pkIRISGrid y TCS

Sesión de Identidad Digital

`https://pki.irisgrid.es/`
`https://www.rediris.es/tcs/`

Javi Masa - javier.masa@rediris.es

GOBIERNO DE ESPAÑA | MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD | MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

red.es

Madrid, 29/11/2017

Índice de contenidos – certificados digitales

1.1 Migración de pkIRISGrid a TCS
Fases

Fase 0 13/03/2016-30/05/2016	Fin de creación de nuevas RAs de pkIRISGrid Desactivación de las RAs sin certificados activos
Fase 1 01/09/2015	Inicio uso de TCS para perfiles Grid/*servidor*
Fase 2 01/05/2016	Inicio uso de TCS para perfiles Grid/*personal* y Grid/*robots*
Fase 3 01/06/2016-17/10/2016	Eliminación perfil *servidor* de las RAs de pkIRISGrid
Fase 4 18/10/2016-14/03/2017	Eliminación perfiles *personal* y *robots* de RAs de pkIRISGrid
Fase 5 28/04/2015-20/03/2017	Baja de RAs de pkIRISGrid
Fase 6 25/01/2017-08/11/2017	**Eliminación del servicio pkIRISGrid** • Revocación del último certificado (10/08/2017) • Eliminación de la CA del círculo de confianza de EUGridPMA (09/10/2017) • Emisión de CRLs periódicas hasta expiración del último certificado válido
08/11/2017-	• Backup para auditorías EUGridPMA • Destrucción física de la clave privada de la CA • Borrado del software de la CA

1.2 Migración de pkIRISGrid a TCS
Fase 4 - problemas para la solicitud de certificados personales

- SAML Portal - acceso federado
  - IdP en eduGAIN
  - Envío de ciertos atributos desde el IdP
    - `https://www.rediris.es/tcs/sso/atributos.html`
  - Composición de los datos enviados en la aserción
  - SAML Portal (febrero 2017)
    - Redirecciones "casi infinitas" a la hora de seleccionar el IdP
    - Pruebas desde `https://www.rediris.es/tcs/sso/wayfless/`
      - Autenticarse en el IdP
      - Abrir varias pestañas del navegador en menos de 1 minuto
- Sin SAML Portal
  - NO RECOMENDADA - uso en caso **excepcional** y de forma **temporal**
  - Atención a la composición del CN
    - *displayName* + *eduPersonPrincipalName*

      `Nombre Apellido1 Apellido2 user@scope.es`

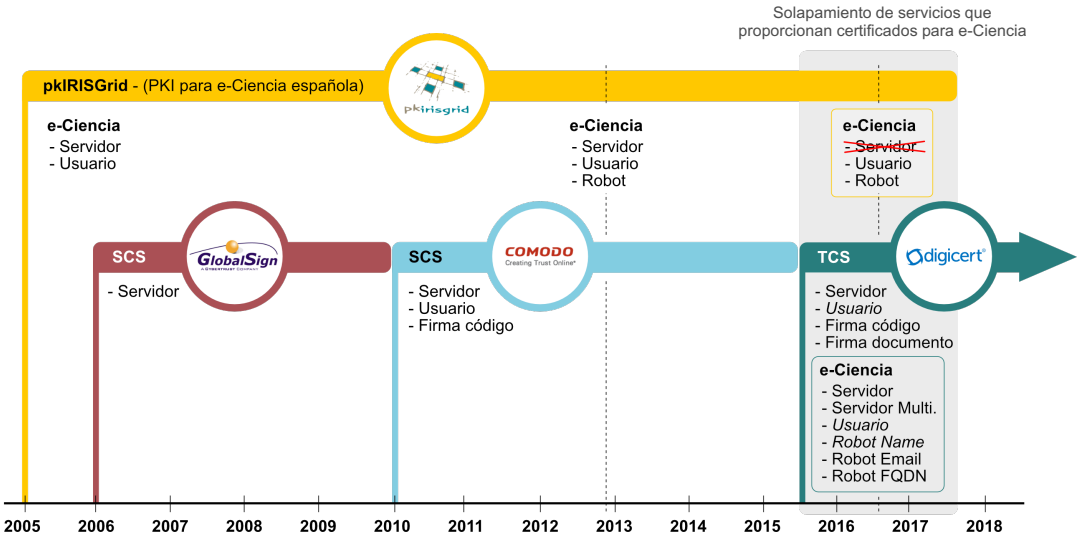
2 Finalización de pkIRISGrid

- Algunos datos estadísticos
  - Hardware “muy duro”




2 Finalización de pkIRISGrid

- Algunos datos estadísticos
  - 12 años de existencia (2005-2017)
  - 50 autoridades de registro (RAs)
  - 180 operadores de RAs
    - **Muchas gracias por vuestro trabajo**
  - Casi 10.000 certificados emitidos
    - ~ 4.500 de usuarios
    - ~ 5.500 de servidor
    - ~ 20 de robots



3.1 TCS
TCS en cifras

- En servicio desde julio de 2015
- 172 instituciones en TCS
  - 383 administradores dados de alta en el portal CertCentral (DigiCert)
- 11.746 certificados emitidos
  - 41.999 nombres certificados
    - 332 certificados wildcards
- Perfiles de Grid (soporte al antiguo pkirisGrid)
  - 873 certificados emitidos desde 23 instituciones
    - 206 Grid Host Multi-Domain SSL
    - 374 Grid Host SSL
    - 286 Grid Premium
      - 7 Grid Robot Name

3.2 TCS
Recortes en los DNs de los certificados

- DigiCert es auditada antes del verano
  - No aplicaba completamente el RFC 5280
    Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
  - Es obligada a su aplicación completa
    - Recortes a 64 caracteres (O y CN)
- Recortes del campo O
  - Más de 120 instituciones afectadas
  - Por ejemplo, el CIEMAT ha tenido estas cadenas en el campo O:

```
O=Centro de Investigaciones Energeticas Medioambientales y Tecnologicas
O=Centro de Investigaciones Energeticas Medioambientales y Tecnolo
O=Centro de Invest. Energeticas Medioambientales y Tecnologicas
```

- Recortes del campo CN
  - SAML Portal daba error con CNs > 64 pero no indicaba la causa

3.3 TCS
Certificados wildcard de tercer nivel (*.dom.ain)

- 332 certificados wildcard solicitados por 96 instituciones
  - 90 certs. wildcard de tercer nivel solicitados por 55 instituciones
- ¿Qué uso se hace de este certificado?
  - ¿Servidor web para toda la institución?
  - ¿Se comparte ese certificado para diferentes sites?
    - ¿Se instala en diferentes servidores?
    - ¿Se gestiona bien la seguridad de la clave privada?
- ¿Es realmente necesario este certificado?
  - ¿Se pide por comodidad o falta de tiempo?
  - ¿Por ser previsor y tenerlo de comodín para una urgencia?

3.4 TCS - Registro CAA
(Certification Authority Authorization)

- RFC 6844
  DNS Certification Authority Authorization (CAA) Resource Record
  - Define la implementación de un estándar para la Autorización de Entidades de Certificación utilizando el registro CAA del DNS
  - P. ej. DigiCert tiene permitido emitir certificados no wildcards para el dominio `universiris.es`

```
universiris.es.   IN   CAA   0   issue "digicert.com"
universiris.es.   IN   CAA   0   issuewild ";"
universiris.es.   IN   XAA   0   iodef "mailto:incidentes@universiris.es"
```

- CAA es voluntario para los propietarios de los dominios
  - Si un dominio no publica un conjunto de registros CAA, la CA emitirá los certificados como hasta ahora
- Pero CAA es obligatorio para las CAs desde septiembre
  - La Universidad Técnica de Múnich ha creado un test para comprobar este cumplimiento, y SURFnet lo ha verificado para DigiCert (`https://github.com/quirins/caa-test`)

3.5 TCS
Recomendaciones generales

- Usuarios
  - Disponer de más de un administrador validado EV
- Certificados
  - Renovar los certificados varios meses antes de su expiración
  - Intentar no renovar todos los certificados a la vez
- Validaciones
  - Validaciones EV de usuario
    - Solicitar a DigiCert por chat:
      - Que os llamen en castellano si hay problemas con el inglés
      - Que lo hagan en un determinado horario
    - Avisar a los responsables de los teléfonos pertinentes para que estén pendientes de las llamadas de DigiCert
- Ante cualquier duda
  - Usar la ventana de chat de CertCentral para contactar con DigiCert

¿Alguna pregunta?

RedIRIS

Muchas gracias por vuestra atención