Trabajo Fin de Carrera

Integración de un metasistema de identidad en la arquitectura eduroam para proporcionar un servicio de inicio de sesión único unificado

Universidad de Alcalá

Samuel Muñoz Hidalgo

2010

Desarrollo de la exposición

- Necesidades
- Problemas
- Solución propuesta
- Metasistema
- Implementación
- Conclusiones
- Preguntas

Servicios

- Sociedad de la información.
- Servicio:
  - Según la RAE:
    prestación humana que satisface alguna necesidad social y que no consiste en la producción de bienes materiales.
  - Automatización.
  - Recursos.

Identidad digital

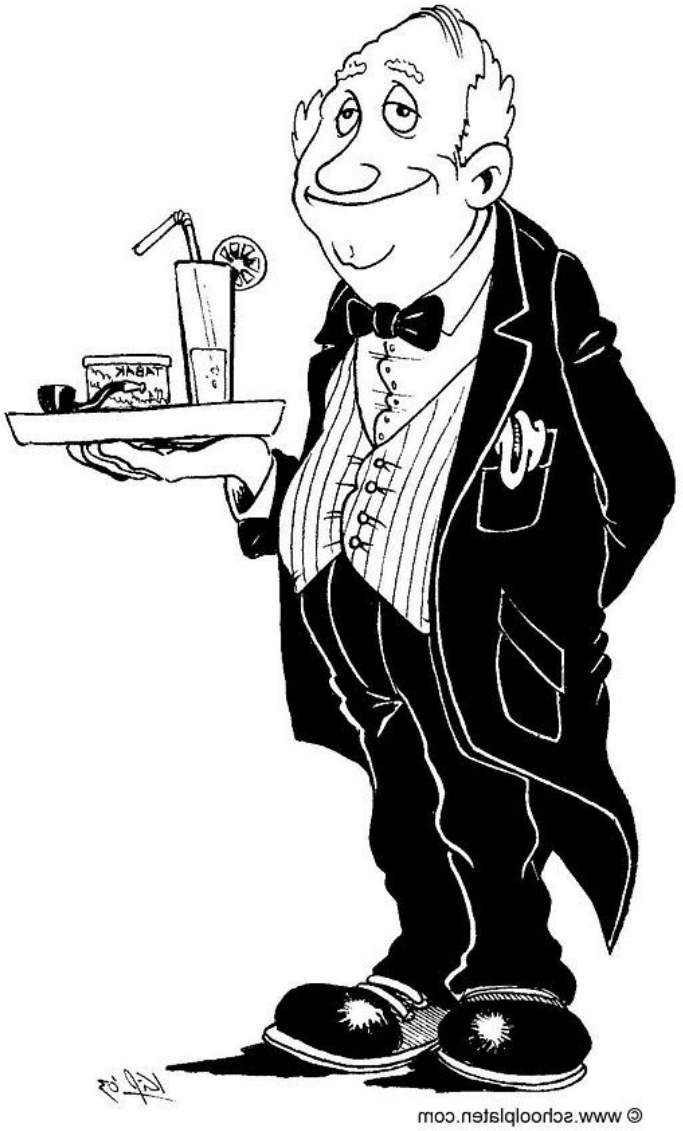
- Características y atributos asociados a un perfil.
- Una persona... ¡varias identidades!
- Privacidad, control sobre los datos.
  - Identidad centrada en el usuario.

Necesidades globales

- Seguridad
  - La base de las relaciones es la confianza.
  - Identificación / autenticación
- Recursos
  - ¿Quién suministra los datos?
  - ¿Dónde se almacenan?

Proveedor

- Autenticación
- Arquitectura sencilla
- Sistema escalable
- ¿Necesita almacenar datos?
  - ¿Cuáles?
  - ¿Para qué?
  - ¡¡LOPD!!



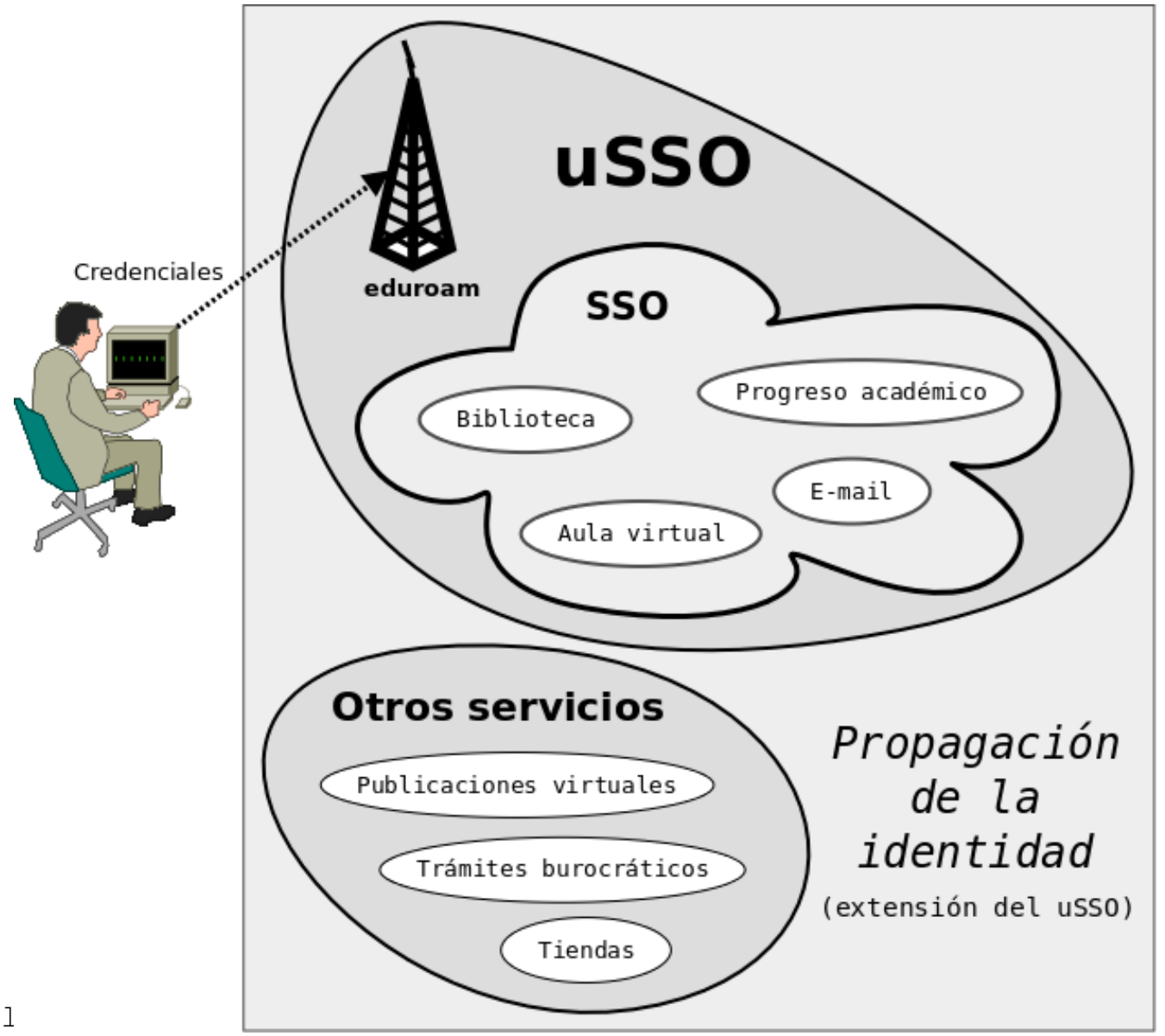
Usuario

- Rapidez
- Sencillez
- Eficacia
- ¡¡¡USABILIDAD!!!

Panorama actual

- Pluralidad de tecnologías
  - Métodos de autenticación.
  - Representación de la identidad.
- Multitud de servicios
  - Fatiga por contraseñas.
- Recursos
  - Federar servicios es una tarea compleja.

Solución ideal

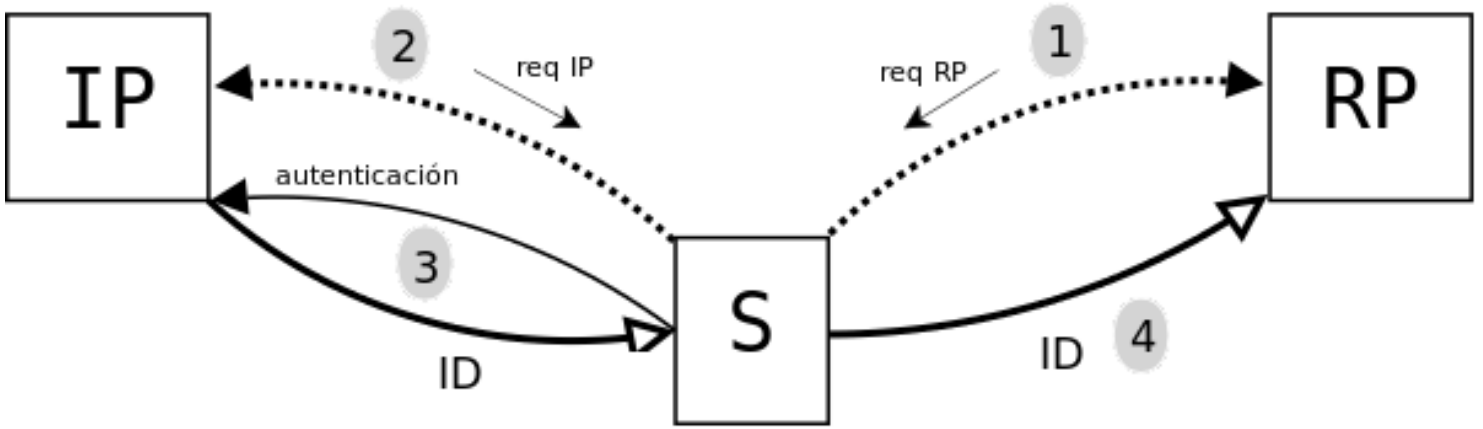


Herramientas

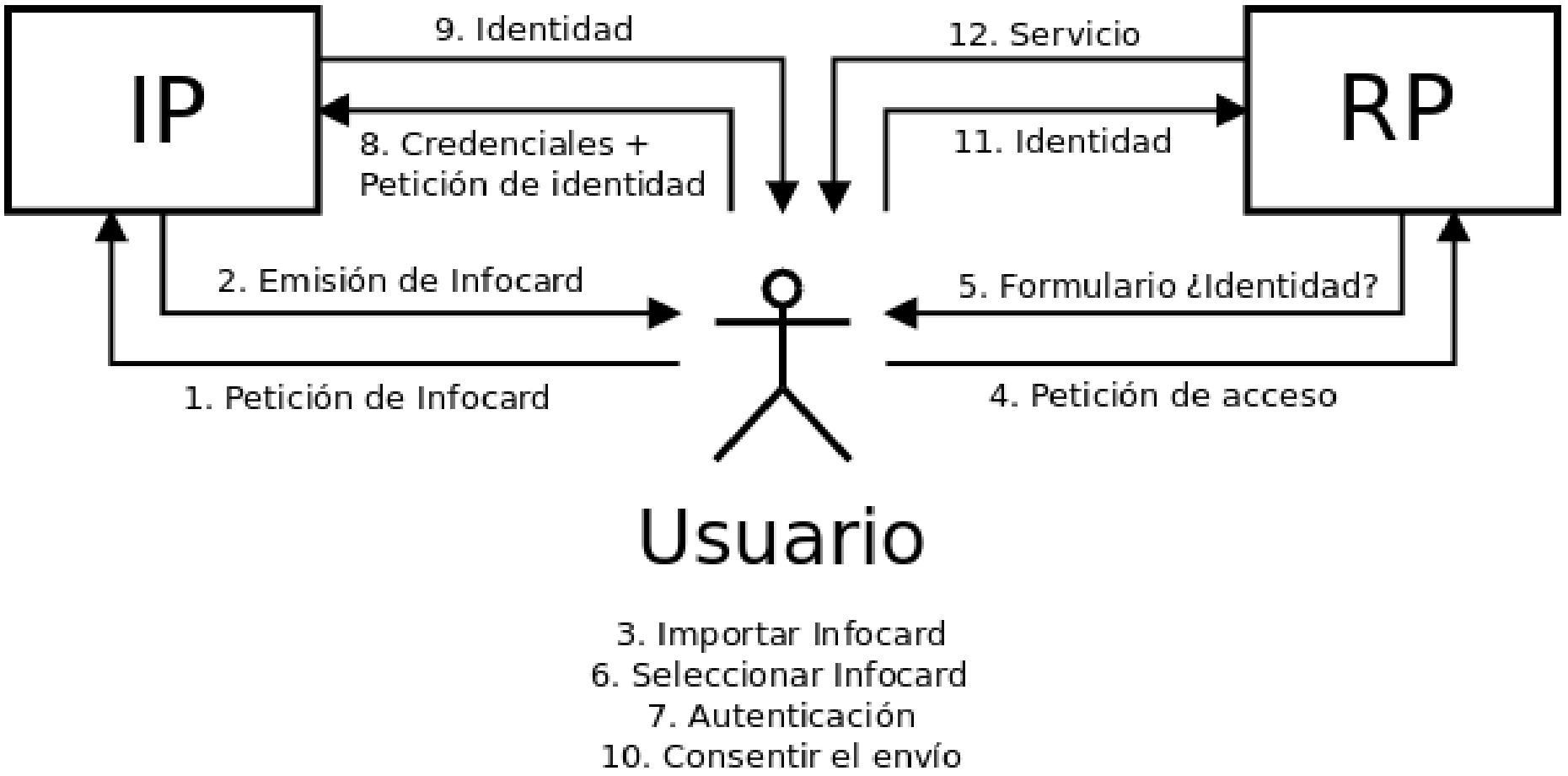
- 7 leyes de la identidad digital
- Servicios Web
- SAML
- InfoCards
- eduroam

Metasistema de identidad

- ¿Qué es?
- Roles:
  - Proveedor de identidad (IP)
  - Consumidor de identidad (RP)
  - Usuario (selector de identidad)



Caso práctico InfoCard

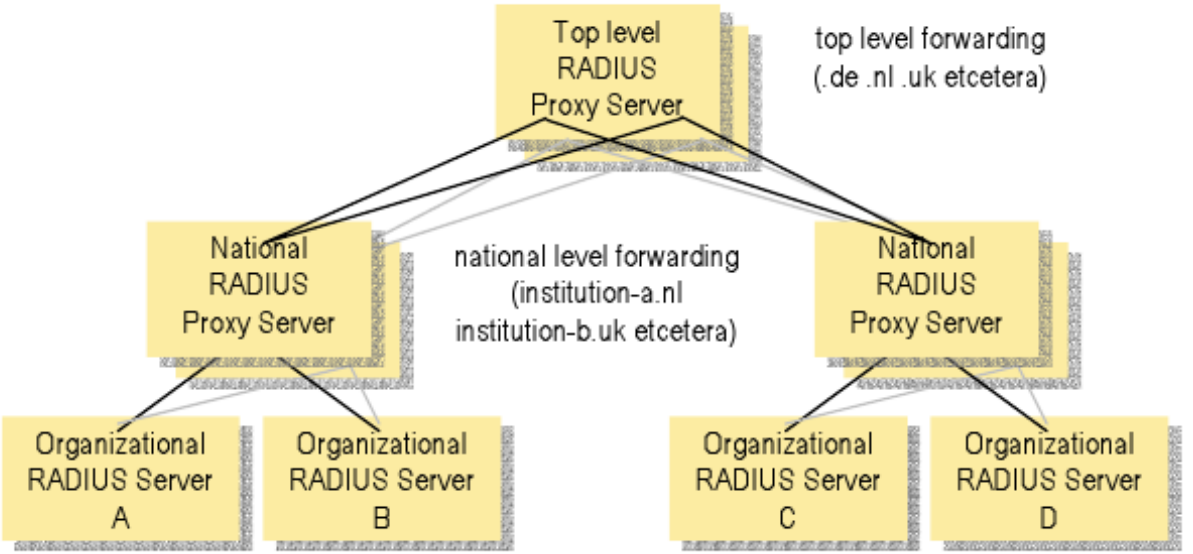


Consideraciones InfoCard

- Automatización de la autenticación
- Tipos de tarjeta
  - Autoemitida
    - Formularios
    - Seguridad no prioritaria
  - Gestionada
- Métodos de autenticación
  - Usuario/contraseña
  - Smartcards, certificados, e-DNI
  - Tarjeta autoemitida (CardId+claves RSA)

eduroam

- “Abre tu portatil y conéctate”
- Red universitaria
- Confederación
- Ventajas e inconvenientes
- Jerarquía



simpleSAMLphp + InfoCard

- simpleSAMLphp
  - SSO (Web)

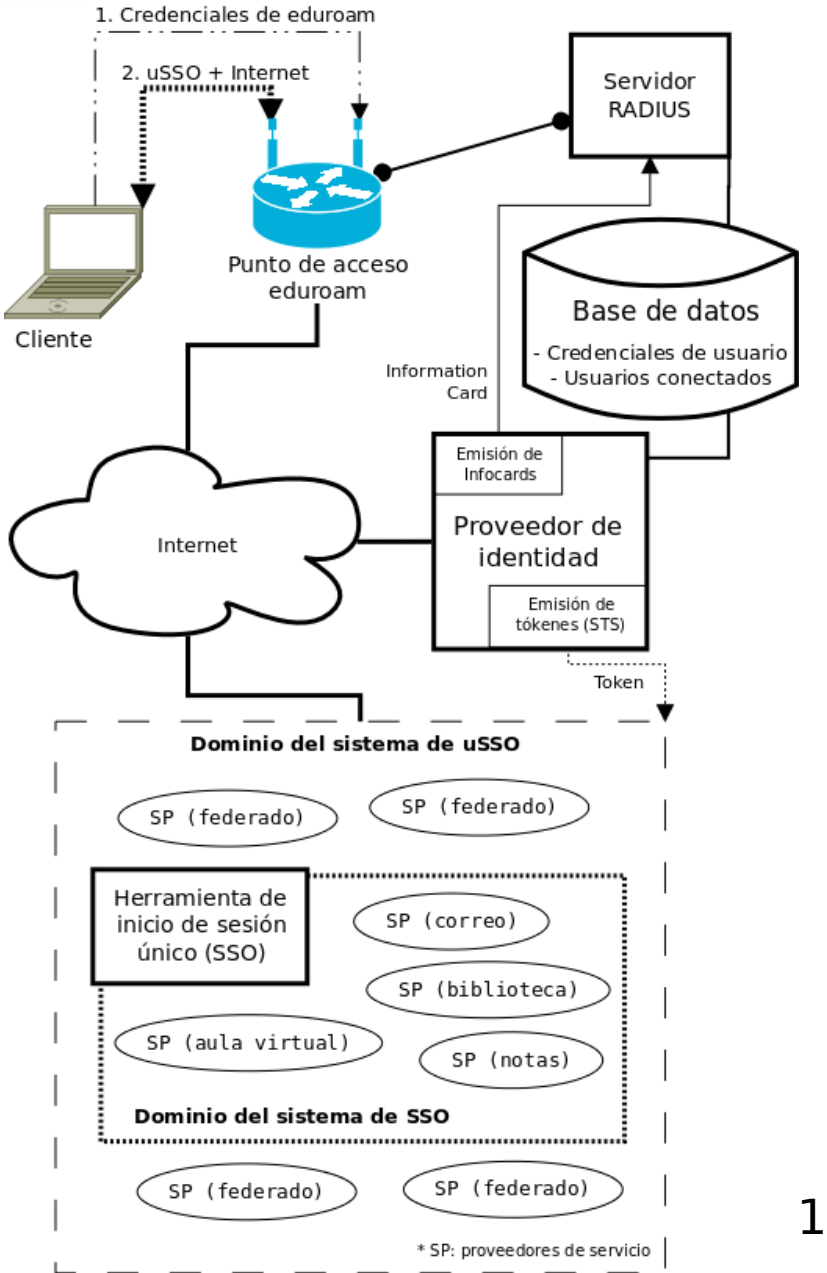
- Módulo InfoCard
  - Fuente de autenticación
  - Generador de tarjetas
  - Proveedor de identidad
  - Intercambio de metadatos (MEX)

Juntando todo

- Tipo de autenticación
  - Credencial autoemitida. ¿Seguridad?
- Objetivo: conectar a eduroam
  - uSSO
  - PEAP
- Cómo fluye por el sistema eduroam
  - Se envía un CardId.
    - PPID (unidireccional)
  - Se recibe una identidad digital.
    - Referencia. URL de un solo uso.

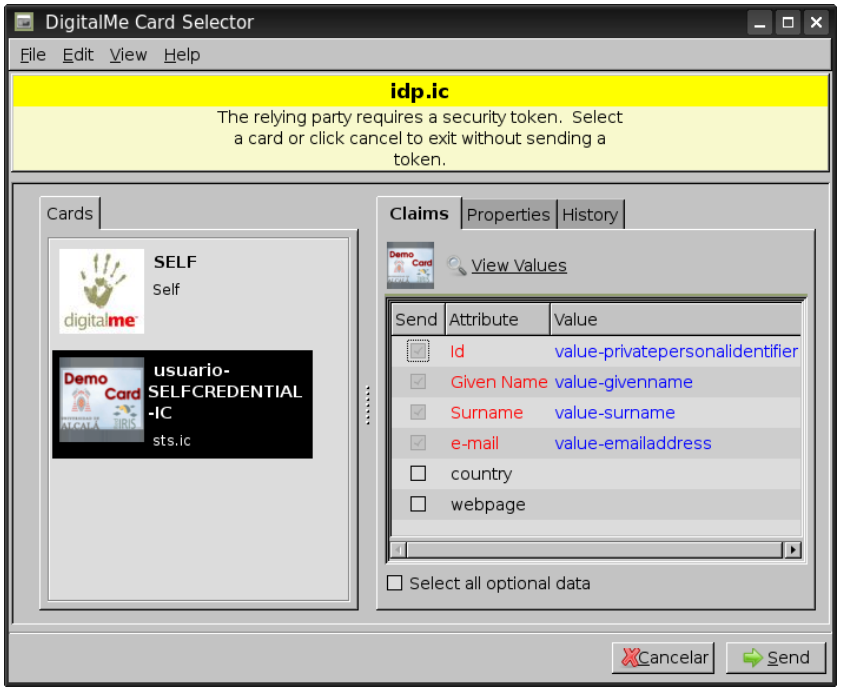
Arquitectura

- Metasistena
  - uSSO
- eduroam
  - conectividad
  - credenciales
- Herramienta de SSO
  - simpleSAMLphp
- BB.DD.
  - PostgreSQL



La máquina del usuario

- Suplicante
- Selector de identidad
- Conector (guión Perl)
  - Conexión con el selector de identidad
  - Gestión de certificados
  - Conexión con el suplicante



Caso de uso completo

- Lanzar conector
  - Verificación automática de certificados
- Seleccionar tarjeta autoemitida
  - O creación de la misma
- Conexión automática con eduroam
- Importar identidad digital
- Uso de la infocard para SSO
- Uso de la infocard para uSSO
  - No real pero automatizable

Conclusiones

- Seguridad
  - Comunicaciones TLS
  - XMLSEC (tarjetas y tókenes)
  - PPID (generación, envío, credencial+RSA)
- Problemas de eduroam
  - Desconexión y abuso
- Aceptación general
- Otros competidores: OpenID

Predicciones

- Desarrollo de librerías
- Necesidad de un selector de identidad
  - Multiplataforma (Android)
  - Extensible por complementos (OpenId, QR, ...)
  - Ejemplos de compras digitales
- Suplicante
  - Open1X
  - Comunicación con el selector (conector innecesario)

A posteriori

- Proyecto Moonshot
- Selector para OpenID
- Active Directory Federation Services 2.0
- e-DNI
- Toma de conciencia de privacidad en las redes sociales.

Contribuciones

- Módulo InfoCard para simpleSAMLphp
  - RP: consumir identidad
  - IP: generar tarjeta, generar token (STS), MEX
- Modificación en wpa_supplicant para el manejo de la identidad digital
  - TLV (SMH): CardId
  - URL de un solo uso.
- Conector
  - Usabilidad, cierre de la prueba de concepto.

Preguntas

- Preguntas
- Sugerencias
- Peticiones
- Ofertas