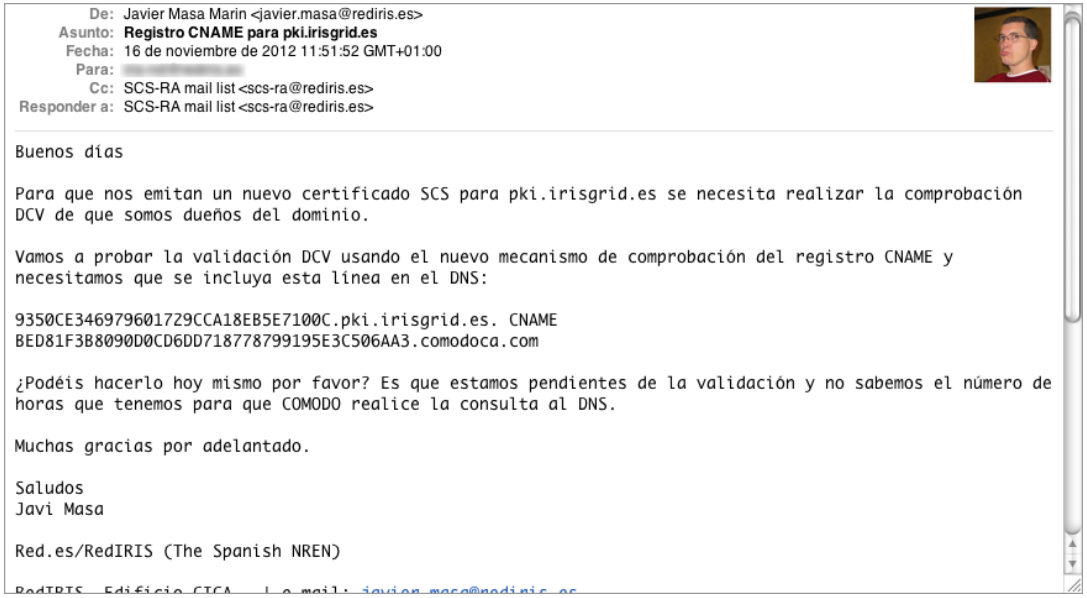
Datos sobre Certificado

Solicitante	**Javier Masa Marin**
Institucion	**rediris**
DN	**C=ES,O=RedIRIS,CN=pruebadcv.rediris.es**
SubjectAltName	**pki.irisgrid.es, www.eduroam.es**
Estado	**Pendiente de emisión**

Estado del Control de Validación de Dominios (DCV)

Dominio	Estado	Método DCV
pki.irisgrid.es	No validado	cname
pruebadcv.rediris.es	Validado	
www.eduroam.es	Validado	

DCV - Ejemplo de solicitud de certificado
Validación DCV - DNS/CNAME



De: Javier Masa Marin <javier.masa@rediris.es>
Asunto: **Registro CNAME para pki.irisgrid.es**
Fecha: 16 de noviembre de 2012 11:51:52 GMT+01:00
Para: [redacted]
Cc: SCS-RA mail list <scs-ra@rediris.es>
Responder a: SCS-RA mail list <scs-ra@rediris.es>

Buenos días

Para que nos emitan un nuevo certificado SCS para pki.irisgrid.es se necesita realizar la comprobación DCV de que somos dueños del dominio.

Vamos a probar la validación DCV usando el nuevo mecanismo de comprobación del registro CNAME y necesitamos que se incluya esta línea en el DNS:

9350CE346979601729CCA18EB5E7100C.pki.irisgrid.es. CNAME
BED81F3B8090D0CD6DD718778799195E3C506AA3.comodoca.com

¿Podéis hacerlo hoy mismo por favor? Es que estamos pendientes de la validación y no sabemos el número de horas que tenemos para que COMODO realice la consulta al DNS.

Muchas gracias por adelantado.

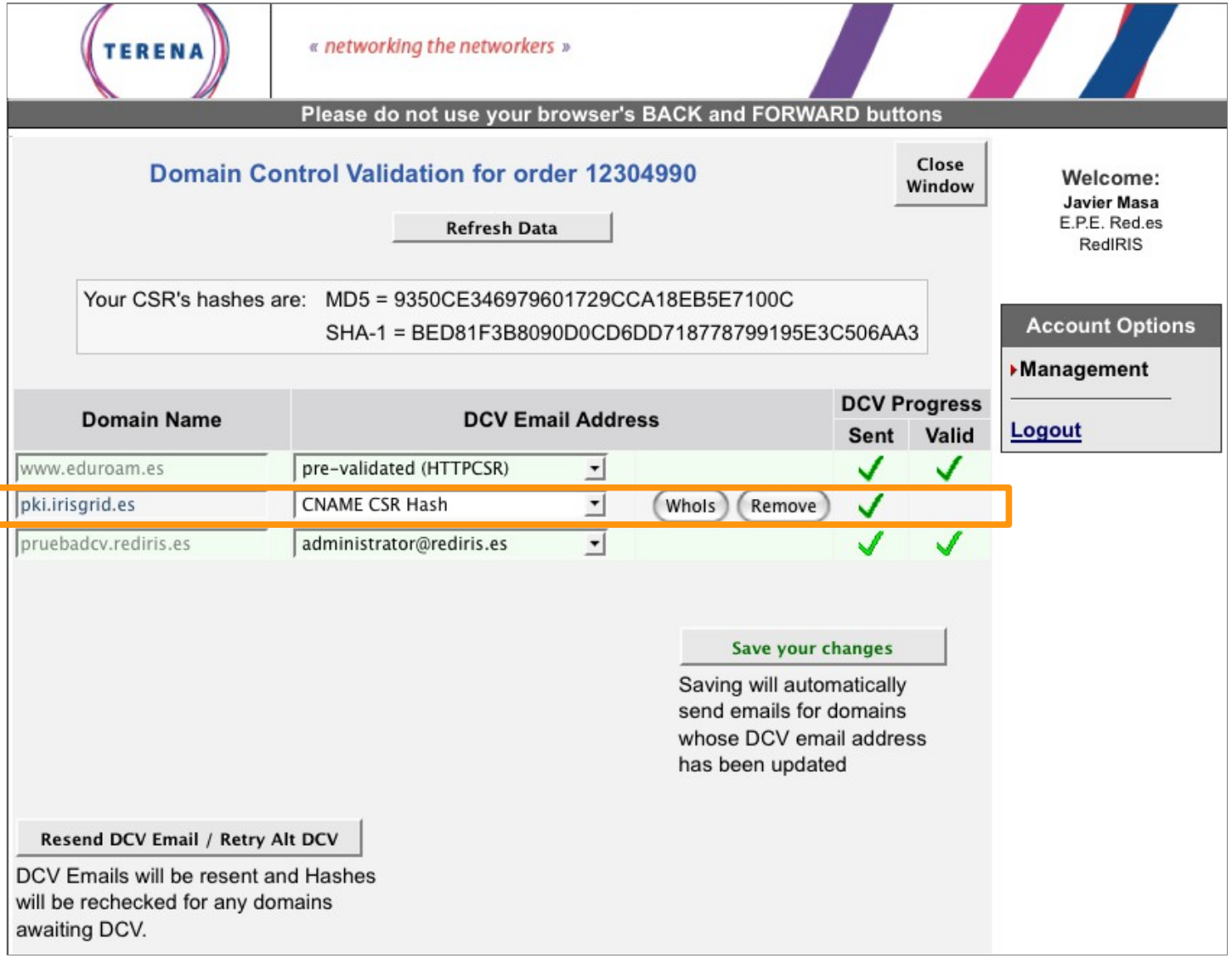
Saludos
Javi Masa

Red.es/RedIRIS (The Spanish NREN)

RedIRIS Edificio CICA | e-mail: javier.masa@rediris.es

DCV - Ejemplo de solicitud de certificado

Estado solicitud - DCV - DNS/CNAME - pendiente



DCV - Ejemplo de solicitud de certificado
Certificado emitido

DCV - conclusiones

- Emisión certificado
  - Comodo no emite el certificado hasta que todos los dominios de los FQDNs solicitados han sido validados
- Comprobación DCV
  - Comodo no inicia el proceso hasta que RedIRIS no valida la solicitud
  - Antes de esto el solicitante debe revisar
    - Que tiene acceso a la dirección de correo seleccionada
    - Que están correctos los ficheros relacionados con DCV-HTTP
    - Que el DNS tiene un CNAME correcto para el método DCV-DNS
  - Solicitud de reenvío/rechequeo de DCV
- Dominios
  - Los dominios deben estar registrados a nombre de la institución

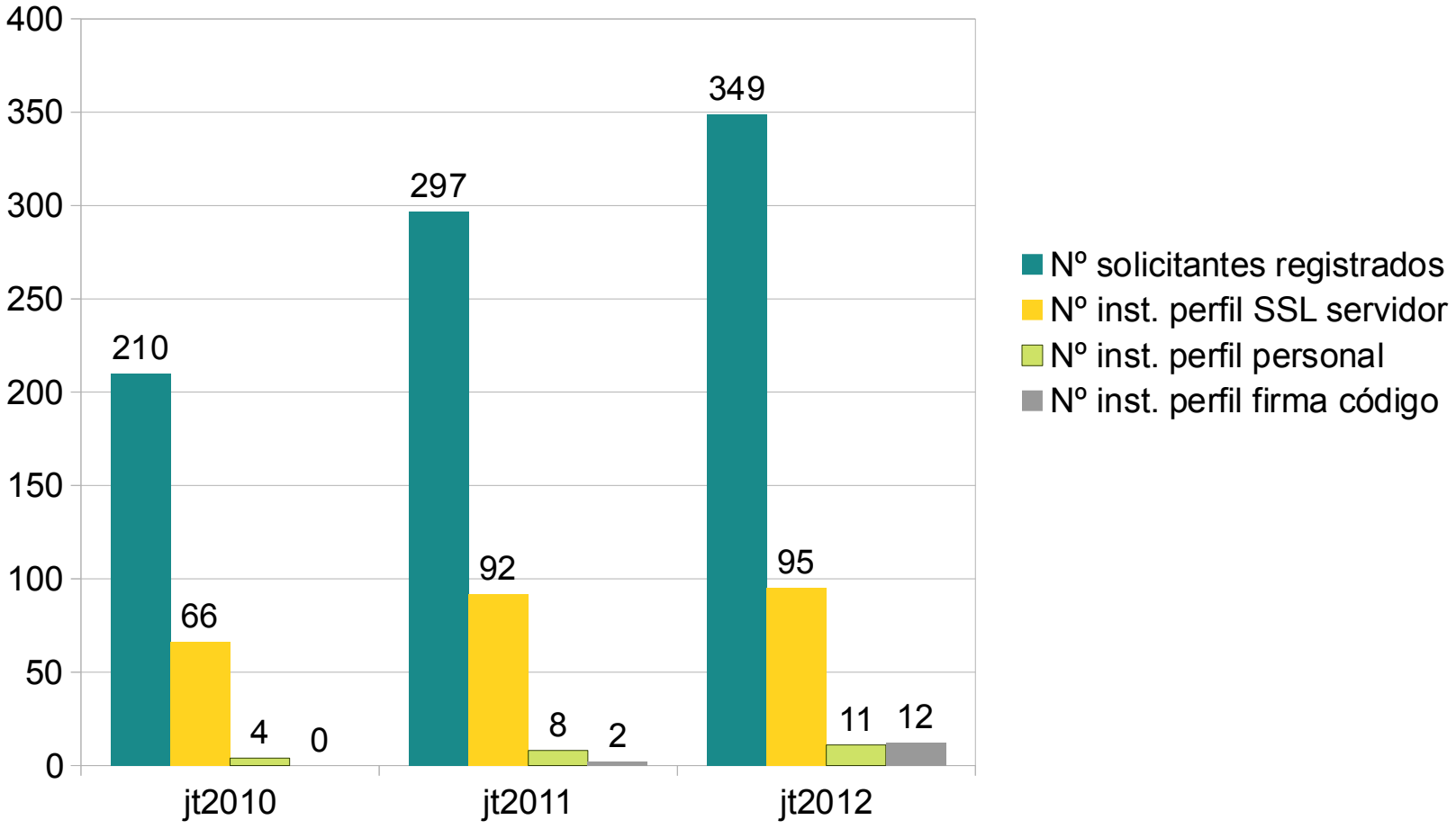
Índice de contenidos

SCP

- Caso de uso
  - Identificación web
  - Correo seguro
  - VPN
  - ¿Alguno lo usa para otras cosas?
- Interface de gestión SCP
  - Administradores
    - ¿Usamos los de SCS?
  - Grupos de usuario
    - ¿En base a atributos SIR: irisClassifCode?

Índice de contenidos

SCS: Estadísticas – evolución histórica



SCS - Estadísticas por perfiles

- SSL servidor
  - Instituciones: 95
  - Solicitantes registrados: 349
  - Dominios: 390

Certificados	SSL	Multi-domain	Wildcard	Certificados	Nombres certificados
Emitidos	3.279	2.037	14	5.330	21.554
Revocados	188	104	1	293	889
Expirados	148	47	0	195	745
Válidos	2.943	1.886	13	4.842	19.758

SCS - Estadísticas por perfiles

- Personal (SCP)
  - Instituciones: 11

    BSC, CICA, CTTC, INTA, IVIE, RedIRIS, UC3M, UDC, UPV, URL, USJC

Certificados	Número
Emitidos	277
Revocados	55
Expirados	6
Válidos	216

- Firma de código (SCC)
  - Instituciones: 12

    CSIC, CTTC, ICFO, RedIRIS, UAH, UDC, UM, UNILEON, UNIRIOJA, UPC, UPV, UV

Certificados	Número
Emitidos	13
Revocados	1
Expirados	0
Válidos	13

¡Muchas gracias!

Red IRIS

Más de 20 años al servicio de la investigación