Novedades del servicio TCS

El servicio de certificados digitales de RedIRIS

Javi Masa - javier.masa@rediris.es

Higinio Maeztu - higinio.maeztu@rediris.es

Índice de contenidos

1 **Bienvenida**

2 Novedades

3 Estadísticas

4 “Problemillas” detectados

5 Preguntas

Bienvenida

- TCS (Trusted Certificate Service)
  - Servicio de certificados digitales de RedIRIS
- Material adicional
  - TCS:
    - http://www.rediris.es/tcs/
  - Presentación:
    - http://www.rediris.es/tcs/coord/jt2015/
  - Alta en el servicio
    - http://www.rediris.es/tcs/alta/

Índice de contenidos

1 Bienvenida

2 **Novedades**

3 Estadísticas

4 “Problemillas” detectados

5 Preguntas

TCS: Novedades - 1
Implantación del servicio TCS

- Solicitantes del servicio: 239 instituciones
- Fase I
  - Migración de las 115 instituciones existentes en SCS a TCS
- Fase II
  - Alta de las 138 instituciones nuevas que solicitaron TCS

	Solicitantes	En TCS	Pendientes
Fase I (SCS: 115)	101	99	2
Fase II (nuevas)	138	39	99
Total	**239**	**138**	**101**

TCS: Novedades - 2
ISC (Interfaz del Servicio de Certificados)

- Requisito: SIR
  - Necesitamos autenticar al administrador y no disponemos de las credenciales almacenadas en CertCentral
- Funcionalidad
  - Filtros
    - Usuarios con sus dominios autorizados
    - Dominios con los usuarios autorizados para cada uno
  - Gestión de solicitudes
    - Filtro por estado (pendiente, rechazado, aprobado)
    - Filtro por tipo de la solicitud (nueva, renovación, revocación)
    - Control de usuarios no autorizados para solicitar certificados bajo un dominio concreto
    - Aprobación, denegación múltiple

TCS: Novedades - 3
ISC (Interface del Servicio de Certificados)

- Listado de certificados emitidos
  - Descarga CSV
- "Valor monetario" estimado
  - Aunque el servicio TCS no supone ningún coste a las instituciones afiliadas, mostramos las tarifas que DigiCert cobraría por los certificados emitidos en base a la fórmula:

<nº años> * (<precio base cert.> + (<nº CNs extra> * <precio 1 CN extra>))

  - Calculamos el valor
    - De cada certificado
    - Agrupado por cada perfil y
    - Total de cada institución

Perfil	CNs	Precio en $/año 1 año	2 años	3 años
SSL Certificates				
1 servidor				
SSL Plus	1	175	157	139
EV SSL Plus	1 cada CN adicional	295 +95	234 +155	-
Multi-dominio, con Subject Alternate Name (SAN)				
Unified Communications	4 cada CN adicional	299 +49	269 +79	239 +99
EV Multi-Domain	3 cada CN adicional	489 +99	389 +169	-
Wildcard (comodín)				
Wildcard Plus	1	595	535	475
Grid Certificates				
Grid Host SSL Grid Host SSL UC Grid Premium Grid Robot Email Grid Robot FQDN	1 25 1 1 1	Precio no proporcionado por DigiCert		
Client Certificates				
Digital Signature Plus Email Security Plus Premium	1 1 1	Precio no proporcionado por DigiCert		
Code Signing				
Code Signing	1	223	198	178
EV Code Signing	1	449	399	331
Document Signing (Organization)				
Document Signing (2000)	1	579	514	465
Document Signing (5000)	1	895	799	716

TCS: Novedades - 4
Coordinación y gestión de centros

- Lista de usuarios del servicio
  - **tcs-user@listserv.rediris.es**
  - Suscripción obligatoria para todos los usuarios con rol de administrador en CertCentral
  - Posibilidad de alta de usuarios adicionales
    - Bajo petición del administrador
    - ¿Direcciones personales/grupo?
- Gestión de centros
  - Creación de organizaciones en CertCentral
  - Filtrado de dominios por cada usuario en ISC
  - Algunos centros
    - IFAE (PIC), CIEMAT (PSA, CETA-CIEMAT), CSIC / (IFCA)
    - ¿Soporte en ISC?

TCS: Novedades - 5
TCS/Grid

- Objetivo
  - Uso de los perfiles Grid de TCS en lugar de la CA de pkIRISGrid
- Piloto TCS/Grid/server
  - Uso de los perfiles *Grid Host SSL* y *Grid Host SSL UC* de TCS en lugar del perfil servidor de pkIRISGrid
  - Ventajas:
    - Eliminamos burocracia (papeleo, reuniones cara a cara, auditorías, …)
    - CA online, revocaciones inmediatas, OCSP
    - Perfil *Grid Host SSL UC* soporta múltiples nombres
  - Participantes
    - PIC (IFAE)
      - 13 certificados *Grid Host SSL*
      - 34 certificados *Grid Host SSL UC* con 103 SAN

Índice de contenidos

1 Bienvenida

2 Novedades

3 **Estadísticas**

4 “Problemillas” detectados

5 Preguntas

TCS: Estadísticas - 1
Públicas

- Listado con los certificados de cada institución
- Listado de todos los certificados emitidos

Institución	Nº Certificados	Nombres		Grid			Valor[1] ($)
		CNs	Wildcard				
UPC - Universitat Politècnica de Catalunya	162	1943	2	0	0	0	requiere ISC
UM - Universidad de Murcia	43	394	3	0	0	0	requiere ISC
UNAV - Universidad de Navarra	115	330	1	0	0	0	requiere ISC
UPV - Universitat Politècnica de València	78	211	3	0	0	0	requiere ISC
UCA - Universidad de Cádiz	26	151	1	0	0	0	requiere ISC
IFAE - Institut de Física d'Altes Energies	47	116	0	0	47	0	requiere ISC
CSIC - Consejo Superior de Investigaciones Científicas	78	114	0	0	0	0	requiere ISC
UC3M - Universidad Carlos III de Madrid	37	92	1	0	0	0	requiere ISC
URJC - Universidad Rey Juan Carlos	39	81	0	0	0	0	requiere ISC
RedIRIS	43	80	2	2	1	0	requiere ISC

TCS: Estadísticas - 2
Privadas (por cada institución)

- Listados de certificados
  - Agrupados por perfiles
  - Detallado por cada perfil

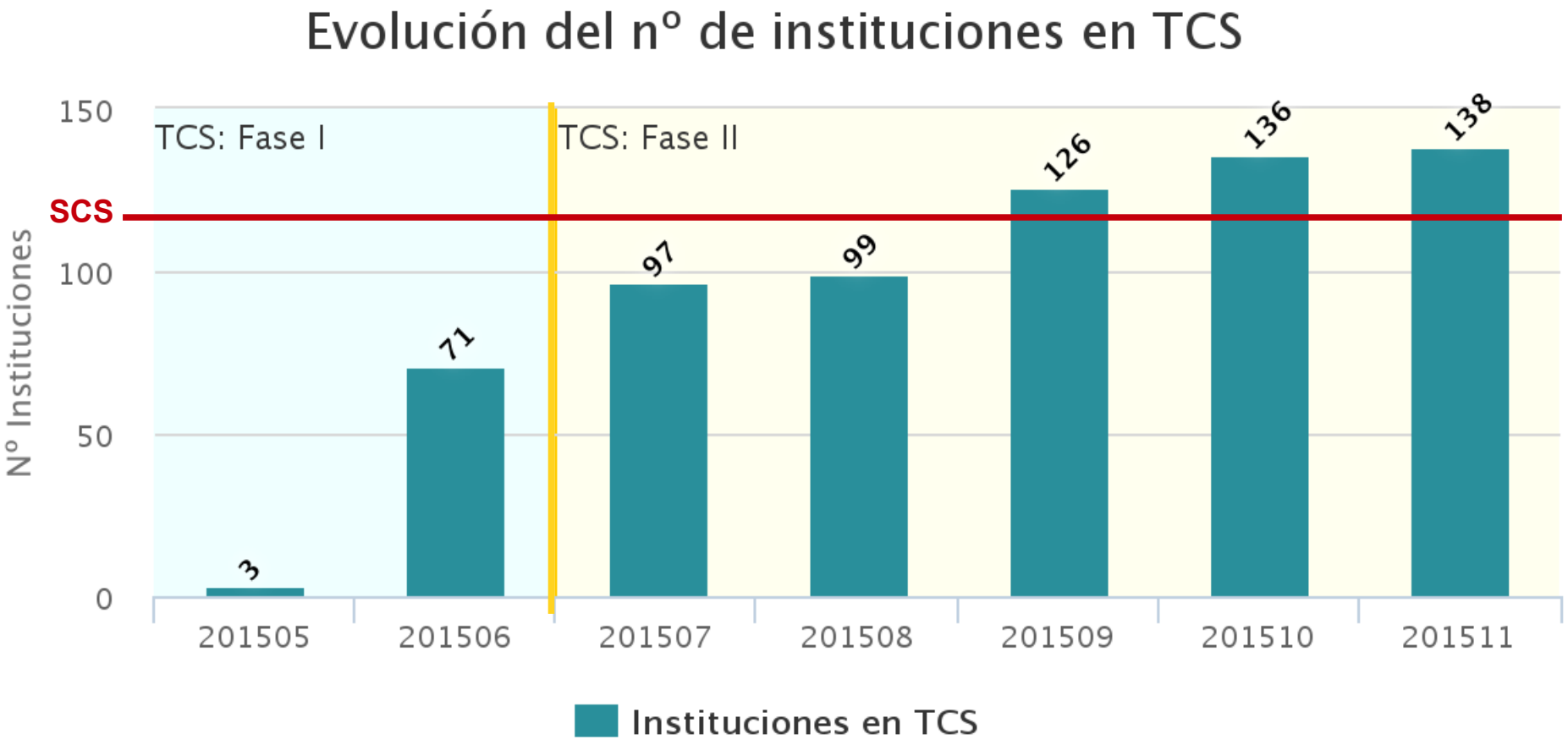
ID	Estado	Valor (1)	Common Name	Tipo	Fecha
691082	Emitido	3 años x	sir2-test.rediris.es	SSL Plus	2015-05-27
691152	Emitido	1 años x	hmaeztu.rediris.es	SSL Plus	2015-05-27
699004	Emitido	1 años x	test1.rediris.es	SSL Plus	2015-06-09
705250	Emitido	3 años x	higinio.rediris.es	SSL Plus	2015-06-18
707278	Revocado	1 años x	hmaeztu.rediris.es	SSL Plus	2015-06-23
708265	Emitido	1 años x	test7.rediris.es	SSL Plus	2015-06-24
708266	Emitido	1 años x	test8.rediris.es	SSL Plus	2015-06-24
708287	Emitido	1 años x	test8.rediris.es	SSL Plus	2015-06-24
710738	Emitido	3 años x	migrador-irismail.rediris.es	SSL Plus	2015-06-29
800294	Emitido	3 años x	www.csirt.es	SSL Plus	2015-11-04
TOTAL					

RedIRIS

Tipo	1 año	2 año	3 año	Valor(1)/tipo ($)
ssl_plus	6 +0	0 +0	4 +0	
ssl_ev_plus	1 +0	11 +0	0 +0	
ssl_multi_domain	0 +0	0 +0	2 +0	
ssl_ev_multi_domain	0 +0	4 +23	0 +0	
ssl_wildcard	0 +0	0 +0	2 +2	
code_signing	1 +0	0 +0	0 +0	
code_signing_ev	0 +0	0 +0	0 +0	0
grid_host_ssl	1 +0	0 +0	0 +0	0
client_premium_sha2	4 +0	0 +0	1 +0	0
client_grid_premium	2 +0	0 +0	0 +0	0
document_signing_org_1	0 +0	0 +0	0 +0	0
document_signing_org_2	0 +0	0 +0	1 +0	
TOTAL				

TCS: Estadísticas - 3

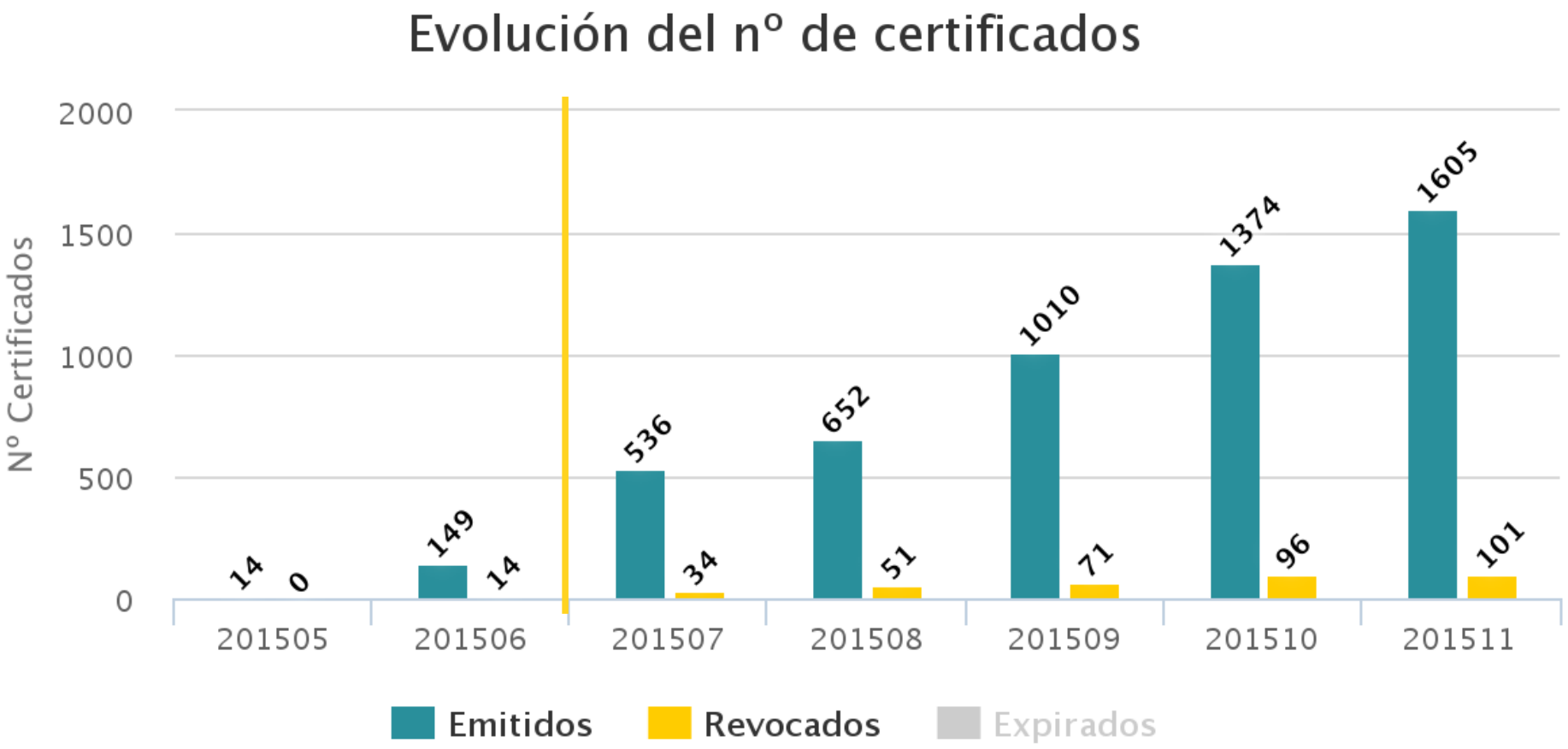
Aumento notable del nº de instituciones participantes respecto a SCS



Datos obtenidos a fecha 18/11/2015

TCS: Estadísticas - 4

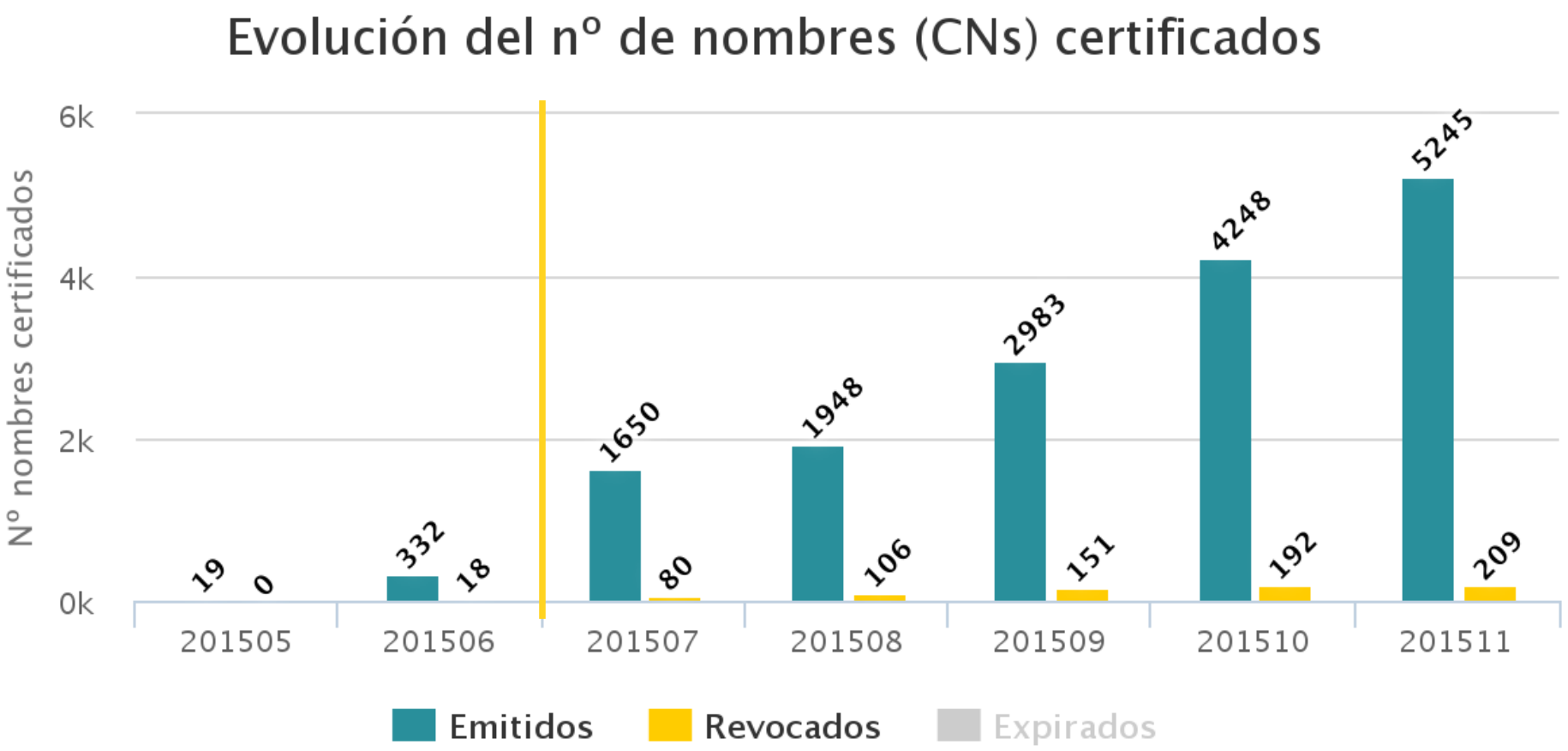
Evolución del número de certificados emitidos en 2015



Datos obtenidos a fecha 17/11/2015

TCS: Estadísticas - 5

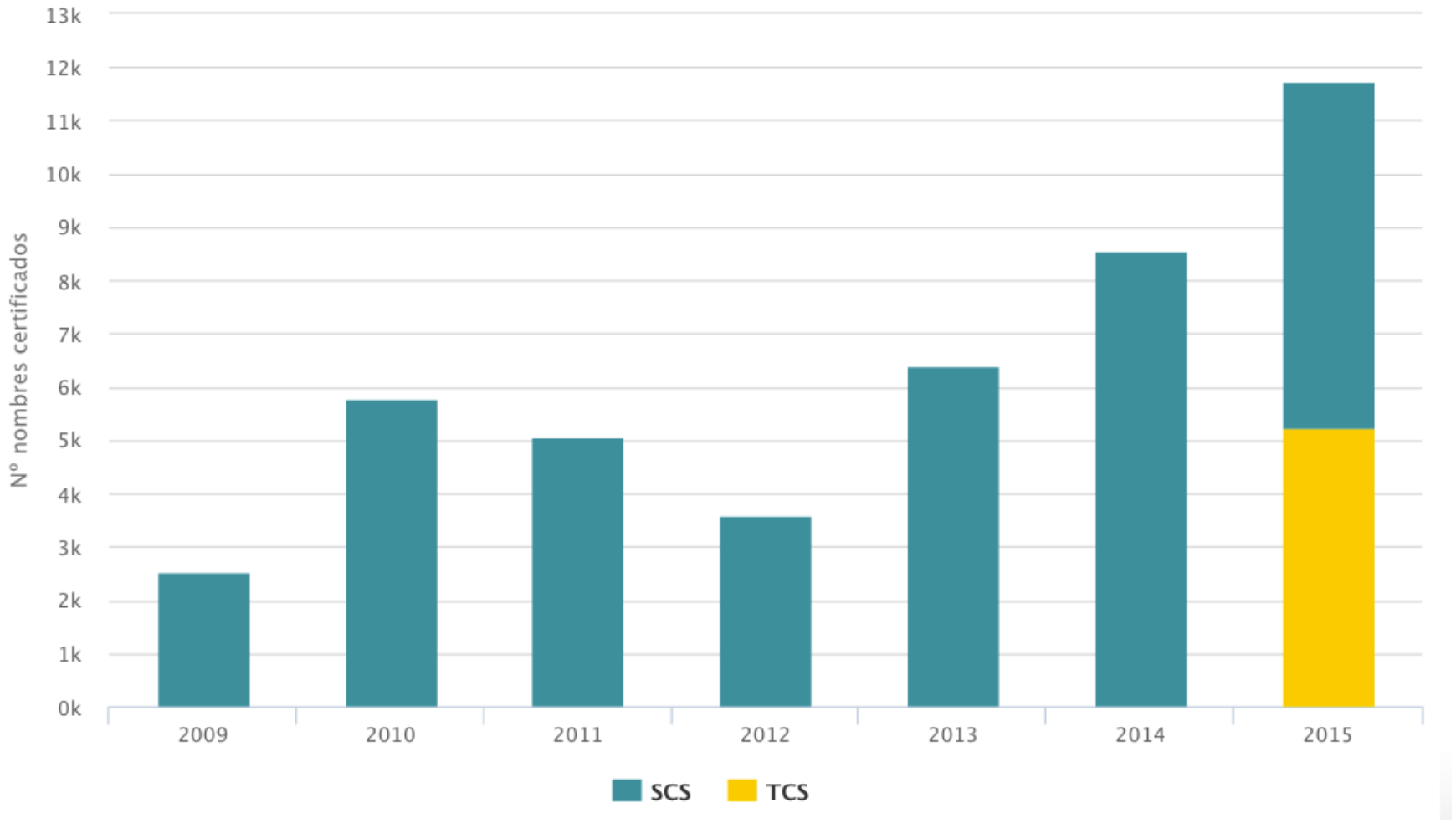
Evolución del número de nombres (CNs) certificados en 2015



Datos obtenidos a fecha 17/11/2015

TCS: Estadísticas - 6

Nombres (CNs) certificados anualmente desde 2009



Datos obtenidos a fecha 17/11/2015

Índice de contenidos

1 Bienvenida

2 Novedades

3 Estadísticas

4 **“Problemillas” detectados**

5 Preguntas

“Problemillas” detectados - 1

- Envío de CUSOs en papel (59)
  - Tardan en llegarnos en papel
  - Soluciones:
    - Envío por mensajería, firma electrónica, ¿Uso de “CUSINATOR”?

- Correos de DigiCert
  - Perdidos: mirar listas negras
  - No válidos: validar en pocos días
- Fallos en el Dpto. de validación de DigiCert
  - Validación EV
    - Error en CIF (cambio de i por 1)
  - Revisad bien la información que aparece en vuestros certificados EV

“Problemillas” detectados - 2

- Centros afiliados a RedIRIS con IdP propio
  - Acceso al ISC
    - ¿Uso de su propio IdP o del IdP institucional?
  - Acceso a CertCentral mediante SSO
    - ¿Uso del IdP de la institución a la que pertenen?
    - Se puede añadir un IdP distinto por organización. ¿Pruebas?
- Uso incorrecto de CertCentral (certificados personales)
  - Problema: solicitud de certificados personales sin federación
  - Solución: uso de la federación
    - Tener el IdP de SIR en eduGAIN
    - Enviar una serie de atributos concretos
    - http://www.rediris.es/tcs/caracteristicas/perfiles/personal/
    - http://www.rediris.es/tcs/caracteristicas/perfiles/personal/federacion.html

“Problemillas” detectados - 3

- Gestión de cargos
  - ¿Puedo crear un certificado personal para un cargo?
  - Problema:
    - El acceso a CertCentral debe ser federado para estos perfiles personales
    - Los atributos del DN se rellenan de los datos de la aserción
  - Solución:
    - Certificado de empleado público

Índice de contenidos

1 Bienvenida

2 Novedades

3 Estadísticas

4 “Problemillas” detectados

5 Preguntas

¿Alguna pregunta?

¡Muchas gracias!

RedIRIS