



SCS

Servicio de certificados de RedIRIS

Javi Masa - javier.masa@rediris.es

Índice de contenidos

1 DCV

2 SCP



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMÍA
Y COMPETITIVIDAD

MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

red.es



Red IRIS

- **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)

- 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

- 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

- Ejemplo

- Certificado multidominio con **FQDN1** y **FQDN2**
- Supongamos que Comodo genera los hashes
MD5: 9350CE346979601729CCA18EB5E7100 y
SHA-1: BED81F3B8090D0CD6DD718778799195E3C506AA3
- Crear ficheros
 - `http://FQDN1/9350CE346979601729CCA18EB5E7100C.txt`
 - `http://FQDN2/9350CE346979601729CCA18EB5E7100C.txt`
- Contenido de cada uno de los 2 ficheros:
 - BED81F3B8090D0CD6DD718778799195E3C506AA3
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: BED81F3B8090D0CD6DD718778799195E3C506AA3
- Añadir al DNS
 - 9350CE346979601729CCA18EB5E7100C.**FQDN1**. CNAME
BED81F3B8090D0CD6DD718778799195E3C506AA3.comodoca.com
 - 9350CE346979601729CCA18EB5E7100C.**FQDN2**. CNAME
BED81F3B8090D0CD6DD718778799195E3C506AA3.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



◀ [Servicios](#) ▶ ◀ [SCS](#) ▶ ◀ [Beta](#) ▶ ◀ [Oper](#)

ISC: Interfaz de Solicitud de Certificados

Javier Masa Marin @ RedIRIS

Introduzca la CSR que desea comprobar.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICwDCCAagCAQAwPjELMAkGA1UEBhMCRVMxEDAoBgNVBAoTB1JlZE1SSVMxHTAb
BgNVBAMTFHBydWViYURDVj5yZWVpY2VzLmVzMIIBIjANBgkqhkiG9w0BAQEFAAOc
AQ8AMIIBCgKCAQEAA7xRii7wYVQpo7JnnxDgVfhM8rf4A0YgN7fCWo+celjR5lwtW
/j66lyopWb/gpjguEXRvJBvLA8LWWIdbBFYYf3IUln4j/omllHukdPyGuiwX/MG0
MW7LAjYC+3DOOt a0b76nVOB+cI/cNunjRYbQDP22UbX7A9ruty/zuiMkw/okG9YE
6qePoTvUaktN3b1gbL9zOH35pqxRF6cH/ppYAMVyuZJm44L5ex0J75LKbp2BmnJj
ip+na5NsPBtcsQULmsIUPUu2vHZYOjXzmYy6+w0aIz15LQGIizgnVBRcbkAPmhd/
afCtPMYwaivIlsJKuRYNzLS6nJn624kNomFv7wIDAQABOD0wOwYJKoZIhvcNAQkO
MS4wLDAqBgNVHREEIzAhgg9wa2kuaXJpc2dyaWQuZXOCdnd3dy5lZHVyY2FtLmVz
MA0GCSqGSIb3DQEBBQUAA4IBAQDByabgU98c4xa8T64dzjBNwNw263vZNu5uRphO
SUUuZqkv42cBicUscukjC6QH3Z7UTjaXyw45SP8nxSESCZR3qy02wB10xYiB+vwz
l6MDt1xpflhOnDq8PR7qVjFGK9qm8DW1xLiHGElA/KVOKpBBc6T09QpkFhBwtbz
scVkmLZ0p5bzuW9Uxa3/V+H1lIYtqoGqJiwlNnH/qOfZerfxef/eNejhsL1z5Slr
kmg+SWsyblagqQ+DC53wvcNCEL4RsL9EFMt+klmYMy+fCPCfTTu+h8frtPlkTE0G
ezlrLcXOPZKaCCRAG9alqEy2HWqeSXlDcwLFXCiljsXZPvEk
-----END CERTIFICATE REQUEST-----
```

Sobre RedIRIS

La Red

Servicios

Proyectos

Actividades

Difusión

Google™ Custom Search

- SCSBeta SSL
 - Comprobar CSR**
 - Solicitar SSL
 - Multi-domain SSL
 - Wildcard
 - Revocar Certificado
 - Gestionar Certs
- SCSBeta Personal
 - Solicitar certificado
 - Revocar certificado
 - Gestionar certificado

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-----

MIIcWdCCAagCAQAwPjELMAkGA1UEBhMCRVMxEDAOBgNVBAoTB1JIZEISSVMxHTAb

BgNVBAMTFHBydWViYURDVi5yZWVpcmlzLmVzMIIBIjANBgkqhkiG9w0BAQEFAAO

AQ8AMIIBCgKCAQEAA7xRIi7wYVQpo7JnnxDgVfhM8rf4A0YgN7fCW0+celjR5lwtW

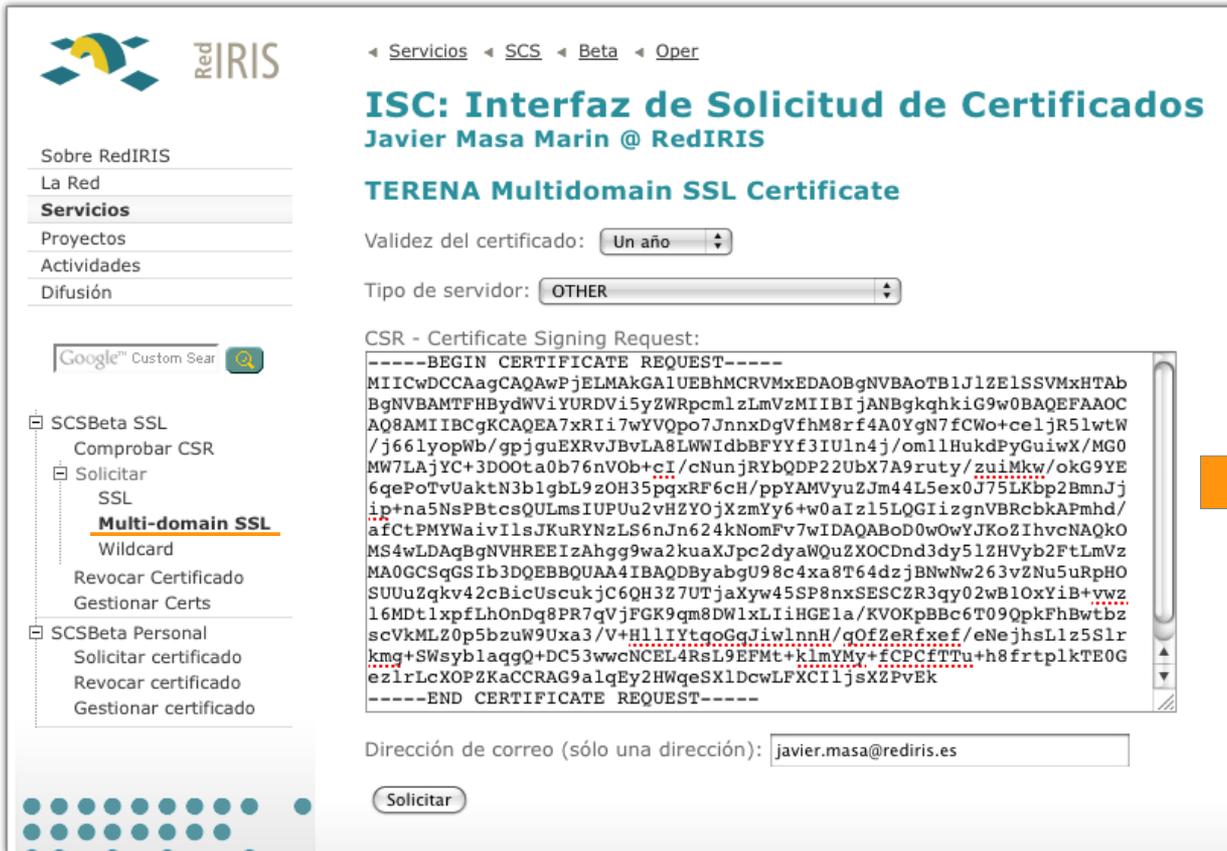
/j66lyopWb/gpjguFXRvJBvLA8IWWIdbBFYf3IUln4j/om1HukdPyGuiwX/MG0

MW7LAiYc3P.../zui...okG9YE



DCV - Ejemplo de solicitud de certificado

Volcado de la CSR en el ISC



RedIRIS

◀ Servicios ▶ SCS ▶ Beta ▶ Oper

ISC: Interfaz de Solicitud de Certificados

Javier Masa Marin @ RedIRIS

TERENA Multidomain SSL Certificate

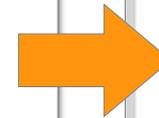
Validez del certificado:

Tipo de servidor:

CSR - Certificate Signing Request:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICwDCCAagCAQAwPjELMAkGA1UEBhMCRVVMxEDAoBgNVBAoTB1J1ZE1SSVMxHTAb
BgNVBAMTFHBydWViYURDVj5yZWpRcmplZmVzMIIBIjANBgkqhkiG9w0BAQEFAAOCC
AQ8AMIIBCgKCAQEAA7xRii7wYVQpo7JnnxDgVfhM8rf4A0YgN7fCWoceljr5lwtW
/j66lyopWb/gpjguEXRvJBvLA8LWwIdbBFYYf3IUln4j/omllHukdPyGuiwX/MG0
MW7LAjYC+3D00ta0b76nVOB+cI/cNunjRYbQDP22UbX7A9ruty/zuiMkw/okG9YE
6qePoTvUaktN3b1gbL9zOH35pqxRF6cH/ppYAMVyuZJm44L5ex0J75LKbp2BmnJj
ip+na5NsPbtcsQULmsIUPUu2vHZYOjXzmYy6+w0aIz15LQGIzgnVBRcbkAPmhd/
aFctPMYwaivIlsJKuRYNzLS6nJn624kNomFv7wIDAQABoD0wOwYJKoZIhvcNAQkO
MS4wLDAqBgNVHREIzAhgg9wa2kuaXJpc2dyaWQuZmVzXOCdnd3dy5lZHVyb2FtLmVz
MA0GCSqGSIb3DQEBBQUAA4IBAQDByabgU98c4xa8T64dzjBNwNw263vZnu5uRphO
SUUuZgkv42cBicUscukjC6QH3Z7UTjaXyW45SP8nxSESCZR3qy02wB10xYiB+vwz
16MDt1xpflhOnDq8PR7qvjFGK9qm8DWlxLiHGElA/KVOKpBBc6T09QpkFhBwtbz
scVkMLZ0p5bzuW9Uxa3/V+H11YtqGgJiwlNnH/qOfZrFxf/eNejsL1z5S1r
kmg+SWsyblagqQ+DC53wncNEL4RsL9EFMt+klmYMy+fCPCITTu+h8frtPlkTE0G
ezlrLcXOPZKaCCRAG9alqEy2HWqeSX1DcwLFXCI1jsXZPvEk
-----END CERTIFICATE REQUEST-----
```

Dirección de correo (sólo una dirección):



RedIRIS

ISSUE - Example of Multidomain SSL Certificate

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

-----BEGIN PRIVATE KEY-----

-----END PRIVATE KEY-----

-----BEGIN X.509 CERTIFICATE REQUEST-----

-----END X.509 CERTIFICATE REQUEST-----

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

-----BEGIN PRIVATE KEY-----

-----END PRIVATE KEY-----

-----BEGIN X.509 CERTIFICATE REQUEST-----

-----END X.509 CERTIFICATE REQUEST-----

DCV - Ejemplo de solicitud de certificado

Descripción DCV - HTTP

contactar con los responsables de su organización que solucionen el problema. Para más información, consulte 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 cadena ".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 un comando para este procedimiento.

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

Selección del método DCV

Por favor, seleccione e continuación el método de validación de dominio para cada uno de los dominios que desea solicitar.

pruebadcv.rediris.es

- admin@pruebadcv.rediris.es
- administrador@pruebadcv.rediris.es
- hostmaster@pruebadcv.rediris.es
- postmaster@pruebadcv.rediris.es
- webmaster@pruebadcv.rediris.es
- admin@rediris.es
- administrador@rediris.es
- hostmaster@rediris.es
- postmaster@rediris.es
- webmaster@rediris.es
- HTTP CSR Hash
- CNAME CSR Hash

pki.irisgrid.es

- admin@pki.irisgrid.es
- administrador@pki.irisgrid.es
- hostmaster@pki.irisgrid.es
- postmaster@pki.irisgrid.es
- webmaster@pki.irisgrid.es
- admin@irisgrid.es
- administrador@irisgrid.es
- hostmaster@irisgrid.es
- postmaster@irisgrid.es
- webmaster@irisgrid.es
- HTTP CSR Hash
- CNAME CSR Hash

www.eduroam.es

- admin@www.eduroam.es
- administrador@www.eduroam.es
- hostmaster@www.eduroam.es
- postmaster@www.eduroam.es
- webmaster@www.eduroam.es
- admin@eduroam.es
- administrador@eduroam.es
- hostmaster@eduroam.es
- postmaster@eduroam.es
- webmaster@eduroam.es
- HTTP CSR Hash
- CNAME CSR Hash

Aceptación de las condiciones del Servicio de Certificados de Servidor

Antes de enviar la solicitud de certificado es necesario que acepte las condiciones del servicio según se indican en:

- [TERENA Server & Codesigning CA Certificate Practice Statement](#)
- [Documento de condiciones de Uso](#)

Acepto las condiciones

DCV - Ejemplo de solicitud de certificado

Envío de la solicitud



The screenshot displays the RedIRIS ISC (Interfaz de Solicitud de Certificados) web application. The top navigation bar includes links for [Servicios](#), [SCS](#), [Beta](#), and [Oper](#). The main heading reads "ISC: Interfaz de Solicitud de Certificados" by "Javier Masa Marin @ RedIRIS". A prominent orange-bordered box contains the message: "Su solicitud ha sido aceptada y se encuentra pendiente de ser aprobada por RedIRIS". On the left, a sidebar menu lists "Sobre RedIRIS", "La Red", "Servicios" (highlighted), "Proyectos", "Actividades", and "Difusión". Below the menu is a "Google Custom Search" box. At the bottom left, a tree view shows "SCSBeta SSL" expanded to include "Comprobar CSR", "Solicitar Certificado", "Revocar Certificado", and "Certs".

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-----

```
MIICwDCCAagCAQAwPjELMAkGA1UEBhMCRVMxEDAoBgNVBAoTB1JlZElSSVMxHTAB
BgNVBAMTFHBydWViYURDV5yZWVpcmlzLmVzMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEAE7xRIi7wYVQpo7JnnxDgVfM8rf4A0Ygn7fCWo+celjR51wtW
/j66lyopWb/gpjpguEXRvJBvLA8LWwIdbBFYF3IUln4j/om1lHukdPyGuiwX/MG0
MW7LAjYC+3DO0ta0b76nVOB+cI/cNunjRYbQDP22UbX7A9ruty/zuiMkw/okG9YE
6qePoTvUaktN3blgbL9zOH35pgxRF6cH/ppYAMVyuZJm44L5ex0J75LKbp2BmnJj
ip+na5NsPBtcsQULmsIUPUu2vH2YOjXzmYy6+w0aIz15LQGIizgnVBRcbkAPmhd/
afCtPMYwaivIlsJKuRYnzLS6nJn624kNomFv7wIDAQABOD0wOwYJKoZIhvcNAQkO
MS4wLDAqBgNVHREEIzAhgg9wa2kuaXJpc2dyaWQuZXOCdnd3dy51ZHVyY2FtLmVz
MA0GCSqGSIb3DQEBBQUAA4IBAQBByabgU98c4xa8T64dzjBNwNw263vZNu5uRphO
SUUuZqkv42cBicUscukjC6QH3Z7UTjaXyw45SP8nxSESCZR3qy02wB1OxYiB+vwz
16MDtlxpfLhOnDq8PR7qVjFGK9qm8DWlxLIiHGE1a/KVOKpBBc6T09QpkFhBwtbz
scVkmLZ0p5bzuW9Uxa3/V+H1lIYtqoGqJiwlennH/qOfZeRfxf/eNejhsLlZ5S1r
kmg+SWSyblaqqQ+DC53wvcNCEL4RsL9EFMt+klmYMy+fCPCfTTu+h8frtjplkTE0G
ezlrLcXOPZKaCCRAG9alqEy2HWqeSX1DcwLFXCI1jsXZPvEk
```

-----END CERTIFICATE REQUEST-----

Aprobar

Denegar

Volver



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMÍA
Y COMPETITIVIDAD

MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

red.es



RedIRIS

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



« networking the networkers »

Domain Control Validation for pruebadcv.rediris.es

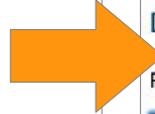
Dear administrator@rediris.es,

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":

aOPAPC1idGGTpLTvPQZSNEJuOEK08AI9



« 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"

Next >



« 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

Reenvío DCV

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



◀ [Servicios](#) ▶ [SCS](#) ▶ [Beta](#) ▶ [Oper](#) ▶ [Manage](#)

ISC: Interfaz de Solicitud de Certificados

Javier Masa Marin @ RedIRIS

Sobre RedIRIS

La Red

Servicios

Proyectos

Actividades

Difusión

Google™ Custom Search



El reenvío de los códigos de validación (DCV) se ha realizado correctamente.

Para los dominios seleccionados para validación mediante mail, recibirá un correo en la dirección indicada con un nuevo código de validación.

Para los dominios seleccionados para validación mediante HTTP/CNAME, se han vuelto a comprobar los ficheros correspondientes.

Para volver a ver el estado del certificado pulse [aquí](#)

SCSBe SSL



GOBIERNO DE ESPAÑA

MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

red.es



RedIRIS

jt2012 - SCS - 27/11/2012

25 . 37

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

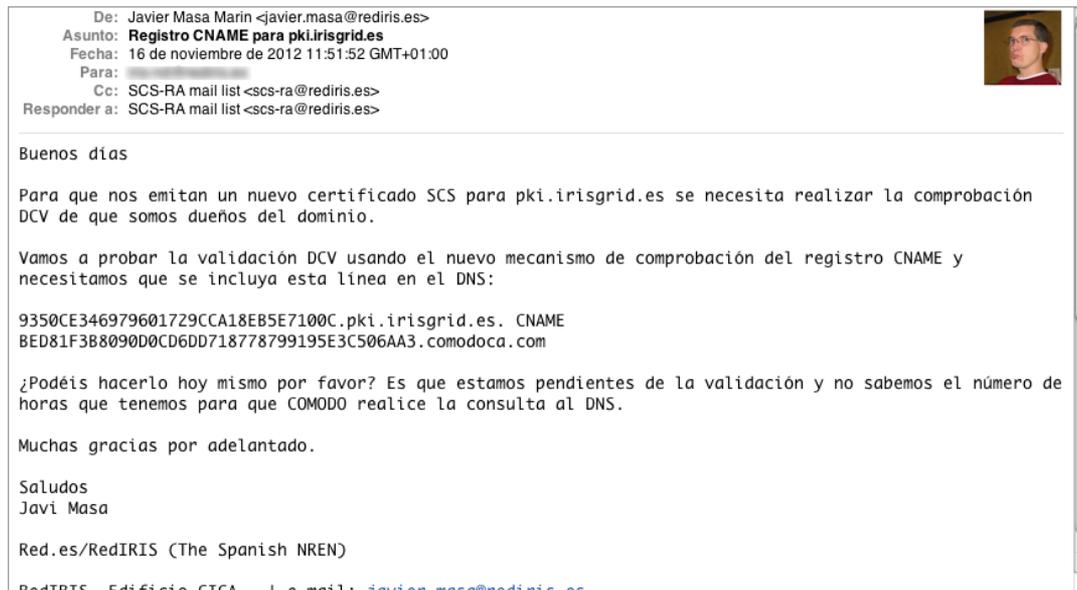
Estado del Control de Validación de Dominios (DCV)

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



```
Default  
1  
woto~ > dig any 9350CE346979601729CCA18EB5E7100C.pki.irisgrid.es +short  
BED81F3B8090D0CD6DD718778799195E3C506AA3.comodoca.com.  
woto~ >  
woto~ >  
woto~ >  
woto~ >
```

DCV - Ejemplo de solicitud de certificado

Estado solicitud - DCV - DNS/CNAME - pendiente



« networking the networkers »

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

Domain Control Validation for order 12304990 Close Window

Refresh Data

Welcome:
Javier Masa
E.P.E. Red.es
RedIRIS

Your CSR's hashes are: MD5 = 9350CE346979601729CCA18EB5E7100C
SHA-1 = BED81F3B8090D0CD6DD718778799195E3C506AA3

Account Options
Management
[Logout](#)

Domain Name	DCV Email Address	DCV Progress	
		Sent	Valid
www.eduroam.es	pre-validated (HTTPCSR)	✓	✓
pki.irisgrid.es	CNAME CSR Hash	✓	✓
pruebadcv.rediris.es	administrator@rediris.es	✓	✓

Save your changes

Saving will automatically send emails for domains whose DCV email address has been updated

Resend DCV Email / Retry Alt DCV

DCV Emails will be resent and Hashes will be rechecked for any domains awaiting DCV.

DCV - Ejemplo de solicitud de certificado

Certificado emitido

◀ Servicios ◀ SCS ◀ Beta ◀ Oper ◀ Manage

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	pruebadcv.rediris.es, pki.irisgrid.es, www.eduroam.es
Estado	Emitido
Válido desde	2012-11-16 01:00
Válido hasta	2013-11-17 00:59

PEM

```
-----BEGIN CERTIFICATE-----
MIIEiDCCA3CgAwIBAgIQMOYvsWvWAwgiate9wKSVr
MQswCQYDVQQGEwJOTDEPMA0GA1UEChMGMGVVSRU5BM
U1NMIENBMB4XDTEyMTExNjAwMDAwMFoXDTEzMTExNjAw
BhMCRVMxEDA0BGNVBAoTB1J1ZE1SSVMxHTAbBgNVB
cm1zLmVzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AM
7JnnxDgVfhM8rf4A0YgN7fCWo+celjR5ltW/j66L
WIdbBFYf3IUln4j/om1lHukdPyGuiwX/MG0MW7LA
NunjRYbQDP22UbX7A9ruty/zuiMkw/okG9YE6qePd
F6cH/ppYAMVyu2Jm44L5ex0J75Lkbp2BmnJjip+na
OjXzmYy6+w0aIz15LQGIizgnVBRcbkAPmhd/afCtF
24kNomFv7wIDAQABo4IBiDCCAYQwHwYDVR0jBBgwF
6pdJue0wHQYDVR0O0BBYEFHYSwe6S5W9ZbJ6A151cV
AwIFoDAMBGNVHRMBAF8EAJAAMB0GA1UdJQQWMBQGC
AjAYBgNVHSAEETAPMA0GCysGAQQBsjEBAGIdMDoGA1UdHwQz
dHA6Ly9jcmwudGNzLnRlcmVuYS5vcmcvVEVSRU5BU1NMQ0EuY3J
BwEBBGFvYwAlBggrBgEFBQcwAoYpaHR0cDovL2Nydc50Y3MudGVy
ZyZy9U
-----END CERTIFICATE-----
```

De: Comodo Security Services <noreply_support@comodo.com>
Asunto: **ORDER #12304990 - Your TERENA Multi-Domain SSL Certificate**
Fecha: 16 de noviembre de 2012 12:08:09 GMT+01:00
Para: Javier Masa Marin <javier.masa@rediris.es>
▶ 1 archivo adjunto, 4,9 KB [Guardar](#) [Vista Rápida](#)



« networking the networkers »

Your TERENA Multi-Domain SSL Certificate is attached!

Dear javier.masa@rediris.es,

Thank you for placing your order. The necessary background checks have been successfully completed and we are pleased to announce that your TERENA Multi-Domain SSL Certificate has been issued.

We strongly recommend that you [click here for instructions](#) to ensure that your certificate is installed and your webserver is configured correctly.

Attached to this email you should find a .zip file containing:

- Your TERENA Multi-Domain SSL Certificate - 12304990.crt
- Your Apache "bundle" file - 12304990.ca-bundle

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

1 DCV

2 SCP



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMÍA
Y COMPETITIVIDAD

MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

red.es



Red IRIS

- 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

- 1 DCV
- 2 SCP
- 3 Estadísticas**



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMÍA
Y COMPETITIVIDAD

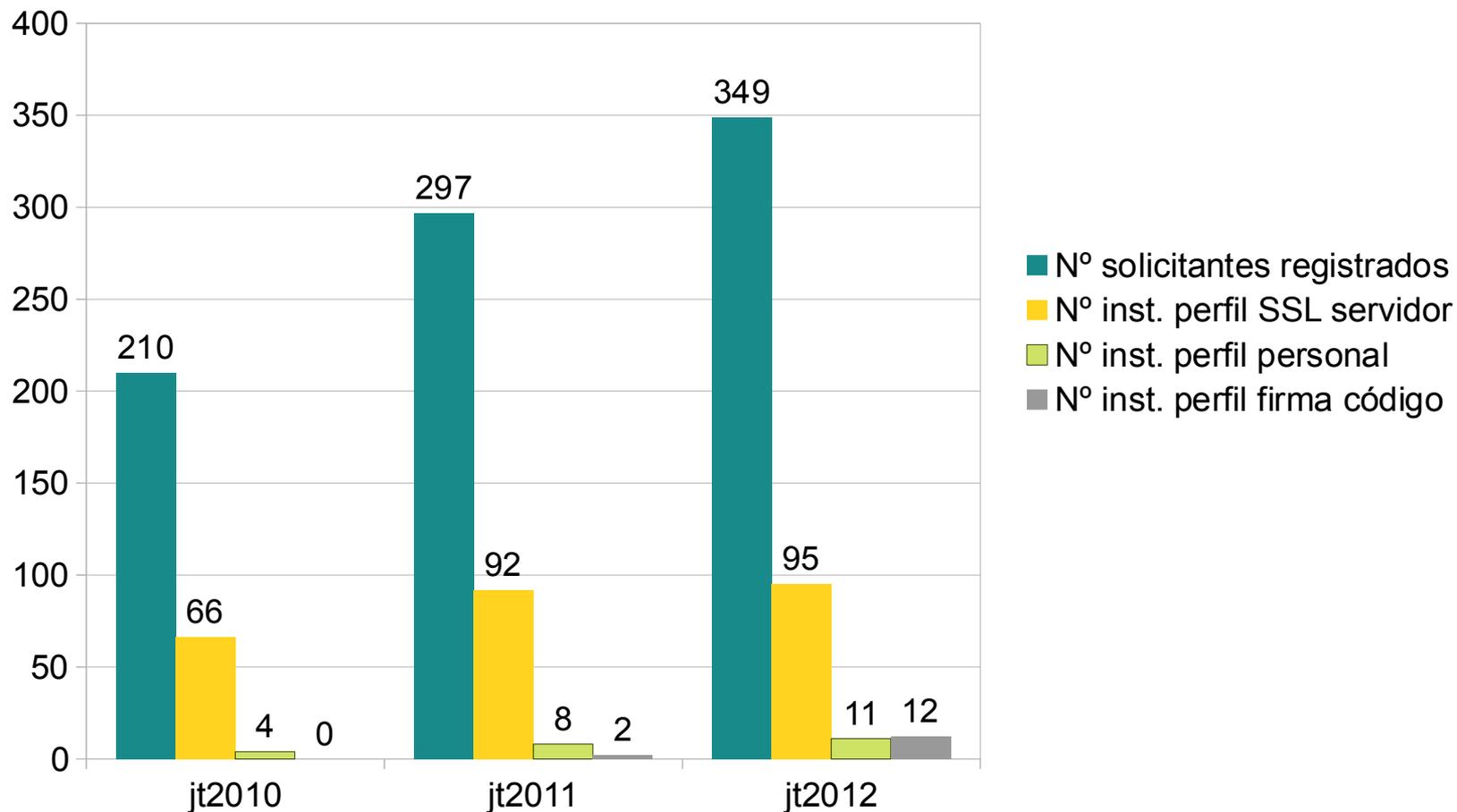
MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

red.es



Red IRIS

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

• Firma de código (SCC)

- Instituciones: 12

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

Certificados	Número
Emitidos	277
Revocados	55
Expirados	6
Válidos	216

Certificados	Número
Emitidos	13
Revocados	1
Expirados	0
Válidos	13

¡Muchas gracias!



Red IRIS

Más de 20 años al servicio de la investigación



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ECONOMÍA
Y COMPETITIVIDAD

MINISTERIO
DE INDUSTRIA, ENERGÍA
Y TURISMO

red.es



Red IRIS

jt2012 - SCS - 27/11/2012

37 . 37