pkIRISGrid2TCS

Migración de pkIRISGrid a TCS

http://pki.irisgrid.es/pkirisgrid2tcs/
http://www.rediris.es/tcs/

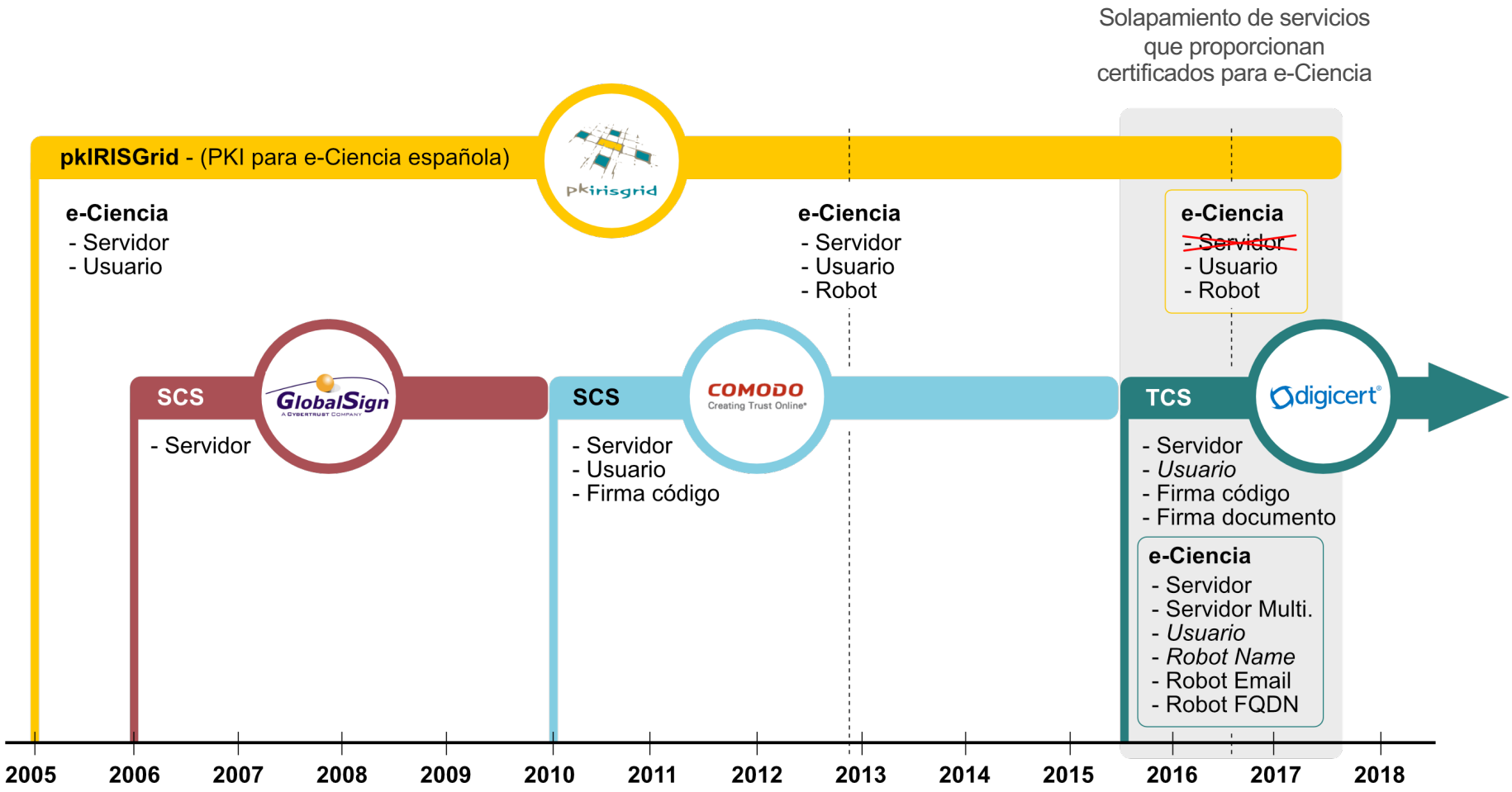
Javi Masa - javier.masa@rediris.es

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
red.es
Red IRIS

Valencia, 14/11/2016

Índice de contenidos

1. Evolución de los servicios de certificación en RedIRIS



2. pkIRISGrid vs TCS
Comparativa de características más importantes - 1/2

	pkIRISGrid	TCS
Autoridad de certificación		
• CA online	N	S
• Servicio 24x7	N	S
• CRLs generadas de forma automática + OSCP	N	S
• Certificados reconocidos en la mayoría de clientes	N	S
Perfiles de certificados Grid		
• Servidor (Grid Host SSL)	S	S
• Servidor multi dominio (Grid Host Multi-Domain SSL)	N	S
• Personal (Grid Premium)	S	S
• Robot Name (Grid Robot Name)	S	S
• Robot Email (Grid Robot Email)	S	S
• Robot FQDN (Grid Robot FQDN)	N	S

2. pkIRISGrid vs TCS
Comparativa de características más importantes - 2/2

	pkIRISGrid	TCS
Simplificación de la burocracia		
• Auditorías de la CA ante la EUGridPMA	S	N
• Auditoría anual de las RAs de pkIRISGrid	S	N
• Reunión anual de coordinación de operadores de RAs	S	N
• Gestión en las RAs		
◦ Entrevistas con los usuarios por cada nueva solicitud	S	N
◦ Entrevistas cada 3 renovaciones de certificados	S	N
◦ Recogida y almacenamiento de documentación con información personal (para las auditorías)	S	N
Autogestión del servicio en las instituciones (sin aviso a RedIRIS)		
• Altas/bajas de los administradores	N	S
• Altas/bajas de organizaciones, dominios, perfiles, solicitantes, …	N	S
• Gestión de solicitudes (aprobación, denegación)	S	S

3. Cambios relevantes en TCS
Composición de los DNs de los certificados

Cambio de espacio de nombre (<prefijo>)

- pkIRISGrid: dc=es,dc=irisgrid
- TCS: dc=org,dc=terena,dc=tcs,c=ES

DNs de los certificados

- Servidores: *<prefijo>*,o=<ORG>[,ou=],cn=<**a.b.c.d**>
- Robots: *<prefijo>*,o=<ORG>[,ou=],cn=**Robot - <robot purpose> managed by <owner>**
- Personas
  - pkIRISGrid:
    <prefijo>,o=<ORG>[,ou=],cn=<**name**>
    dc=es,dc=irisgrid,o=pic,cn=manuel.delfino
  - TCS:
    <prefijo>,o=<ORG>[,ou=],cn=<**name**> <**id_IdP**>
    dc=org,dc=terena,dc=tcs,c=ES,o=PIC,cn=Manuel Delfino delfino@pic.es

    A reasonable representation of the name of the Applicant appended with an Identifier that uniquely and persistently represents the Applicant in the Subscriber's IdP as described in Section 3.1.5 "Uniqueness of Names".

3. Cambios relevantes en TCS
Gestión de usuarios

- pkIRISGrid
  - Alta administrador
    - Cada RA envía una ficha de solicitud de alta por cada administrador
  - Alta usuario
    - Los usuarios finales introducen sus datos en el portal de pkIRISGrid en cada solicitud de certificado nuevo
      - Serán auditados posteriormente por los administradores de las RAs
- TCS
  - Alta administrador
    - RedIRIS añade al administrador principal de cada institución en el portal CertCentral de DigiCert
  - Alta usuario
    - El administrador da de alta a sus usuarios una sola vez
      - Asigna diferente roles a sus usuarios

3. Cambios relevantes en TCS
Solicitud de certificados

- pkIRISGrid
  - Certificados de **servidor** y **usuario**
    - Portal de pkIRISGrid
  - Certificados **robot**
    - Portal de pkIRISGrid (control de acceso mediante certificado de usuario) + máquina local usuario (generación par de claves)
- TCS
  - Certificados **no personales**
    - Opción 1: Desde el portal CertCentral + cuenta de usuario en el portal
    - Opción 2: Enviando solicitud a un usuario con cuenta en CertCentral
    - Opción 3: Usando API + desarrollo particular en cada institución
  - Certificados **personales**
    - Desde CertCentral + acceso federado (eduGAIN) + atributos (sHO, ePPN, dispN, mail, ePE = *urn:mace:terena.org:tcs:escience-user*)

3. Cambios relevantes en TCS
Administración de solicitudes de certificados

- pkIRISGrid
  - Desde el portal de pkIRISGrid + acceso federado (SIR) + cuenta administrador
- TCS
  - Certificados **no personales**
    - Opción 1: Desde el portal CertCentral + cuenta admin en CertCentral
    - Opción 2: Desde el portal ISC de RedIRIS + acceso federado (SIR/SIR2) + cuenta admin en CertCentral
    - Opción 3: Desde el portal ISC de RedIRIS + acceso federado (SIR/SIR2) + cuenta operador de ISC para el perfil Grid (no necesita cuenta en CertCentral)
  - Certificados **personales**
    - No es necesaria la autorización del administrador
      - Se emiten directamente ya que el acceso es federado

4. Planificación de la migración de pkIRISGrid a TCS

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-	Eliminación perfiles *personal* y *robots* de RAs de pkIRISGrid
Fase 5 28/04/2015-	Baja de RAs de pkIRISGrid
Fase 6	Eliminación del servicio pkIRISGrid • Emisión de CRLs periódicas hasta expiración del último certificado válido • Eliminación de la CA del círculo de confianza de EUGridPMA • Eliminación de la lista de correo de operadores de RAs • Eliminación de la lista de correo de operadores de la CA • Destrucción física de la clave privada del certificado de la CA • Borrado del software de la CA

¿Alguna pregunta?

RedIRIS

Muchas gracias por vuestra atención