Actualidad

SIR/SIR2

José Manuel Macías <jmanuel.macias@rediris.es>

GT2015, Madrid, 9 de junio de 2015

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

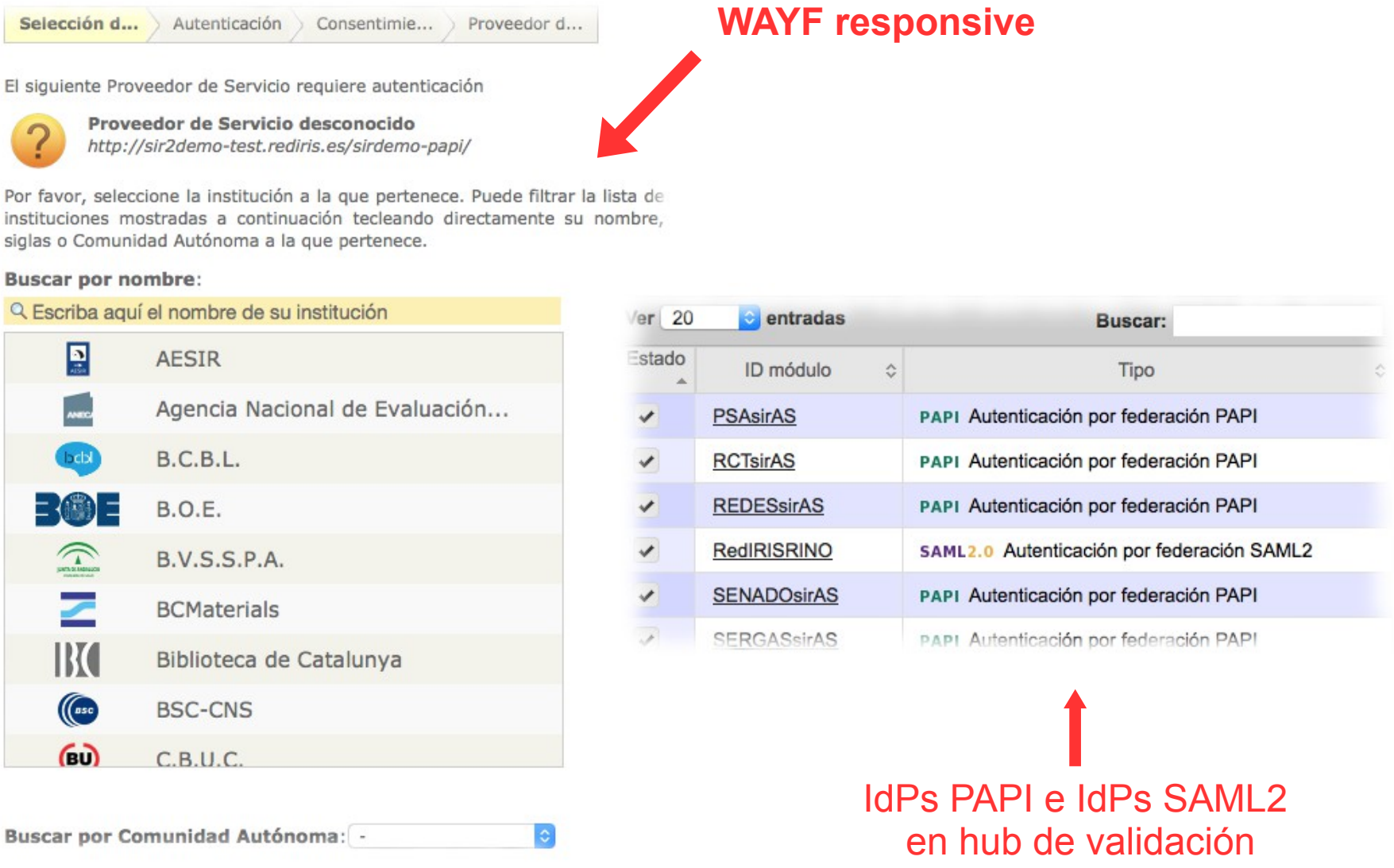
Agenda

- Estado despliegue nuevo hub
- Herramienta de gestión de metadatos
- Instalador IdP de referencia
- Actualización fechas del plan previsto
- Procedimiento de actualización
- Política de la federación SIR2
- Contenido del manos en la masa

Estado despliegue nuevo hub

- El nuevo hub está desplegado en un entorno de validación, realizándose en estos momentos:
  - Pruebas de interoperabilidad entre IdPs (tanto los legacy PAPI, como los nuevos SAML2)
  - Validación características (módulo de consentimiento, grupos de IdP, UX)
  - Pruebas de balanceo de carga y correcto funcionamiento de persistencia
  - Pendientes:
    - Pruebas exhaustivas de las pasarelas propietarias
    - Pruebas de acceso wayfless viniendo del hub de SIR
    - Traducción de mensajes
    - Despliegue de aplicaciones de validación

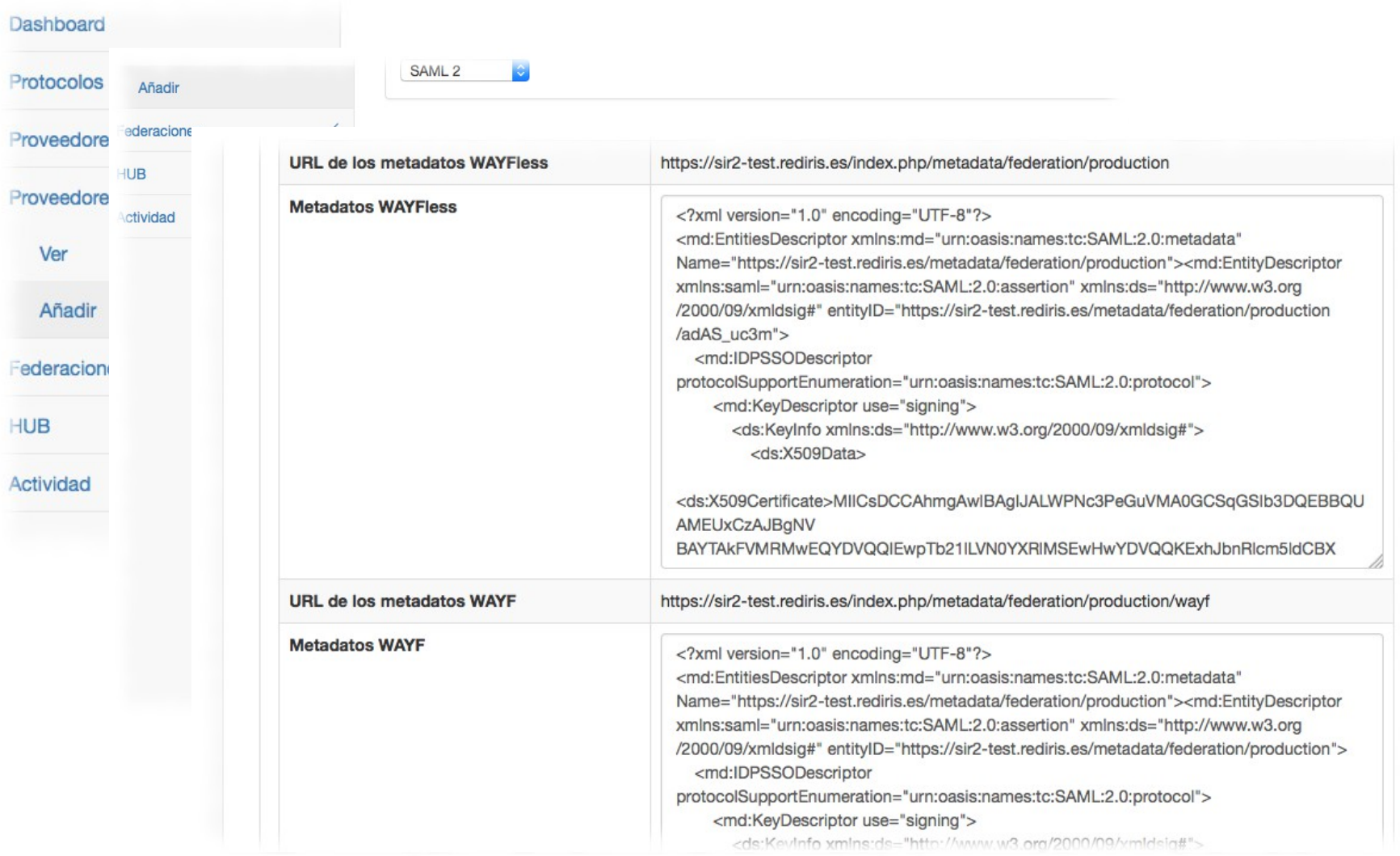
Estado despliegue nuevo hub (II)



Herramienta de gestión de metadatos

- Es una herramienta pensada principalmente para el operador de la federación, aunque en el futuro permitirá la autogestión de los metadatos propios de un IdP
- Están realizándose pruebas:
  - De importación de metadatos de distinta procedencia
  - De agregación de metadatos
  - De *rollback* de cambios en los metadatos
  - De conjuntos de metadatos WAYF y WAYF-less
  - De incorporación de metadatos a distintos SPs
- Pendientes:
  - Facilitar el acceso a IdPs
  - Verificar el flujo IdP→ operador de federación

Herramienta de gestión de metadatos (II)



Instalador IdP de referencia

- Módulo de SimpleSAMLphp (http://git.io/vIwrU)
- Es un asistente en 7 pasos que creará una configuración básica del IdP
- El instalador genera par de claves del IdP
- También genera metadatos, y descarga los metadatos de la federación (ahora mismo entorno test de SIR)
- Añadido un script que hace una descarga previa de todo el software:
  - Dependencias: módulos php, git, curl
  - El script configura también apropiadamente permisos y propietario
- Este instalador se usará mañana en el manos en la masa de instalación de IdPs SIR2

Instalador IdP de referencia (II)

Actualización de fechas

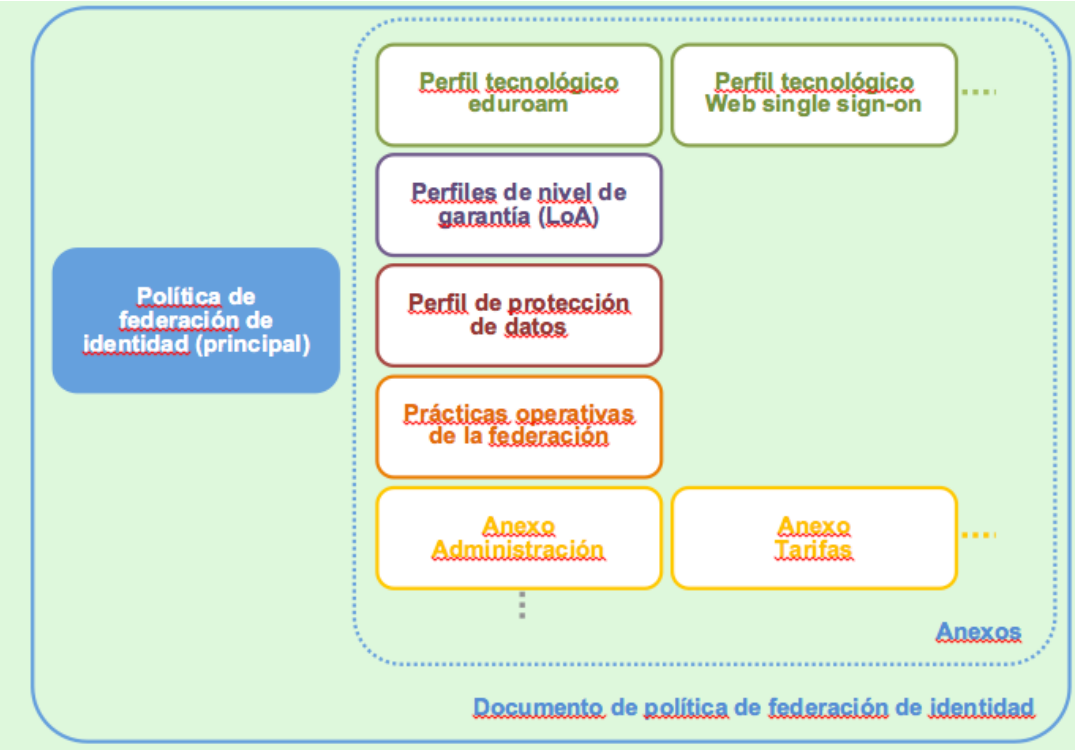
fase	¿qué ocurre?	meses	Nueva previsión
0	Pruebas iniciales de validación y del IdP de referencia	marzo - mayo	✔
1	Validación IdP PAPI legacy	abril - mayo	**junio-julio**
2	Conexión IdP PAPI legacy a nueva federación	junio	**[julio]**
3	Migración de IdPs PAPI a IdPs SAML2int	junio - noviembre	**[julio]** - noviembre
4	Migración de SPs a nueva federación	[junio] a [noviembre]	[**julio**] a [noviembre]
5	Apagado de la actual federación	[noviembre]	[noviembre]

Proceso de actualización

1) Prueba del IdP actual PAPI en entorno de validación de SIR2
   - Consistirá en acceder a un SP que mostrará que los atributos actuales llegan bien a través del nuevo hub
2) Conexión del IdP SIR con la conexión WAYFless SIR2
   - Con esto validaremos que la transición no provocará ningún tipo de interrupción
3) Prueba del nuevo IdP en entorno de validación de SIR2
   - Con esto se validará que el nuevo IdP suelta todos los atributos requeridos en SIR2
4) Validación del nuevo documento de condiciones de uso
   - A través de un nuevo SP SAML conectado a SIR2
5) Cambio del IdP PAPI por el IdP SAML2int en producción

Política de la federación SIR2

- Basada en el trabajo realizado en el grupo FOP (*Federation Operation Best Practice*) de REFEDS (https://refeds.org/)
  - https://wiki.refeds.org/display/FBP/Federation+Operator+Best+Practice+-+FOP
- Se trata de un framework de políticas en torno a un documento principal + anexos



¡¡¡¡Muy poco hecho y mucho por hacer!!!

Contenido del manos en la masa

- Módulo 1: Introducción a la federación de identidad
- Módulo 2: Atributos
- Módulo 3: Proveedor de identidad
  - El IdP de referencia de SIR2
  - Repositorios de identidad: LDAP, *SQL, CAS,...
  - Consideraciones de seguridad
- Módulo 4: Proveedores de servicio
- Módulo 5: procedimiento para unirse a SIR2
- Módulo 6: eduGAIN

Contenido del manos en la masa (II)

- Ejercicio 1. Pre-instalación del IdP de referencia
- Ejercicio 2. Configuración segura de nuestro servidor web
- Ejercicio 3. Ejecución del instalador de IdP
- Ejercicio 4. Comprobación de nuestro IdP
- Ejercicio 5. Configuración de fuente de datos LDAP
- Ejercicio 6. Acceso federado
- Ejercicio 7. Depuración con SAML Tracer
- Ejercicio 8. Atributos