Hacia un nuevo SIR

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

Cáceres, 24 de noviembre de 2014

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

Agenda

- El equipo actual de SIR
- CASIR
- Mismo servicio, nueva federación
  - La federación en la actualidad
  - Licitación de herramientas
  - Características de la nueva federación
    - Arquitectura y protocolos soportados
    - Atributos
    - Conexión con eduGAIN
    - Nueva política y nuevo CUSO
  - ¿cómo será la transición?
    - Descripción de las distintas fases
    - Fechas a tener en cuenta
  - Nombre de la nueva federación

El equipo actual de SIR

Miss Rabbit

Miss Rabbit has many jobs. She runs the supermarket checkout, has an ice cream stall, sell tickets at the museum, drives the bus, drives the school coach, flies a rescue helicopter, flies a hot air balloon etc etc. Miss Rabbit is Rebecca and Richard Rabbit's aunty. The sound Miss Rabbit makes is: Squeak!

CASIR

Un Anillo para gobernarlos a todos, un Anillo para encontrarlos, un Anillo para atraerlos a todos y atarlos en las tinieblas.

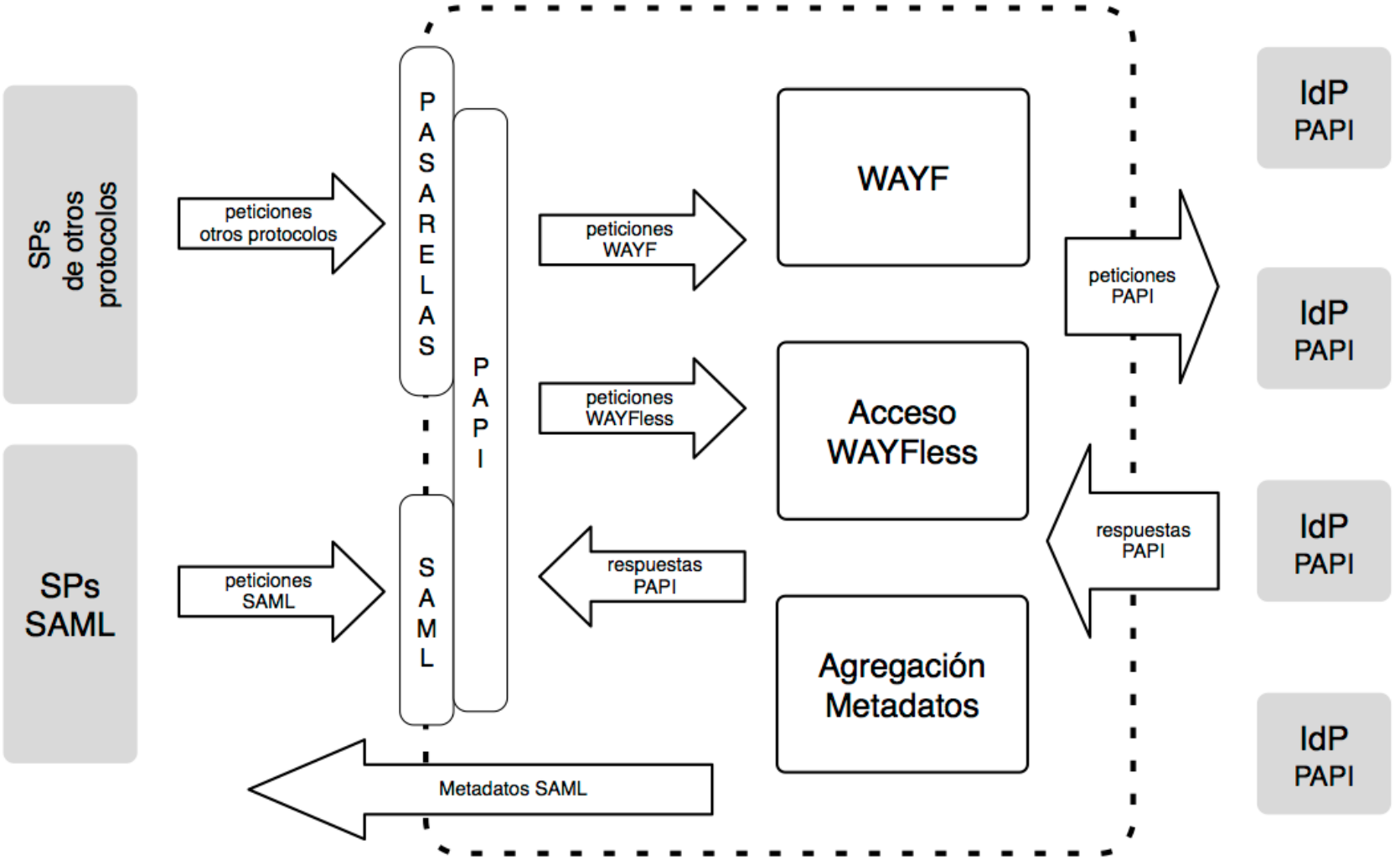
Mismo servicio…

- Misma arquitectura, *hub & spoke*
- Soporte de los mismos protocolos en salida como mínimo
- Tenemos intención de que todos los IdPs y SPs actuales estén en la nueva federación

… nueva federación

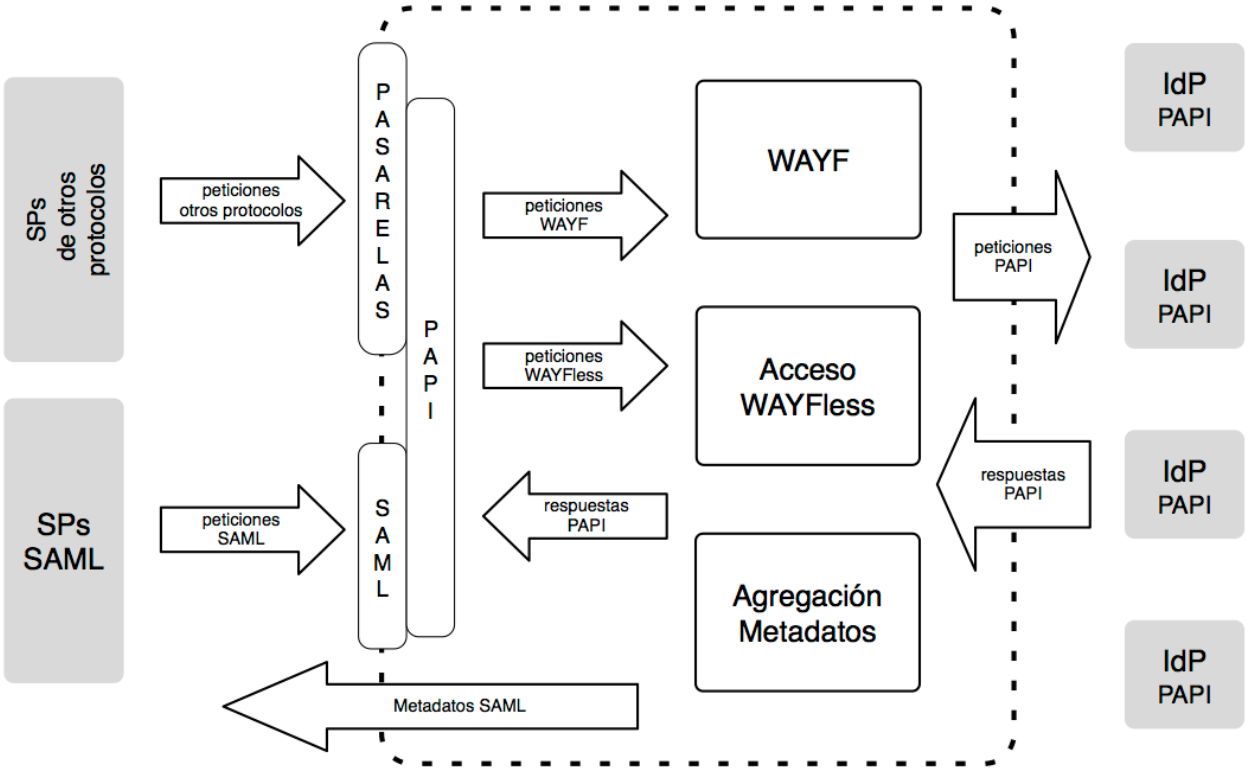
- Nueva política
- Nuevo protocolo intra-federación: SAML2int
- Nuevos conjunto de atributos mínimos
- Nuevos conjuntos de metadatos
- Soporte de nuevos protocolos de salida
- eduGAIN opt-out

La federación en la actualidad



SIR hoy en día (II)

> 250
Proveedores de servicio



7.450.862
autenticaciones procesadas en 2013

122
Proveedores de identidad

Licitación de herramientas (I)

- Exp. 117/14-RI (5 de agosto)
- Qué pretendíamos:
  - Cambiar el protocolo que hablamos con los IdPs
  - Integración/implementación de un 'IdP de referencia'
  - Mejoras sobre el WAYF
  - Mantenimiento de las pasarelas actuales valorando el soporte de nuevos protocolos
  - Mejorar la gestión de metadatos de la federación

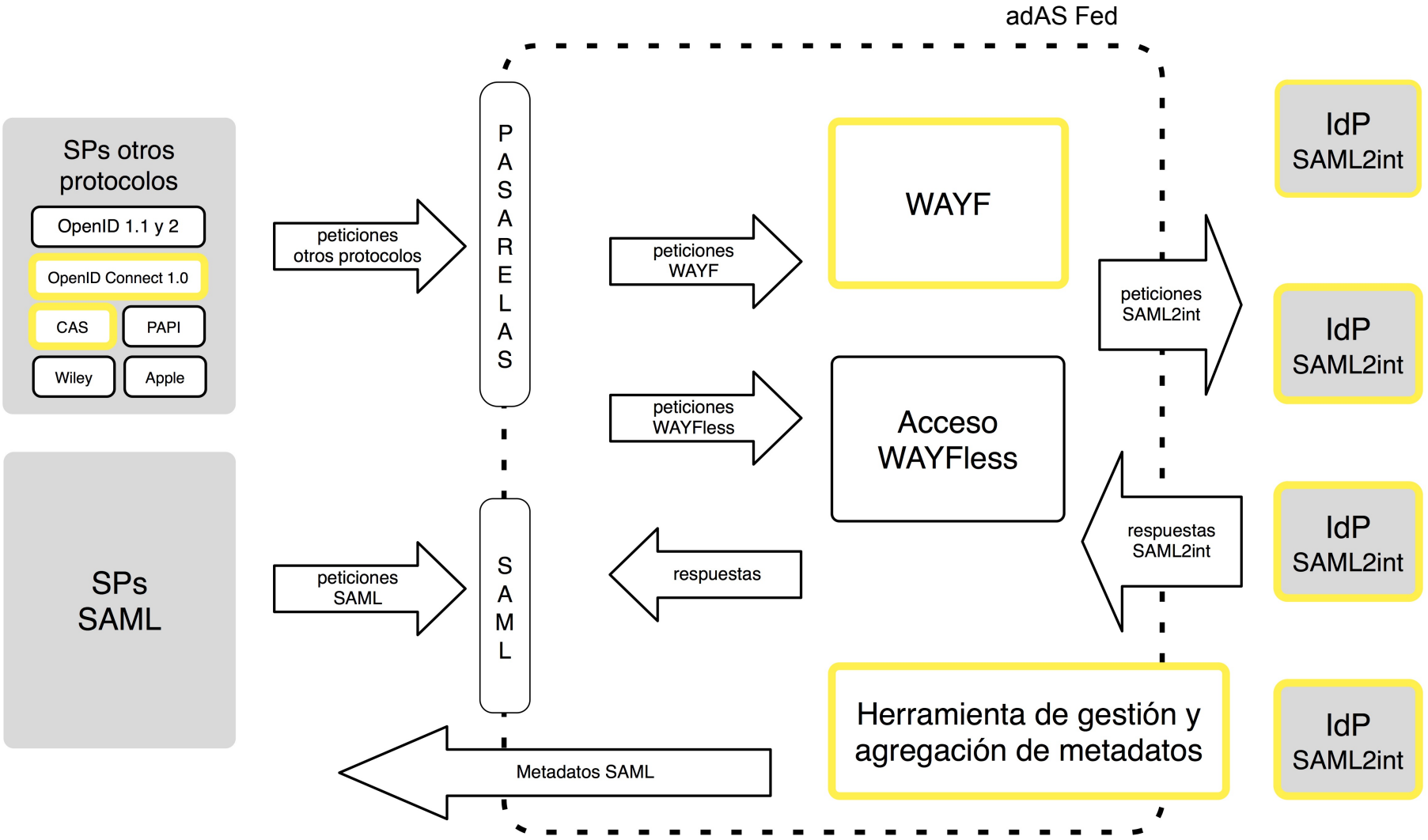
Licitación de herramientas (II)

- Lo que el adjudicatario ha ofrecido:
  - Hub de la federación basado en adAS Fed
    - Incorpora herramienta de configuración, administración y operación de la federación
  - IdP de referencia basado en simpleSAMLphp
  - Soporte de protocolos en salida
    - se mantienen los soportados y pasarelas propietarias
    - se suman OpenID Connect y CAS
  - Herramienta de gestión de metadatos según los requisitos
    - permitirá una gestión más ágil de metadatos
    - incorpora la delegación de gestión de metadatos a IdPs
  - El WAYF se implementará manteniendo características del actual y añadiendo mejoras

Licitación de herramientas (III) - IdP de referencia

- simpleSAMLphp
- Licencia GPL
- Reúne los requisitos solicitados:
  - IdP SAML2int, mapeo de atributos
  - Integración con LDAP y bases de datos relacionales
  - Integración con CAS y ADFS
- Se proporcionará un instalador pensado para configurar simpleSAMLphp para la nueva federación
- Se creará documentación de soporte para los distintos protocolos solicitados
- Se ofrece soporte a un número de instituciones, sobre la base del instalador y la documentación generada

La nueva federación



Atributos

Recomendación (SHOULD)

(según la definición de la RFC 2119)

Atributo	SIR	eduGAIN	Nueva federación
eduPersonTargetedID	✔ REC	✔ REC	✔ MUST R&S LS
eduPersonAffiliation	✔ REC	✔ REC	✔ REC
schacHomeOrganization	✔ REC	✔ REC	✔ REC
eduPersonEntitlement	✔ REC	-	✔ REC LS
schacPersonalUniqueCode	✔ REC	-	✔ REC
uid	☐ OPC	-	☐ OPC OpenID
mail	☐ OPC	-	☐ OPC R&S
displayName	-	✔ REC	✔ REC R&S
commonName	-	✔ REC	✔ REC
eduPersonScopedAffiliation	-	✔ REC	✔ REC R&S LS
eduPersonPrincipalName	-	✔ REC	✔ REC R&S
schacHomeOrganizationType	-	✔ REC	✔ REC

Conexión con eduGAIN

- eduGAIN reúne en la actualidad a 1128 SPs y 1081 IdPs, de federaciones de identidad de todo el mundo
- La nueva política y los nuevos requisitos de atributos permitirán que los IdPs sean compatibles con eduGAIN por defecto
- Los IdPs estarán por tanto en eduGAIN
  - ...salvo si no quieren, es decir, opt-out para IdPs
- Los SPs seguirán siendo Opt-In
- Servicio de descubrimiento para SPs eduGAIN

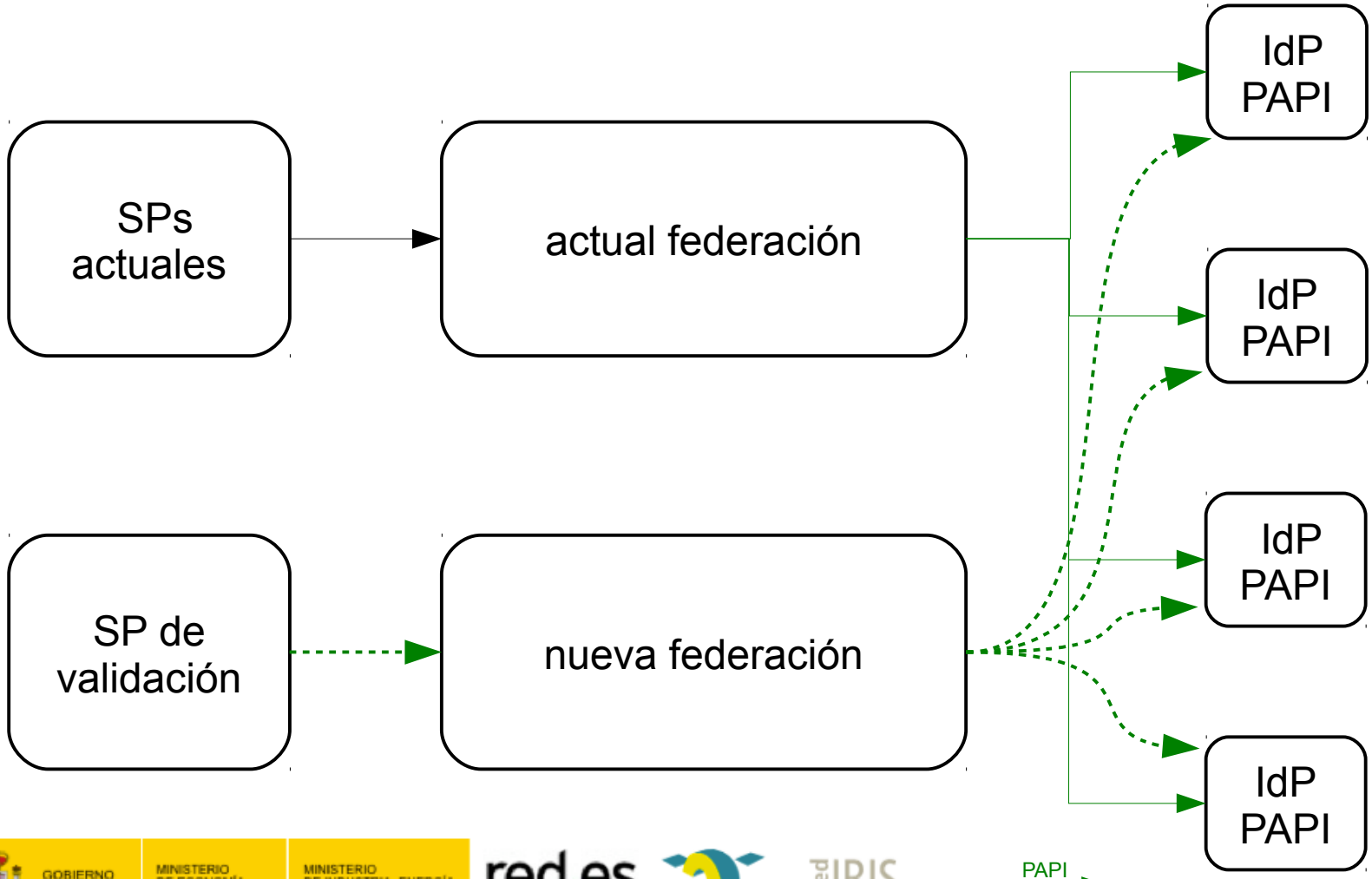
Nueva política y nuevo CUSO

- Se basará en el borrador de políticas definido a nivel europeo
- El nuevo CUSO será más sencillo:
  - por decidir si será genérico para SPs e IdPs
  - remitirá al documento de política
  - incluirá la no pertenencia a eduGAIN como opción
  - podrá ser firmado y entregado digitalmente
- Los borradores estarán en los próximos meses

¿cómo será la transición a la nueva federación?

Fase 1. Conexión IdPs PAPI al nuevo hub y usar SP de validación.

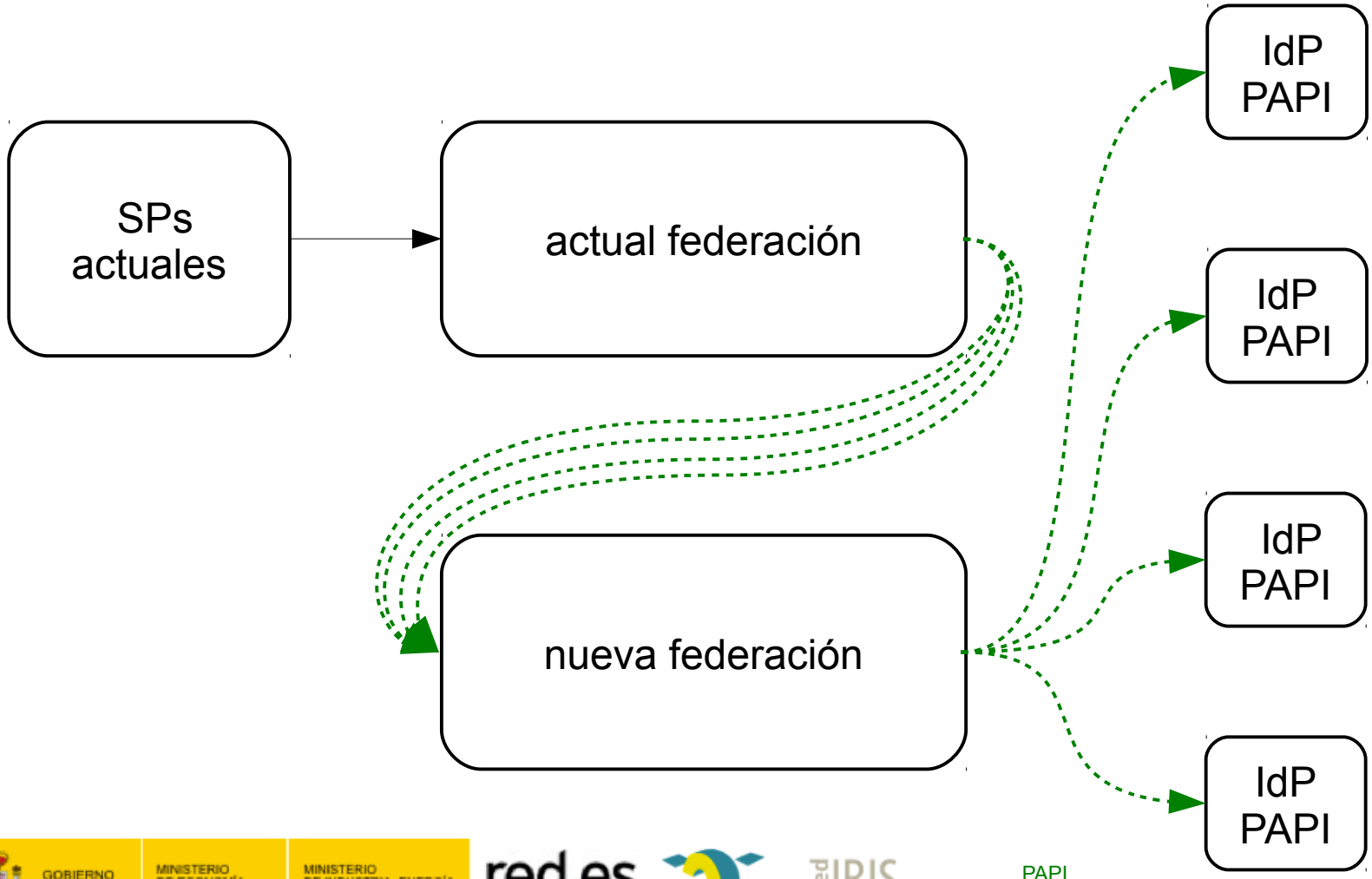
Fecha estimada: abril-mayo 2015



¿cómo será la transición a la nueva federación?

Fase 2. Se apuntan los IdPs PAPI actuales a entrada *wayfless* en el nuevo hub

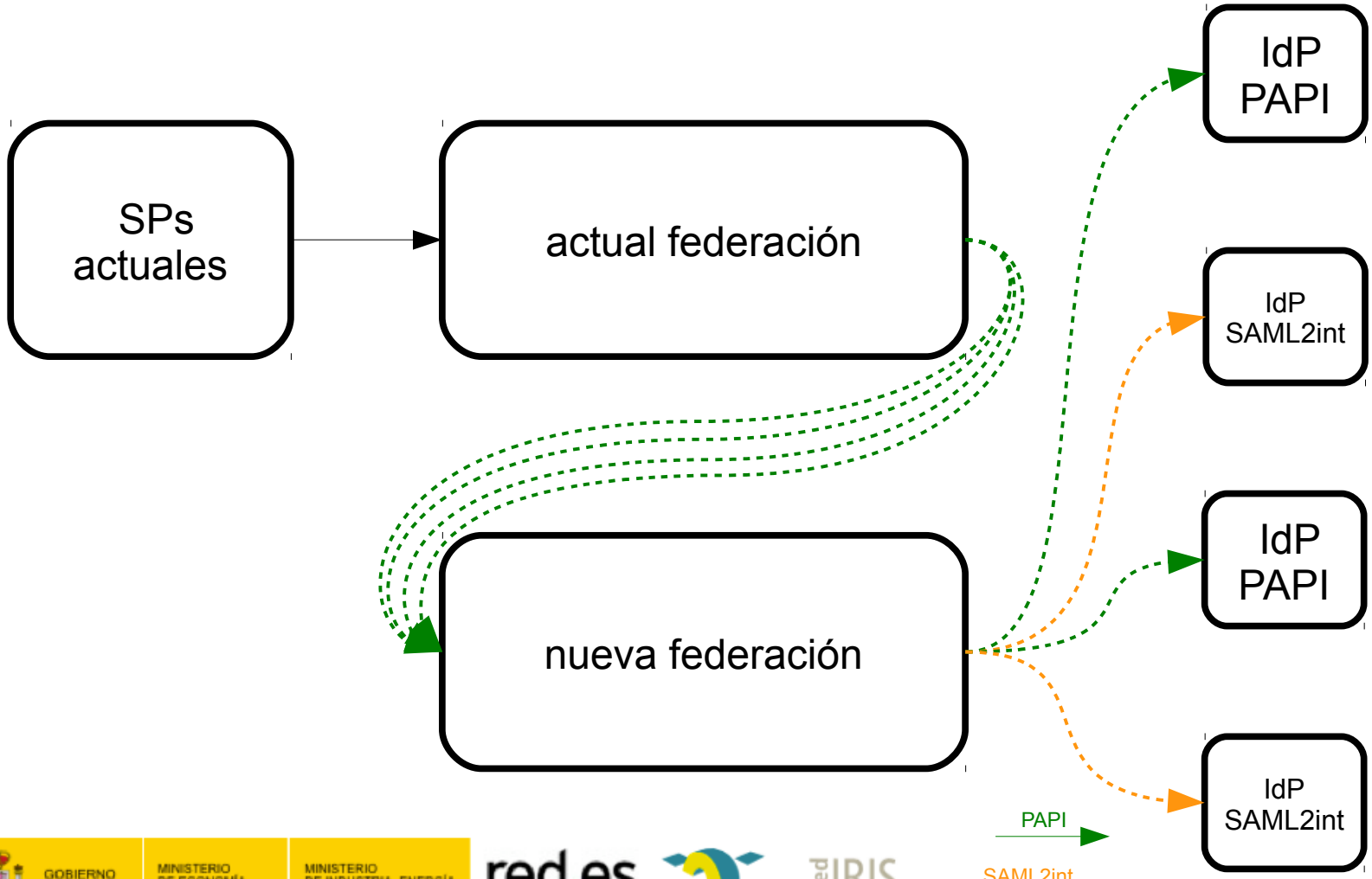
Fecha estimada: junio 2015



¿cómo será la transición a la nueva federación?

Fase 3. Migración de los IdPs PAPI a SAML2int

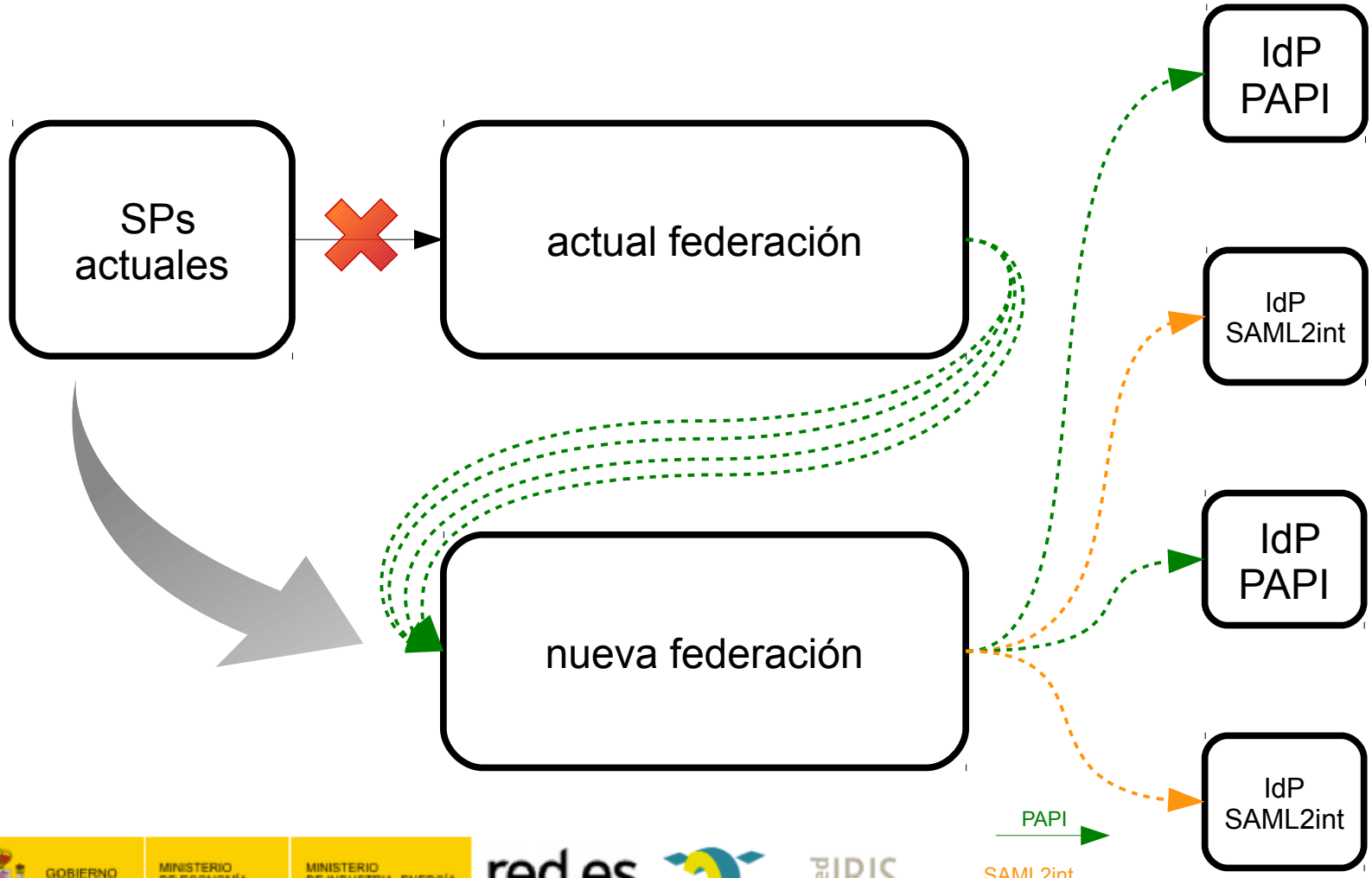
Fecha estimada: junio a noviembre 2015



¿cómo será la transición a la nueva federación?

Fase 4. Migración de los SPs a la nueva federación

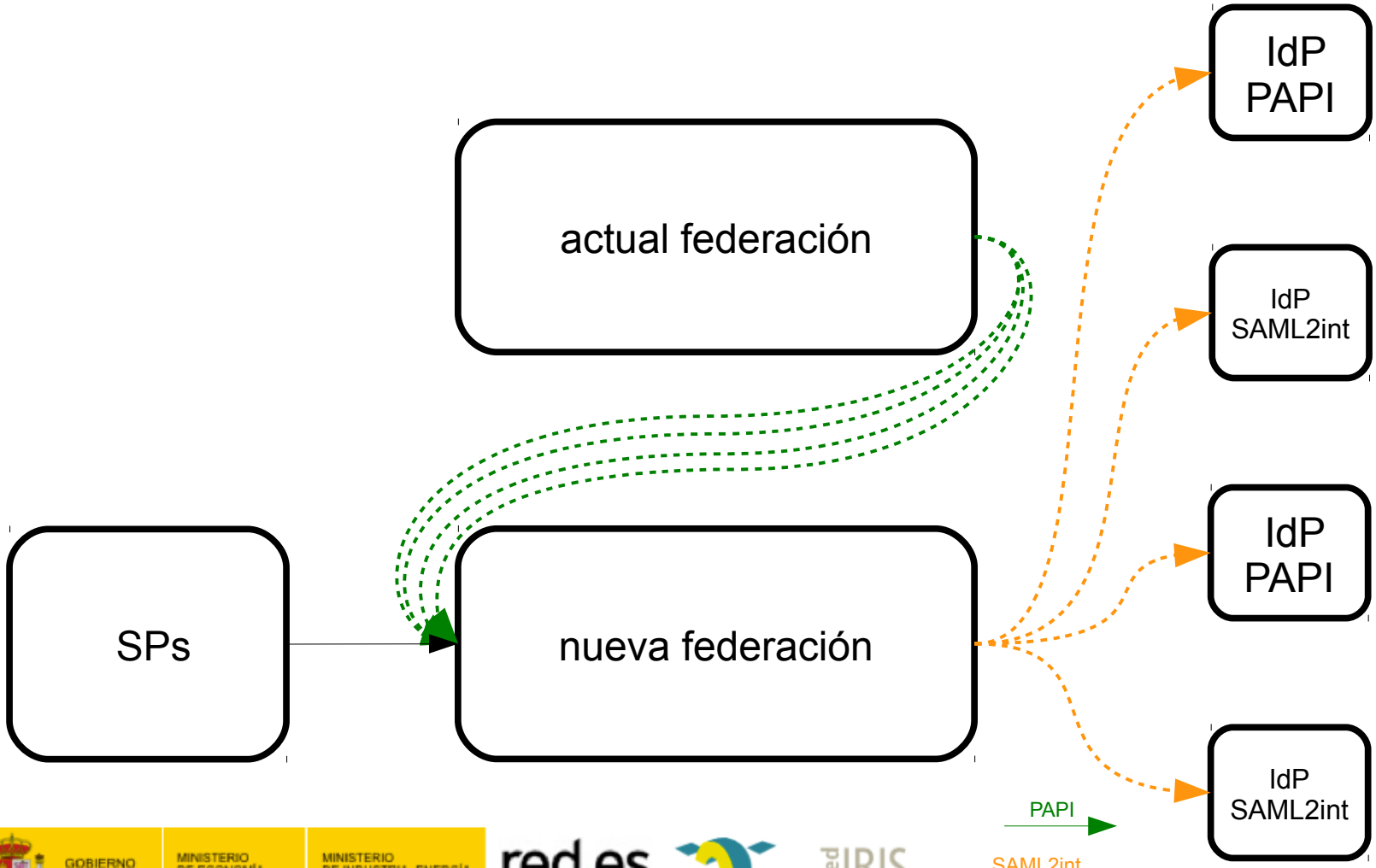
Fecha estimada: [junio] a [noviembre] 2015



¿cómo será la transición a la nueva federación?

Fase 5. apagado de la antigua federación

Fecha estimada: [noviembre] 2015



Resumen de fechas

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