

# Revisión de TCS

El nuevo servicio de certificados digitales  
de RedIRIS

Javi Masa - [javier.masa@rediris.es](mailto:javier.masa@rediris.es)

# Bienvenida

---

- Disculpas por la no asistencia presencial
- Material adicional
  - TCS:
    - <http://www.rediris.es/tcs/>
  - Presentación:
    - <http://www.rediris.es/tcs/coord/gt2015/>
  - Alta en el servicio
    - <http://www.rediris.es/tcs/alta/>

# Índice de contenidos

---

- 1** Introducción
- 2 Evolución histórica del servicio
- 3 Perfiles disponibles
- 4 CAs
- 5 Alta. Requisitos
- 6 Modelo de servicio y acceso
- 7 Operación del servicio
- 8 Próximas acciones



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE ECONOMÍA  
Y COMPETITIVIDAD

MINISTERIO  
DE INDUSTRIA, ENERGÍA  
Y TURISMO

red.es



Red IRIS

# TCS: Introducción

---

- **Nuevo servicio de certificados digitales**

- RedIRIS presta el nuevo servicio gracias al acuerdo entre GÉANT y DigiCert tras un concurso público
- No es una continuación del anterior servicio SCS
  - Los certificados emitidos por Comodo no se reemitirán con DigiCert  
(Al pasar de GlobalSign a Comodo, se emitieron con las CAs de Comodo y bajo petición, todos los certificados válidos con GlobalSign usando las antiguas CSRs)

- **Cambio de siglas del nuevo servicio**

- De SCS (Servicio de Certificados de Servidor) a TCS, siguiendo el nombre dado por GÉANT (TCS - Trusted Certificate Service)
- Nombre más coherente con los perfiles ofrecidos

# TCS: Introducción

## Mejoras del nuevo servicio - I

---

- Nuevos perfiles
  - Firma de documentos
  - Grid (personal, servidor, robot)
- Mejoras en las condiciones del proveedor
  - Económicas
  - Perfiles: EV, wildcard
  - Validaciones (¿2 años?)
  - Tiempos de firmado
    - OV < 20min, EV < 60min.
  - Gestión de revocaciones una vez finalizado el contrato
  - Validaciones sin necesidad de reuniones cara a cara (Grid)
    - Acceso federado
  - Acceso: Portal, API

# TCS: Introducción

## Mejoras del nuevo servicio - II

---

- **Simplificación de la burocracia**
  - 1 único documento de condiciones de uso por institución
- **Autogestión del servicio en cada institución**
  - Mayor control en cada institución
    - Altas y validaciones
  - Uso del portal de DigiCert
  - Uso del portal ISC de RedIRIS
  - Posibilidad de desarrollos propios (API)

# Índice de contenidos

---

- 1 Introducción
- 2 Evolución histórica del servicio**
- 3 Perfiles disponibles
- 4 CAs
- 5 Alta. Requisitos
- 6 Modelo de servicio y acceso
- 7 Operación del servicio
- 8 Próximas acciones



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE ECONOMÍA  
Y COMPETITIVIDAD

MINISTERIO  
DE INDUSTRIA, ENERGÍA  
Y TURISMO

red.es



Red IRIS

# Evolución del servicio de certificados digitales

De 2006 a 2015

	2006 - GlobalSign	2010 - Comodo	2015 - DigiCert
Perfiles de certificados	<ul style="list-style-type: none"><li>• SSL servidor</li></ul>	<ul style="list-style-type: none"><li>• SSL servidor</li><li>• Personal</li><li>• Firma de código</li></ul>	<ul style="list-style-type: none"><li>• SSL servidor</li><li>• Personal</li><li>• Firma de código</li><li>• Firma de documentos</li><li>• e-Ciencia (Grid)</li></ul>
Doc. requerida	<ul style="list-style-type: none"><li>• 1 CUSO / certificado (especificar FQDNs)</li><li>• Uso Fax</li></ul>	<ul style="list-style-type: none"><li>• 1 CUSO / solicitante (especificar dominios)</li><li>• 1 CUSO / cert. código</li></ul>	<ul style="list-style-type: none"><li>• 1 CUSO / institución</li></ul>
Acceso al servicio	<ul style="list-style-type: none"><li>• Portal GlobalSign</li></ul>	<ul style="list-style-type: none"><li>• ISC/RedIRIS (SIR)</li></ul>	<ul style="list-style-type: none"><li>• Portal DigiCert</li><li>• ISC/RedIRIS (SIR)</li><li>• API</li></ul>
Roles	<ul style="list-style-type: none"><li>• Solicitante</li></ul>	<ul style="list-style-type: none"><li>• Admin ~ Solicitante</li><li>• Usuario final</li></ul>	<ul style="list-style-type: none"><li>• Administrador</li><li>• Usuario solicitante</li><li>• Usuario final</li></ul>
Instituciones participantes	<ul style="list-style-type: none"><li>• 89</li></ul>	<ul style="list-style-type: none"><li>• 115</li></ul>	<ul style="list-style-type: none"><li>• 222 solicitudes</li><li>• 27 en producción</li></ul>



# Índice de contenidos

---

- 1 Introducción
- 2 Evolución histórica del servicio
- 3 Perfiles disponibles**
- 4 CAs
- 5 Alta. Requisitos
- 6 Modelo de servicio y acceso
- 7 Operación del servicio
- 8 Próximas acciones



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE ECONOMÍA  
Y COMPETITIVIDAD

MINISTERIO  
DE INDUSTRIA, ENERGÍA  
Y TURISMO

red.es



Red IRIS

# Nuevo servicio: TCS

## Perfiles de certificados

---

- **SSL certificates**

- EV SSL Plus
- EV Multi-Domain
- SSL Plus
- Unified Communications (SSL Multi-Domain 25 SANs)
- Wildcard Plus (con SAN automático + SAN adicionales)

- **Code Signing**

- Code Signing
- EV Code Signing

- **Document Signing**

- Document Signing - Organization (2000)
- Document Signing - Organization (5000)

# Nuevo servicio: TCS

## Perfiles de certificados

---

- Client Certificates

- Email Security Plus (key scrow and recovery)
- Digital Signature Plus
- Premium

- Grid Certificates

- Grid Host SSL
- Grid Host SSL Unified Communications (25 SANs)
- Grid Premium
- Grid Robot Name
- Grid Robot Email
- Grid Robot FQDN

# Índice de contenidos

---

- 1 Introducción
- 2 Evolución histórica del servicio
- 3 Perfiles disponibles
- 4 CAs**
- 5 Alta. Requisitos
- 6 Modelo de servicio y acceso
- 7 Operación del servicio
- 8 Próximas acciones



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE ECONOMÍA  
Y COMPETITIVIDAD

MINISTERIO  
DE INDUSTRIA, ENERGÍA  
Y TURISMO

red.es



Red IRIS

# Nuevo servicio: TCS

## CAs

---

- CAs raíz de DigiCert

- <https://www.digicert.com/digicert-root-certificates.htm>

- CAs de TCS

- <https://www.terena.org/activities/tcs/repository-g3/>
- Raíz: DigiCert Assured ID Root CA
  - TCS SSL CA 3
  - TCS eScience SSL CA 3
  - TCS Personal CA 3
  - TCS eScience Personal CA 3
  - TCS Code-Signing CA 3
- Raíz: DigiCert High Assurance EV Root CA
  - TCS SSL High Assurance CA 3

# Nuevo servicio: TCS

CAs y DN's de los certificados emitidos bajo cada una

---

- TCS Server CA

- CA: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA SSL CA 3
- DN: /C=ES/[ST=<ST>]/L=<L>/O=<O>/[OU=<OU>]/CN=fqdn

- TCS eScience Server CA

- CA: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA eScience SSL CA 3
- DN: /DC=org/DC=terena/DC=tcs/C=ES/[ST=<ST>]/L=<L>/O=<O>/[OU=<OU>]/CN=fqdn

- TCS Code Signing CA

- CA: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA Code Signing CA 3
- DN: /DC=org/DC=terena/DC=tcs/C=ES/[ST=<ST>]/L=<L>/O=<O>/[OU=<OU>]/CN=name

# Nuevo servicio: TCS

CAs y DNs de los certificados emitidos bajo cada una

---

## • TCS Personal CA

- CA: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA Personal CA 3
- DN: /C=ES/[ST=<ST>]/L=<L>/O=<O>/[OU=<OU>/]CN=name/[email]

## • TCS eScience Personal CA

- CA: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA eScience Personal CA 3
- DN: /DC=org/DC=terena/DC=tcs/C=ES/O=<O>/[OU=<OU>/]CN=name + unique and persistent ID

## • TCS Document Signer CA

- CA: C=NL, ST=Noord-Holland, L=Amsterdam, O=TERENA, CN=TERENA Document Signing CA 3
- DN: /C=ES/[ST=<ST>/]L=<L>/O=<O>/[OU=<OU>/]CN=name/[email]

# Índice de contenidos

---

- 1 Introducción
- 2 Evolución histórica del servicio
- 3 Perfiles disponibles
- 4 CAs
- 5 Alta. Requisitos**
- 6 Modelo de servicio y acceso
- 7 Operación del servicio
- 8 Próximas acciones



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE ECONOMÍA  
Y COMPETITIVIDAD

MINISTERIO  
DE INDUSTRIA, ENERGÍA  
Y TURISMO

red.es



Red IRIS



# TCS: Requisitos para el alta

---

- **Instituciones afiliadas a RedIRIS**
  - No empresas con departamentos I+D+i con afiliación temporal
  - Los centros afiliados accederán desde sus instituciones
- **Elección de un administrador principal**
- **Firma de un único acuerdo de usuario institucional**
  - <http://www.rediris.es/tcs/doc/cuso/tcs-acuerdo-usuario-v3-rev14.doc>
  - Y envío a RedIRIS firmado digitalmente por email.
    - Estamos trabajando en un sistema para facilitar el envío de los CUSOs y su validación sin necesidad de firma (mediante autenticación SIR)
- **Alta opcional en SIR**
  - Para algunos perfiles (Client certificates, Grid premium, Grid robots)
  - Servicios de valor añadido (ISC)

# TCS: Requisitos para el alta Acuerdo de usuario

- Complimentar correctamente el documento

- <PER>, <INSTITUCIÓN>, <NOMBRE-ADMINISTRADOR>, <EMAIL-PERSONAL>, <INSTITUCIÓN>

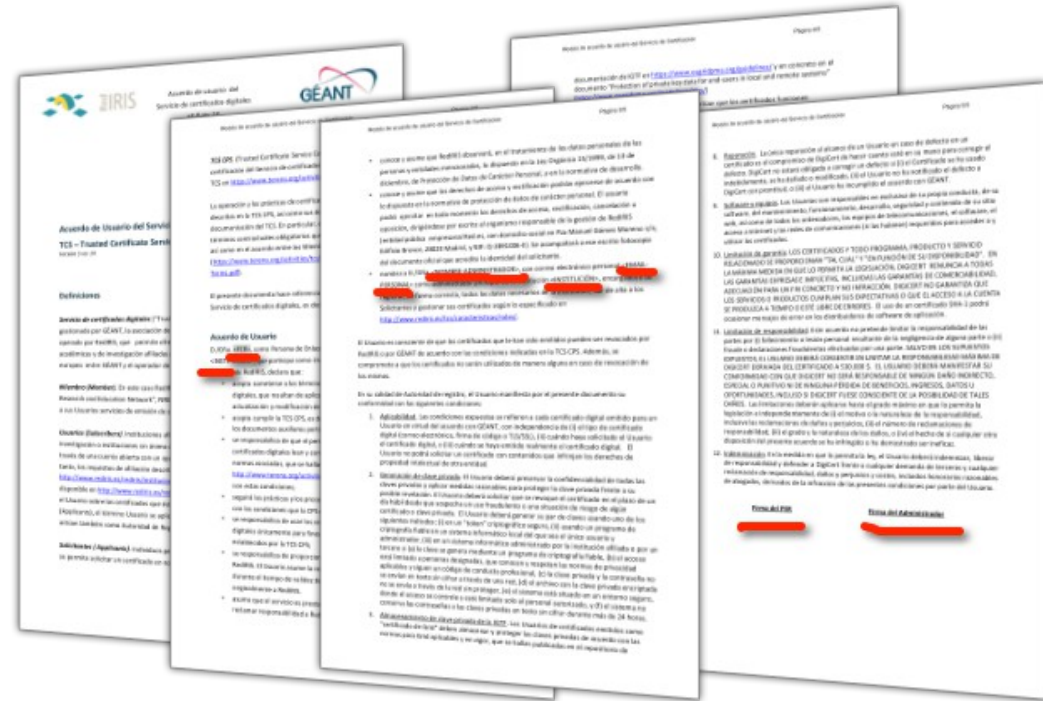
- Exportarlo a PDF

- Firmarlo digitalmente

- PER
- Administrador

- Envío a RedIRIS

- Email
- (Correo postal)



# Índice de contenidos

---

- 1 Introducción
- 2 Evolución histórica del servicio
- 3 Perfiles disponibles
- 4 CAs
- 5 Alta. Requisitos
- 6 Modelo de servicio y acceso**
- 7 Operación del servicio
- 8 Próximas acciones



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE ECONOMÍA  
Y COMPETITIVIDAD

MINISTERIO  
DE INDUSTRIA, ENERGÍA  
Y TURISMO

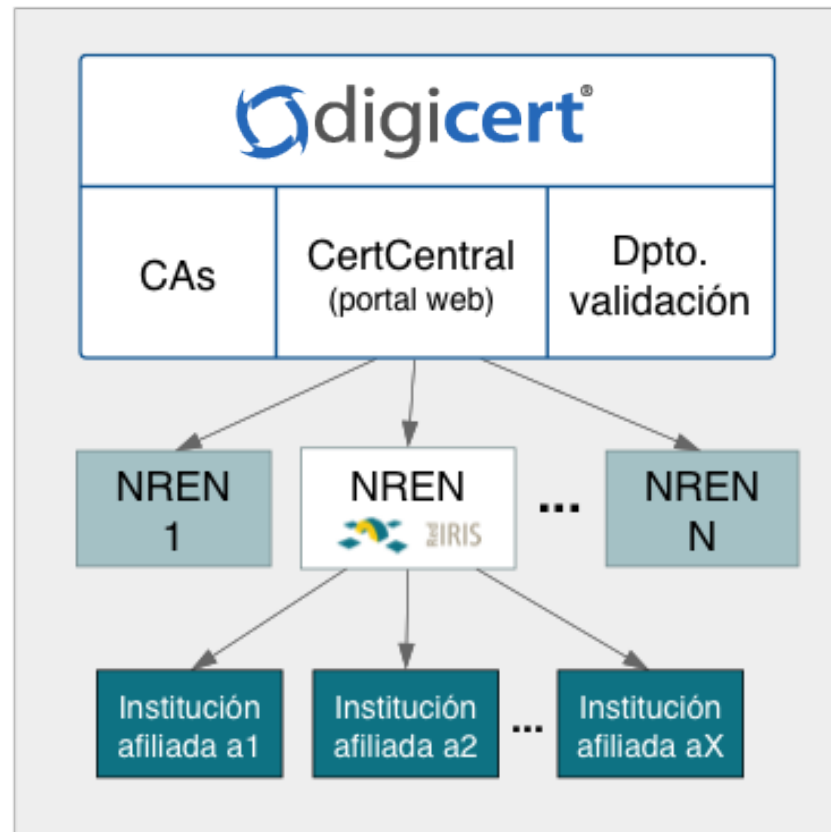
red.es



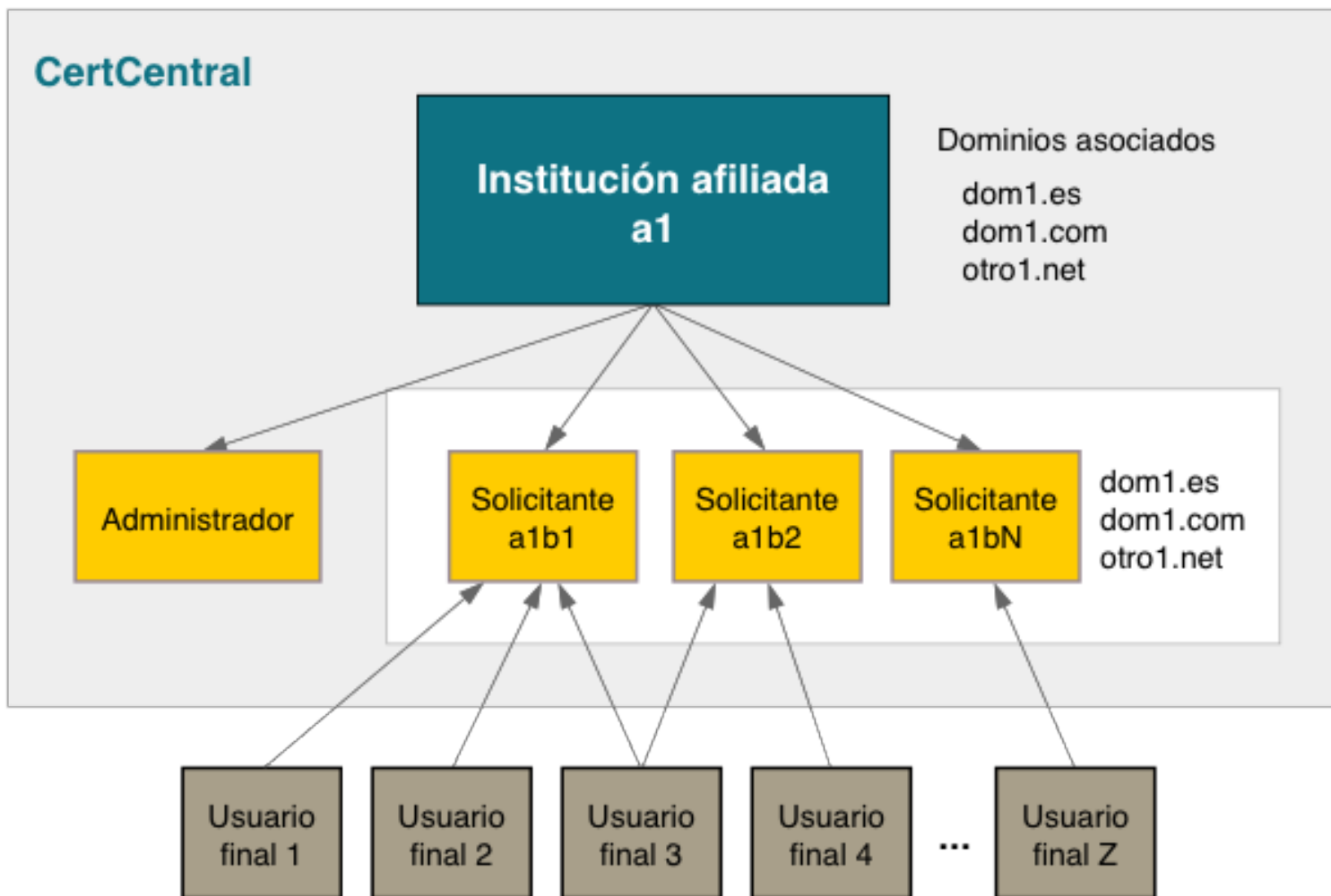
Red IRIS

# TCS: Modelo de servicio

- TCS CAs de DigiCert
- CertCentral
  - DigiCert proporciona una zona de trabajo para cada NREN participante
  - Cada NREN divide esa zona en partes para sus instituciones afiliadas (**divisiones**)
- Dpto. Validación
  - Encargado de verificar datos de instituciones y dominos.



# Modelo de servicio: TCS con CertCentral



- Tareas del administrador - I

- **Registros y altas**

- Edición de la ficha de su institución (división)
  - Logo, descripción, preferencias
- Alta de organización
  - Nombre legal, Nombre comercial, Teléfono, ...
  - Contacto de validación
- Alta de los dominios de su institución
  - Deben estar registrados, en los registros de dominio correspondiente, a nombre de la institución
- Elección de los perfiles a usar bajo cada dominio
- Alta/baja de otros administradores
- Alta/baja de los usuarios solicitantes de su institución

- **Tareas del administrador - II**

- **Validaciones**

- Gestionar las validaciones de
  - Organización/perfiles asociados
  - Dominios
- Aprobar/denegar todas y cada una de las las solicitudes de certificado de los solicitantes de su institución

- **Formación y asesoramiento**

- A administradores y usuarios solicitantes

- **Control**

- De acuerdo con los textos legales almacenados en el repositorio de TCS
  - <https://www.terena.org/activities/tcs/repository-g3/>

- Tareas del usuario solicitante

- **Gestión de solicitudes**

- Recepcionar las solicitudes de los usuarios finales
- Comprobar que la solicitud es correcta según los controles impuestos por la institución
- Volcar las solicitudes a CertCentral
- Enviar el certificado, una vez emitido, al usuario final
- Contactar con el administrador si hay algún problema con la emisión y avisar al usuario final del problema

- **Hacer un correcto uso del servicio**

- De acuerdo con los textos legales almacenados en el repositorio de TCS
  - <https://www.terena.org/activities/tcs/repository-g3/>



- **Tareas del usuario final**

- **Contacto inicial con un usuario solicitante**

- Para informar de que desea un certificado

- **Gestión de solicitudes**

- Generar una clave privada y una CSR
- Almacenar la clave en lugar seguro
- Enviar la CSR al usuario soliciante
- Recibir el certificado una vez emitido o
- Recibir explicación del motivo de la no emisión del certificado

- **Hacer un correcto uso del servicio**

- De acuerdo con los textos legales almacenados en el repositorio de TCS
  - <https://www.terena.org/activities/tcs/repository-g3/>

# Modelo de servicio: TCS con CertCentral

## Inconvenientes encontrados

---

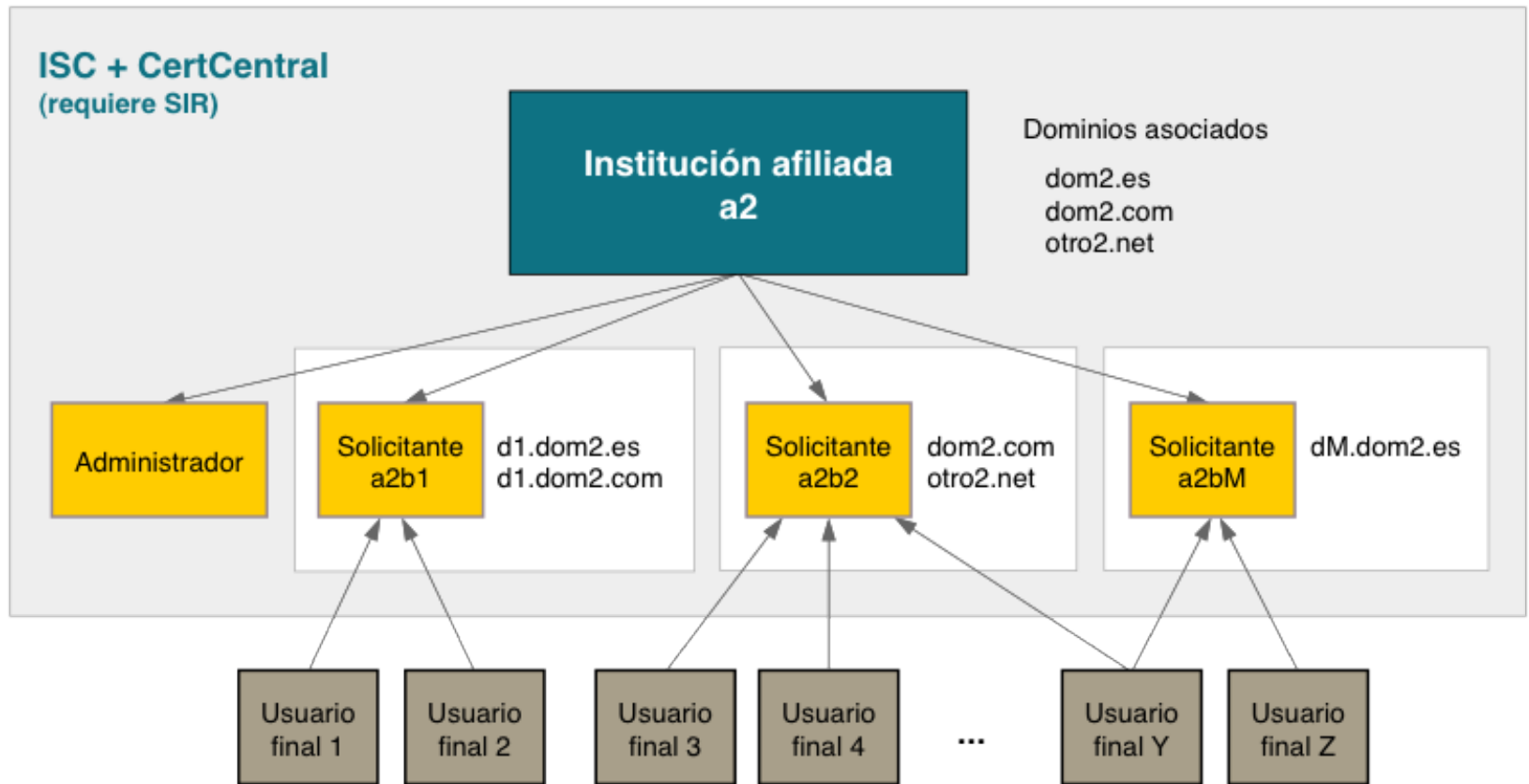
- Inconvenientes encontrados

- Todos los usuarios solicitantes pueden pedir certificados para todos los dominios habilitados para su institución
- El administrador tiene que comprobar, una a una, cada solicitud, para ver si el solicitante (o usuario final) tiene permiso para pedir certificados para esos dominios
- No permite la gestión de múltiples solicitudes de certificados

- Propuesta de RedIRIS

- Herramientas de valor añadido para facilitar el trabajo a los administradores y demás usuarios
  - ISC (Interfaz del Servicio de Certificados)
    - No pretende reemplazar CertCentral, sólo complementarlo

# Modelo de servicio: TCS con ISC + CertCentral



# Modelo de servicio: + API

## API de servicios de DigiCert

---

- Claves de acceso por usuarios (API Key)
  - Cada usuario puede obtener una clave para usar la API
  - Permitirá desarrollos propios en cada institución
- Documentación de la API
  - <https://www.digicert.com/services/v2/documentation/>

# Índice de contenidos

---

- 1 Introducción
- 2 Evolución histórica del servicio
- 3 Perfiles disponibles
- 4 CAs
- 5 Alta. Requisitos
- 6 Modelo de servicio y acceso
- 7 Operación del servicio**
- 8 Próximas acciones



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE ECONOMÍA  
Y COMPETITIVIDAD

MINISTERIO  
DE INDUSTRIA, ENERGÍA  
Y TURISMO

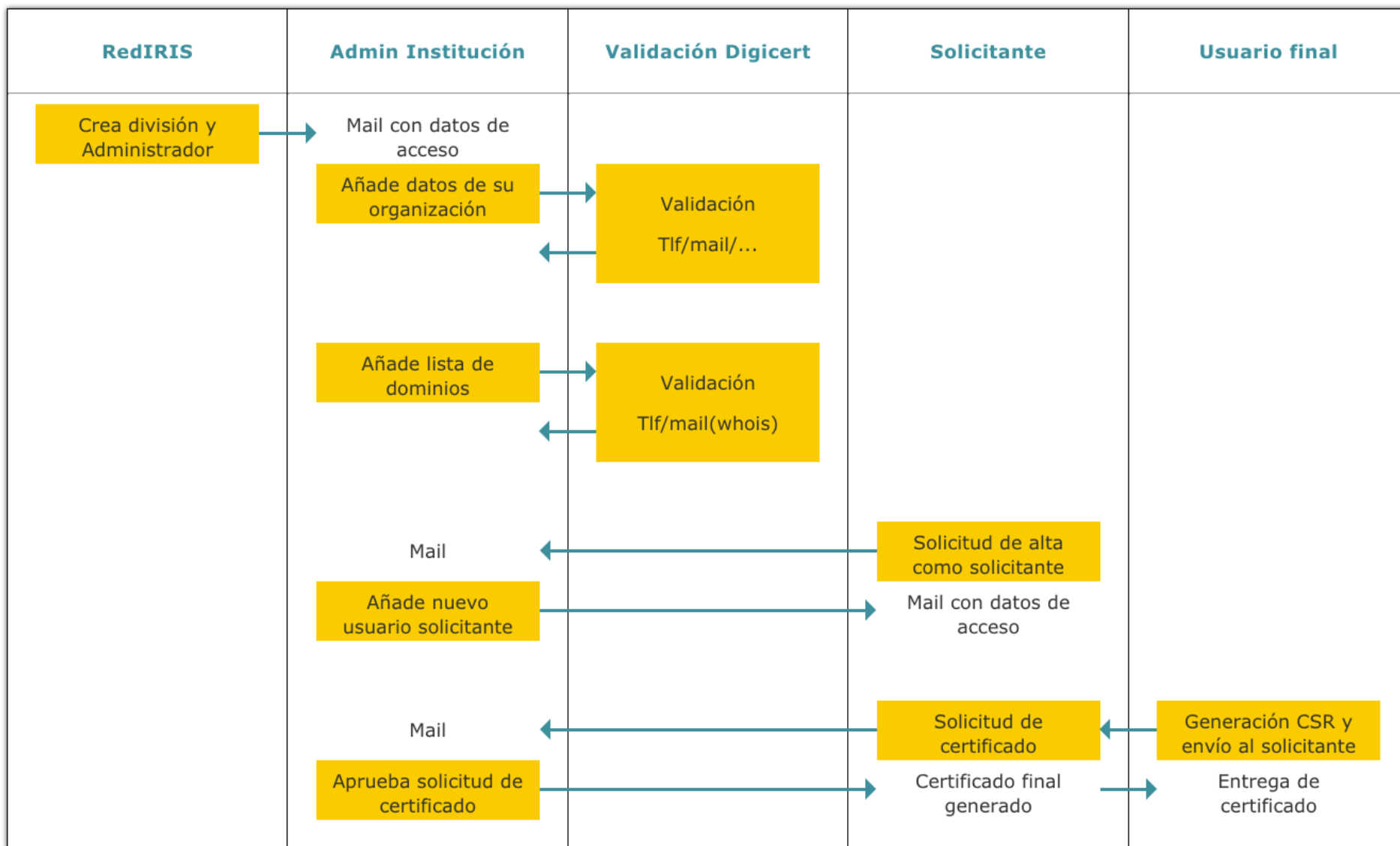
red.es



Red IRIS

# TCS: Operación del servicio

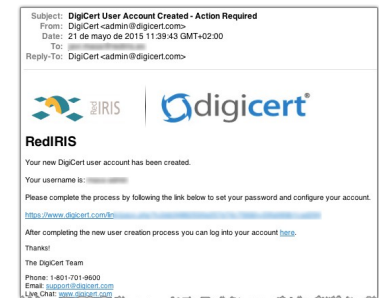
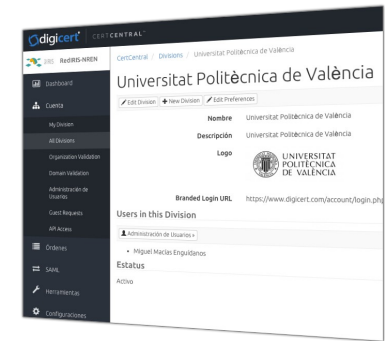
## Flujograma de operación



# CertCentral: Alta de institución y administrador

## Flujograma de operación

- La institución solicita el alta
  - Nombra el Administrador
  - Firma el acuerdo de usuario digitalmente
  - Lo envía a RedIRIS por email
- RedIRIS crea la división
  - Tras comprobar que la documentación es correcta crea la división en CertCentral
- Registro del administrador
  - Recibe un correo de DigiCert
  - Accede a CertCentral para registrarse en su división

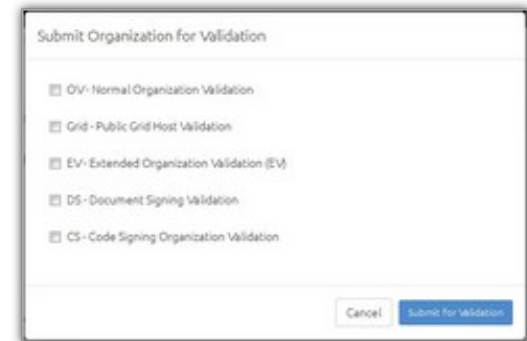
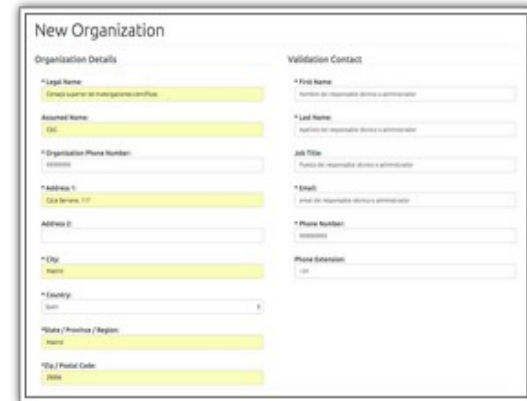


# CertCentral: Alta de organización

## Flujograma de operación

### • Añadir organización

- La organización debe contener el nombre legal de la institución
  - Excepciones:  
Caracteres nacionales/Grid
  - Importante: datos del contacto de validación
- Asignar perfiles (OV, **EV**, Grid, DS, CS)
- Validar la organización
  - Para los perfiles de certificados elegidos



### • Más info

- <http://www.rediris.es/tcs/doc/certcentral/administrador/cuenta/organizacion/>



# CertCentral: Alta de dominios para la organización

## Flujograma de operación

- Añadir dominios

- Esperar validación DCV de DigiCert
  - Mail de [admin@digicert.com](mailto:admin@digicert.com) a [admin@](mailto:admin@), [administrator@](mailto:administrator@), [webmaster@](mailto:webmaster@), [hostmaster@](mailto:hostmaster@), [postmaster@#domain#](mailto:postmaster@#domain#)

Division:

Organización	Nombre de Dominio	Fecha Agregada	Verificado p
Fundacio Institut de Ciencies Fotoniques	icfo.cat	2015-06-02 11:53 AM	EV, OV
Fundacio Institut de Ciencies Fotoniques	icfo.net	2015-06-02 11:53 AM	OV, EV
Fundacio Institut de Ciencies Fotoniques	icfo.eu	2015-06-02 11:53 AM	EV, OV
Fundacio Institut de Ciencies Fotoniques	icfo.es	2015-06-02 11:52 AM	EV, OV



- Una vez validada la organización y un dominio, todos los solicitantes de la división podrán solicitar certificados para ese dominio

# CertCentral: Gestión de usuarios (admin y solicitante)

## Flujograma de operación

- Administración de usuarios
  - Y asignación de roles

The image shows a screenshot of the CertCentral user management interface. On the left, there is a table titled 'Administración de Usuarios' with columns for Nombre, Nombre de Usuario, Dirección Electrónica, Roles, and Division. The user 'Javier Masa Marín' with the username 'masa-admin' is highlighted with a red circle. A red arrow points from this user to a detailed view on the right. The detailed view shows the user's profile, including their name, email, phone number, title, and roles. The roles listed are 'User' and 'SAML Admin'. The 'Access' section shows the user is associated with the 'RedIRIS' division and has the role of 'User'.

Nombre	Nombre de Usuario	Dirección Electrónica	Roles	Division
Chelo Malagón	chelorediris	chelo.malagon@rediris.es	Administrator	RedIRIS
Higinio Maeztu Herrera	higinioeditoris	higinio.maeztu@rediris.es	Administrator SAML Admin	RedIRIS
Higinio Maeztu Herrera	higiniouser	higinio.maeztu@rediris.es	User	RedIRIS
Javier Masa Marín	masa-user	masa@rediris.es	User	RedIRIS
Javier Masa Marín	masa-admin	javi.masa@rediris.es	Administrator SAML Admin	RedIRIS
José Manuel Macías	macias@rediris.es	macias@rediris.es	Administrator User SAML Admin	RedIRIS

**Javier Masa Marín**

Editar Usuario Manage API Keys

**Nombre:** Javier Masa Marín

**Correo electrónico:** masa@rediris.es

**Teléfono:** +34 955056623

**Title:** Middleware Engineer

**Access**

**Division:** RedIRIS

**Usuario:** masa-user

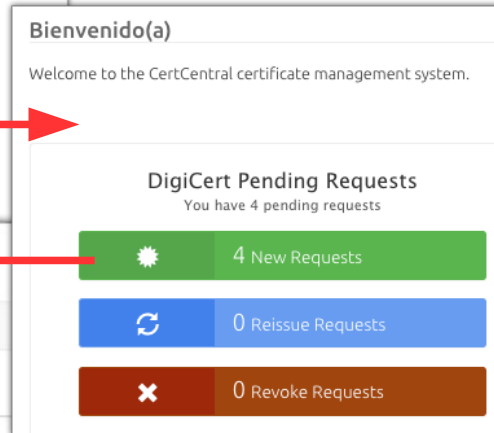
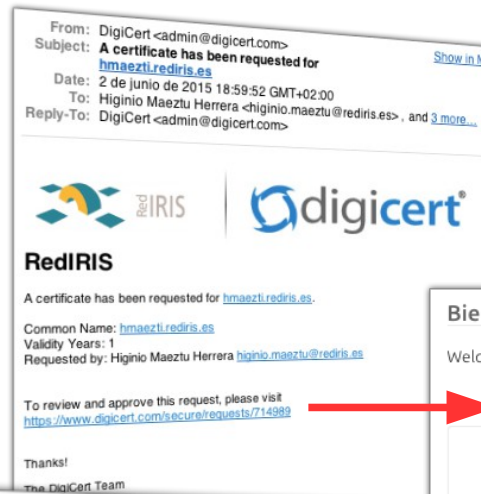
**Roles:** User

**API Keys**

Fecha de emisión	Estatus	Nombre
------------------	---------	--------

# CertCentral: Gestión de solicitudes pendientes

## Flujograma de operación



### Solicitudes

+ Request a Certificate | Download CSV

**Estatus:** Pendiente | **Type:** Todas | **Division:** RedIRIS

Order Id	Nombre Común	Type	Estatus	Division	Requested	Requester	
694956	hmaeztu.rediris.es	EV Multi-Domain	Pendiente	RedIRIS	2015-06-02 8:43 PM	Higinio Maeztu Herrera	<a href="#">View &gt;</a>
694915	hmaeztu.rediris.es	EV Multi-Domain	Pendiente	RedIRIS	2015-06-02 8:04 PM	Higinio Maeztu Herrera	<a href="#">View &gt;</a>
694912	hmaeztu.rediris.es	EV Multi-Domain	Pendiente	RedIRIS	2015-06-02 8:00 PM	Higinio Maeztu Herrera	<a href="#">View &gt;</a>
694911	hmaezti.rediris.es	EV SSL Plus	Pendiente	RedIRIS	2015-06-02 7:59 PM	Higinio Maeztu Herrera	<a href="#">View &gt;</a>

### EV SSL Plus Certificate Request

You do not have permission to approve this request. Please Contact your account administrator to have a user that has been validated for EV approve this request.

[Rechazar](#) [Editar](#)

#### Información de Solicitud

**Division:** RedIRIS  
**Fecha de Solicitud:** 2015-06-02 7:59 PM  
**Requested By:** Higinio Maeztu Herrera <higinio.maeztu@rediris.es>  
**Org Contact:** Chelo Malagón <chelo.malagon@rediris.es>

#### Certificate Details

**ID de Orden:** 694911  
**Producto:** EV SSL Plus  
**Validity Years:** 1  
**Nombre Común:** hmaezti.rediris.es  
**Organización:** Red Académica y de Investigación Nacional  
**Signature Hash:** sha256  
**Longitud de Clave:** 2048  
**Plataforma de servidor:** Apache

**CSR**

```
-----BEGIN CERTIFICATE REQUEST-----
MIICpTCCAY0CAQAwYDEEMHkGA1UEShMCRVh0EDAOBgNVBAgTB1Nldm1sZ
BglVBAwTB1Nldm1sZGExZDA0OTg3MjEhVjE1SSVMxGZAZBgNVBAQTE
dHpuemVkaXJpcy5lc2CCASIAwDQgT7K0ZihvcNAQEBBQADggEPADCCAQo
cggqjwVuhFwCWRjwK87ovR6zqg40BixN5lqDRc1rjy+URnmb92om2pd2
Yt1jml7suo9NA3dggw85hsqkon3ax4P4uAQZ1LYN8v9g+/885sIdHX
Y3n0VYTaxi8T0z1+8DT660GHR441s0G7Gq8Fj85DgRQkR1yjaZ
Q51RfHvpm7emAsP9FrGe6nFgscM9-shNM3zxcLdoKyB1oleynJxllge
apBufRgkRtd8Eeszx12ubGATT4hRznmcbEFP0aAl0LS2iTh1P+vt
2g98mp5H8dki
-----END CERTIFICATE REQUEST-----
```

# ISC + CertCentral: Filtros de dominios por solicitante

## Flujograma de operación

- Lista de dominios permitidos
  - Similar a lo que se hacía en SCS
  - Posibilidad de añadir lista de dominios permitidos por solicitante
  - Seleccionados de la lista de dominios habilitados para la división
- Permite “gestionar centros”
  - Asignando los dominios apropiados a los solicitantes de cada centro
  - Usando ISC para aprobar las solicitudes

**ISC: (Interface del Servicio)**  
Portal de RedIRIS del servicio TCS

**Datos del usuario**

Nombre:  
Chelo

Nombre:  
Malagón

Email:  
chelo.malagon@rediris.es

**Dominios permitidos**

Muestra 50 entradas

Dominio	Acción
prueba1.rediris.com	X
rediris.es	X

Mostrando 1 de 2 de un total de 2 entradas

**Añadir Dominio**

añadir

- ✓ rediris.es
- rediris.com
- rediris.org
- rediris.net

# ISC + CertCentral: Gestión de solicitudes pendientes

## Flujograma de operación

---

- **Gestión de solicitudes en bloque**
  - Aprobación/denegación de varias solicitudes a la vez
- **Control automático de solicitudes “piratonas”**
  - Solicitudes con nombres bajo dominios no permitidos para el usuario solicitante del certificado
    - No cumple los filtros impuestos por la institución
  - Funcionalidad disponible desde ISC
    - Pero desde CertCentral siempre podrán ser aprobadas por el administrador
  - ISC permite la posibilidad de aprobar solicitudes “piratonas”
    - Bajo la responsabilidad del administrador
    - Configurable por institución

# ISC + CertCentral: Gestión de solicitudes pendientes

## Flujograma de operación

### ISC: Solicitudes

Portal de RedIRIS del servicio TCS

Filtrar por estado: pendiente

Muestra 50 entradas Buscar:

ID	Common Name	Tipo	Fecha	Solicitante	Acción
<input type="checkbox"/> 699004	<span>test1.rediris.es</span>	ssl_plus	2015-06-09	Higinio Maeztu Herrera	<input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 699007	test2.rediris.es <span>test3.rediris.es</span>	ssl_multi_domain	2015-06-09	Higinio Maeztu Herrera	<input type="checkbox"/> <input type="checkbox"/>

Mostrando 1 de 2 de un total de 2 entradas Inicio | Anterior | 1 | Siguiente | Final

seleccionar todos aprobar rechazar

Nombre bajo dominio no permitido para el usuario solicitante del certificado.

# Certificados personales (Client Certificates)

## Acceso federado

---

- **Perfiles afectados**

- Premium, Grid Premium, Grid Robot Name

- **Acceso federado**

- CertCentral es un SP de eduGAIN (SAML 2.0)
  - Usuarios finales no necesitan cuenta en el portal CertCentral
- Atributos requeridos
  - ePE (eduPersonEntitlement)
    - urn:mace:terena.org:tcs:personal-user
    - urn:mace:terena.org:tcs:escience-user
  - sHO (schacHomeOrganization)
  - ePPN (eduPersonPrincipalName)
  - displayName
  - mail
- Acceso: <https://www.digicert.com/sso> (próximamente)

# Certificados personales (Client Certificates)

Ejemplo de acceso federado y solicitud de certificado

The image illustrates the process of requesting a client certificate through the DigiCert CERTCENTRAL interface. It consists of four sequential screenshots:

- Screenshot 1 (Top Left):** Shows the "IDP Selection" page. The user is prompted to "Please enter the Identity Provider to authenticate with:" and "RedIRIS" is entered in the text box. A "Start single sign-on" button is visible.
- Screenshot 2 (Middle Left):** Shows the "Request a Certificate" page. The "Product" dropdown menu is open, showing options: "Choose a product", "Premium", "Grid Premium", and "Grid Robot Name". The "Common Name" field contains "Javier Masa Marin".
- Screenshot 3 (Middle Right):** Shows the "Request a Certificate" page. The "Product" dropdown is set to "Premium". The "Common Name" field contains "Javier Masa Marin".
- Screenshot 4 (Bottom Right):** Shows the "Request a Certificate" page. The "Product" dropdown is set to "Grid Premium". The "Common Name" field contains "Javier Masa Marin masa@rediris.es".

Red arrows indicate the flow of the process: from the IDP selection to the certificate request page, then to selecting a product, and finally to selecting a specific product and entering the common name.



# TCS: Recomendaciones

---

- Validación EV
  - Puede requerir llamadas telefónicas (idioma inglés)
  - Documentación legal
- No solicitar certificados personales desde CertCentral
  - Sin usar el protocolo especial para uso no federado
  - *TCS Model Process Non-SAML Personal Issuance*  
<https://wiki.geant.org/display/TCSNT/Documents>
  - Seguir el protocolo para no incumplir lo especificado en la política
- No usar cuenta invitado (Guest Request)
  - GÉANT no recomienda su uso para evitar incumplir las políticas

# Índice de contenidos

---

- 1 Introducción
- 2 Evolución histórica del servicio
- 3 Perfiles disponibles
- 4 CAs
- 5 Alta. Requisitos
- 6 Modelo de servicio y acceso
- 7 Operación del servicio
- 8 Próximas acciones**



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE ECONOMÍA  
Y COMPETITIVIDAD

MINISTERIO  
DE INDUSTRIA, ENERGÍA  
Y TURISMO

red.es



Red IRIS

# TCS - Próximas acciones

---

- Finalizar fase I
  - Con todas las instituciones pendientes que están en SCS
- Comienzo fase II
  - Con el resto de instituciones que no están en SCS
- Activación de ISC
  - Para las instituciones con SIR
- Lista administradores y usuarios
  - tcs-admin
  - tcs-user
- Videosesión

---

# ¡Muchas gracias!



Red IRIS



GOBIERNO  
DE ESPAÑA

MINISTERIO  
DE ECONOMÍA  
Y COMPETITIVIDAD

MINISTERIO  
DE INDUSTRIA, ENERGÍA  
Y TURISMO

red.es



Red IRIS