II Jornadas de Identidad Digital RedIRIS.
5 de octubre Cuenca 2011

DNIe
y fuentes adicionales de Identidad

Inmaculada Bravo
inma@usal.es

VNiVERSiDAD D SALAMANCA

Cándido Rodriguez
candido.rodriguez@prise.es

prise

DNIe y fuentes adicionales de identidad

1. Conceptos sobre E-Autenticación
2. Validación DNI-e
3. Problemática de usuarios adicionales
4. Autenticación delegada
5. Autorización - Niveles de confianza (LoA)
6. Conclusiones

Identidad Digital

- ¿Cuántas Id Digitales tiene un usuario?
- ¿Anonimas? ¿Reales?
- Tendencia a enlazar identidades
- Privacidad vs Redes Sociales

E-Autenticación

Proceso de Registro

- Autoridad de registro
- Almacen de credenciales
- Token

Proceso de Autenticación

- Verificador
- Aserción de usuario
- Relay Party

Proceso de Registro:

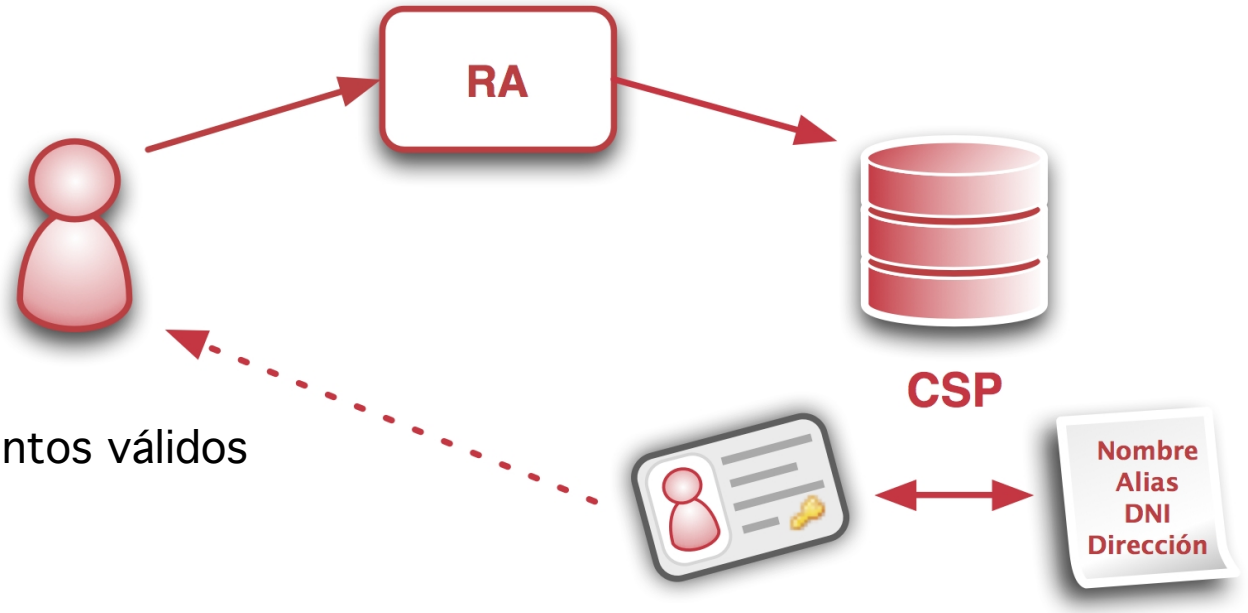
"Autoridad de Registro (RA)
Asegurar que la persona que se registra y recibe el token es quien dice ser y sus datos son correctos. Evitar repudio."

"Proveedor de Credenciales(CSP)
Asegurar la privacidad e integridad de los datos"

Proceso de registro:
- En persona
- Remoto

Validación de atributos:
- Confiar en el usuario
- Contrastarlos con documentos válidos

Proceso de entrega del Token:
- Depende del tipo de token

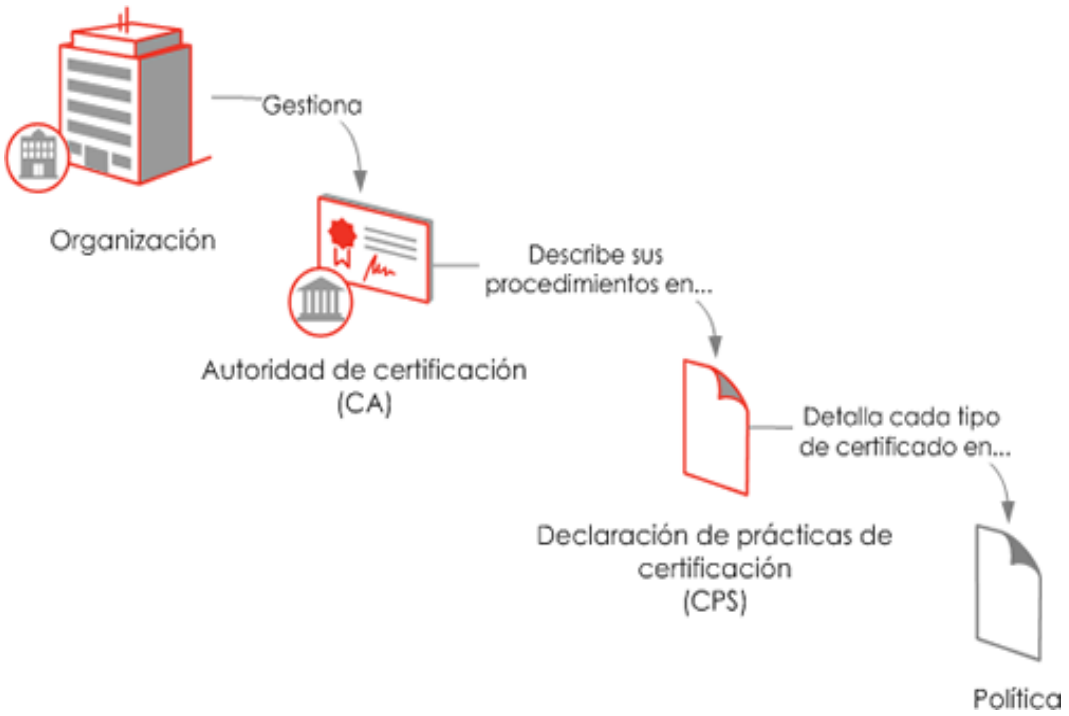


Proceso de Registro: Tipos de Token y Riesgos

Se basan en algo que...	Ejemplos	Amenazas
SABES	Pin o contraseña	Descubrimiento: · Ingeniería Social · **Keylogger** · **Fuerza bruta** · **Interceptados (Sniffer, Mitm...)** · **Acceder al CSP**
TIENES	Certificados: · Hardware · Software	Falseados Duplicados Robados
ERES	Huella digital, iris, reconocimiento facial, etc. (identificador biométrico)	Replicados

Proceso de Registro: Confiabilidad de los Certificados

- Criptografía asimétrica RSA: Clave pública + Clave privada
- Certificado Digital X.509: Clave pública y datos de identificación firmados por una CA
- Autoridad de Certificación (CA): Autoridad de confianza que emite y revoca certificados



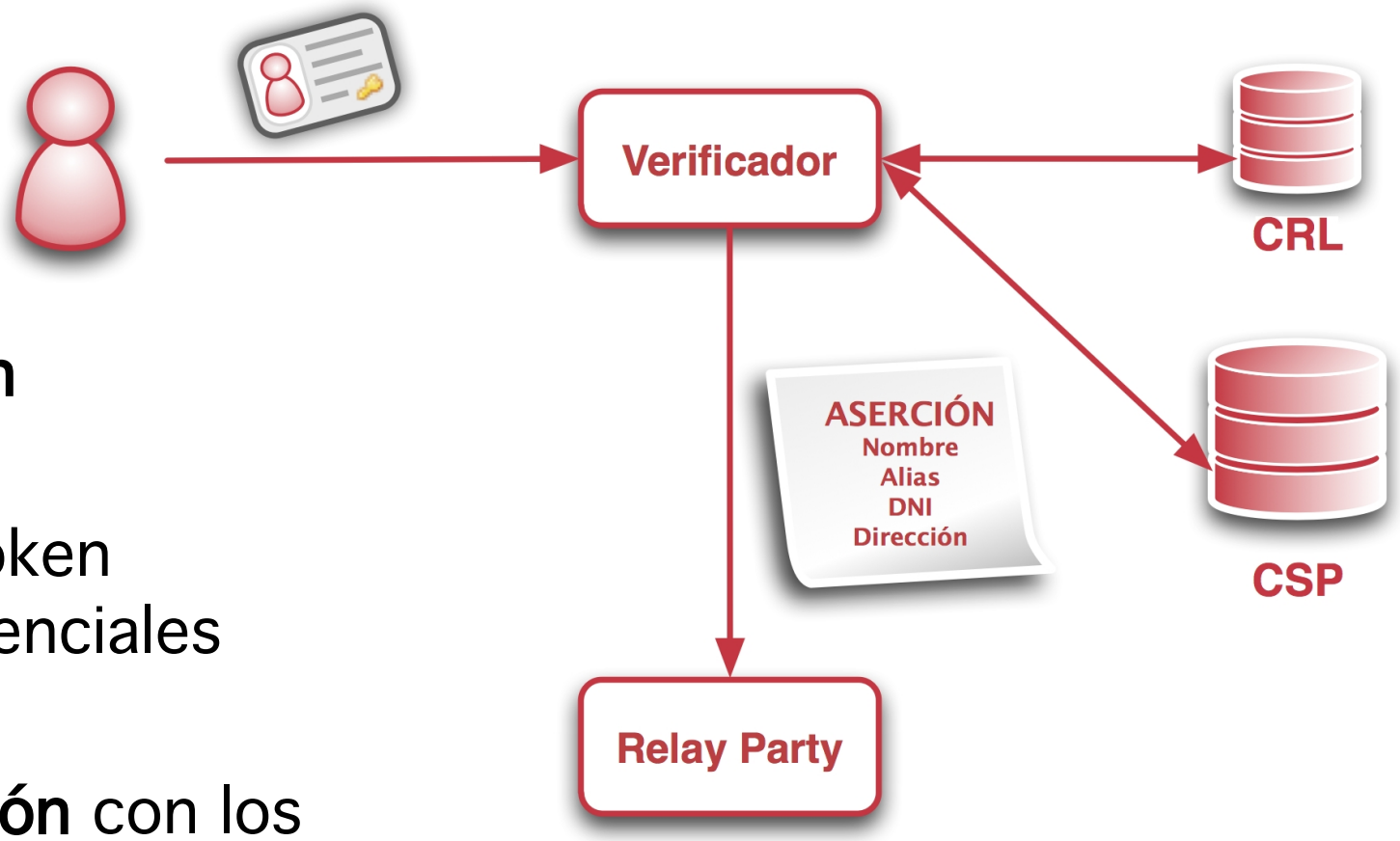
Política:

- **Algoritmo** de firma,
- **Longitud** de clave,
- **Soporte** del **certificado**,
- Proceso de **emisión** del certificado:
  - Si requiere de **presencia física**
  - Si requiere de algún tipo de **documento** de identificación
- **Acceso público** a **CRL**
- **...**

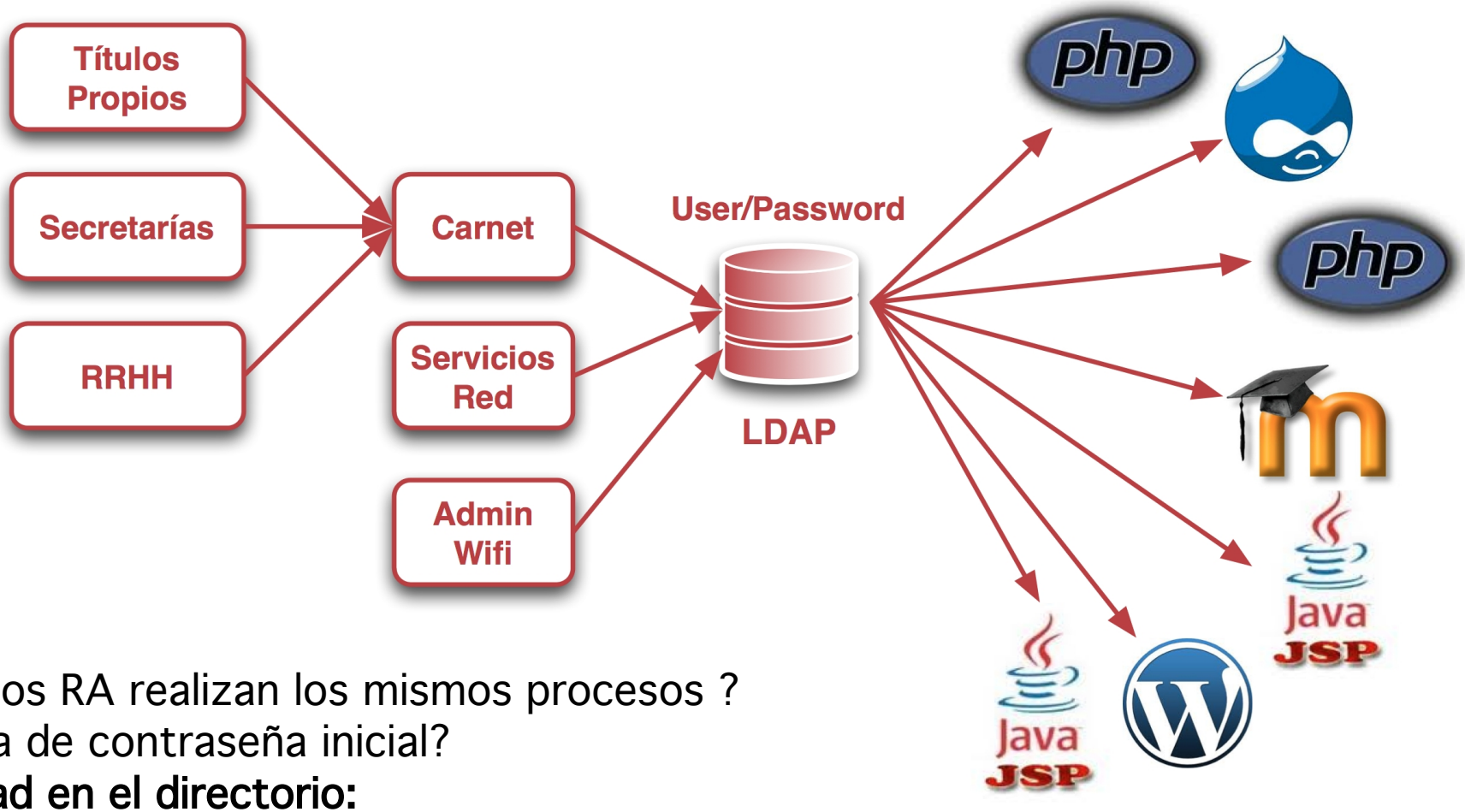
No todas las CA son iguales de confiables y seguras

Proceso de Autenticación

- El usuario **prueba** que conoce o posee el **token**
- El verificador **comprueba** el token y recupera credenciales del CSP
- Envia una **aserción** con los datos del usuario al RP
- El RP **permite** al usuario **acceder** a sus servicios

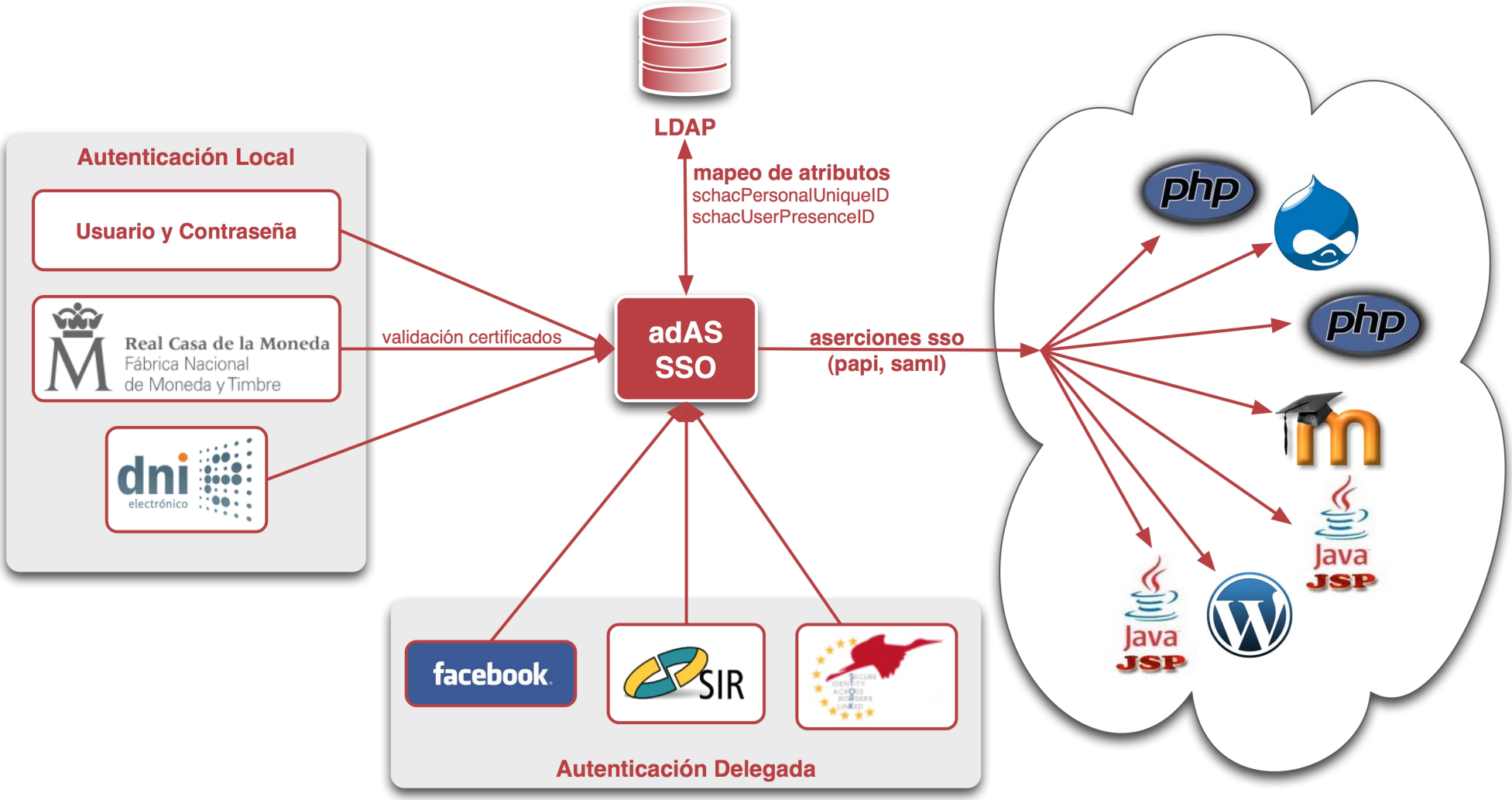


Estado inicial USAL



- ¿Todos los RA realizan los mismos procesos ?
- ¿Entrega de contraseña inicial?
- **Seguridad en el directorio:**
  - ¿Se almacena cifrada con algoritmos seguros?
  - ¿Política de contraseñas?
  - ¿Bloqueos por logins fallidos?

Objetivo en la USAL



Niveles de confianza → Autorización!!

DNIe y fuentes adicionales de identidad

1. Conceptos sobre E-Autenticación
2. **Validación DNI-e**
3. Problemática de usuarios adicionales
4. Autenticación delegada
5. Autorización - Niveles de confianza (LoA)
6. Conclusiones

Validación DNI-e

Problemática de usuarios adicionales:

- Alumnos Selectividad
- Ciudadanos que se autentican correctamente con su DNI pero no son usuarios usal

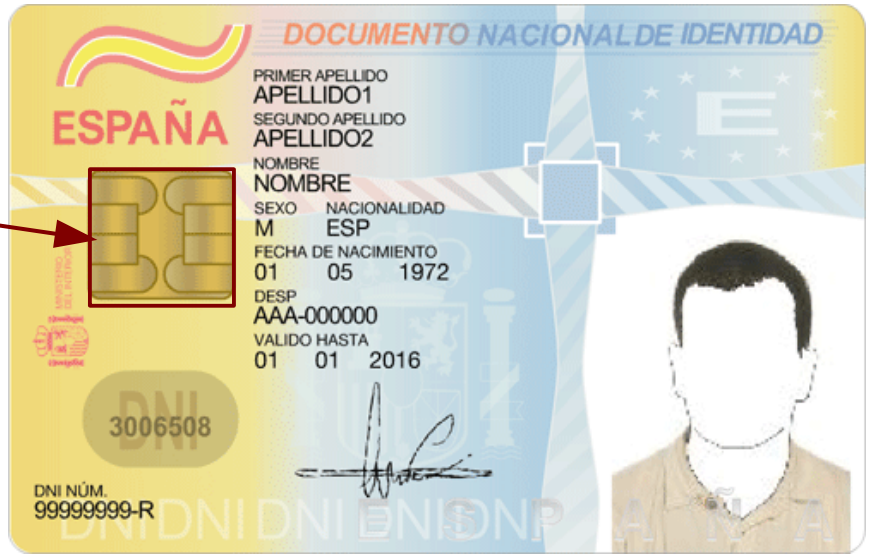
Servicios que podrían requerir generar nuevos registros con usuarios autenticados pero no son miembros

Presentación DNI-e

El DNI está compuesto de:

Tarjeta física

Chip DNIe



Presentación DNI-e

Nosotros nos interesamos por el Chip del DNIe

- CHIP criptográfico
- Capaz de **almacenar** certificados, foto, datos de filiación etc...
- Posee un **sistema operativo propio** DNIe v1.1
- Realiza **operaciones criptográficas**

Presentación DNI-e

DNIe organiza los datos en tres zonas

Zona pública

Zona Privada

Zona de Seguridad

Presentación DNI-e

Zona Pública

- Se puede leer **sin restricciones**
- Contiene la **información** necesaria para establecer el **canal seguro**

- Certificado de la CA intermedia.
- Claves Diffie-Helman.
- Certificado x509 de componente, usado para autenticar la tarjeta del DNIe.

Presentación DNI-e

Zona Privada

- Se puede leer **sin restricciones** y está **protegida** por el **PIN**
- Contiene los certificados del ciudadano

- Certificado de firma electrónica
- Certificado de autenticación

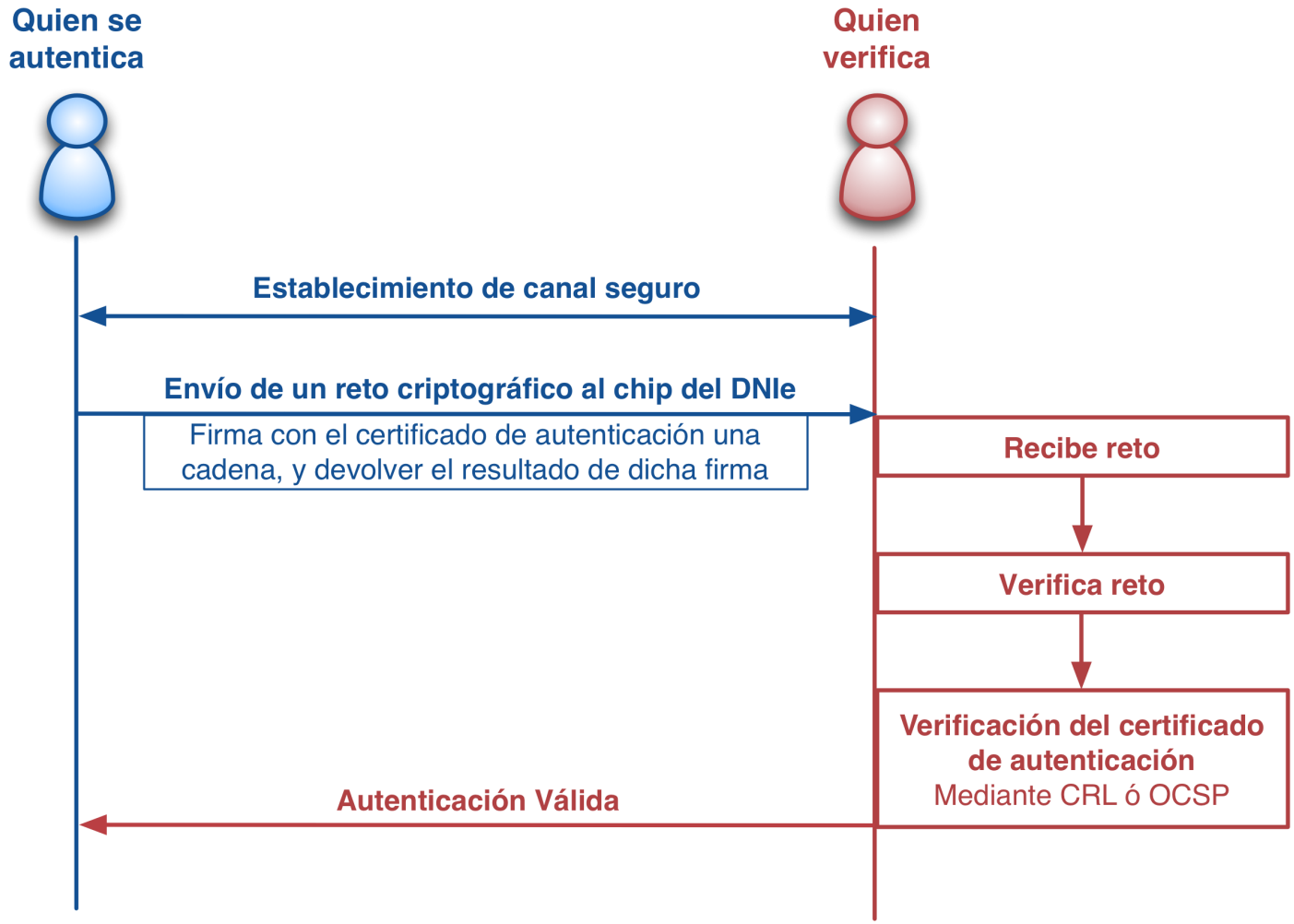
Presentación DNI-e

Zona de Seguridad

- Se puede **leer** pero solo desde los **puntos** de **actualización** del **DNIe**
- Contiene:
  - Datos de filiación del ciudadano
  - Imagen fotográfica
  - Firma manuscrita

Autenticación mediante DNI-e

La autenticación con DNIe/x509 consiste en



Autenticación mediante DNI-e

Valor añadido de esta autenticación

- Seguridad dispositivo hardware
- Más confiable que identificar mediante DNI físico

¿ Quién de nosotros sabe distinguir "a simple vista" un DNI falso ?

Autenticación mediante DNI-e

Pero ...

Esta seguridad la ofrecen otros token criptográficos

Entonces ...

¿ Dónde está el valor añadido ?

Autenticación mediante DNI-e

Valor añadido de esta autenticación reside en ...

- Nivel **muy alto** de confianza
  - No sólo por el token seguro
  - Sino por el emisor del certificado

Al estar emitido el certificado por la DGP, estamos depositando la confianza de la identificación inicial del sujeto en la misma DGP

Dificultades de uso del DNI-e

Difusión del DNI-e

El DNI-e lo tenemos casi todos

Pero ¿y los lectores? ¿Están igualmente difundidos?

Mejor no hablo de los drivers...

Si restringimos el acceso a autenticaciones mediante DNIe podemos dejar fuera a parte de nuestros usuarios

Dificultades de uso del DNI-e

Dificultad de uso

- Para el usuario que desea autenticarse
  - Buscar driver, instalarlos
  - En algunos ss.oo misión casi imposible
- Para los desarrolladores
  - Pruebas en todas las plataformas
  - Poca información técnica de sobre desarrollo
  - Ejemplos incompletos, sólo pruebas de concepto
  - Problemas con las versiones de las librerías dinámicas

Dificultades de uso del DNI-e

Educación del usuario

- Población tecnológicamente activa
  - Saben que es un certificado digital
  - Autenticación como ciudadano o usuario de un servicio
- Población tecnológicamente NO activa
  - Dejarán el DNIe y el PIN a sus familiares/amigos
  - Mejor no lo pensamos

DNIe y fuentes adicionales de identidad

1. Conceptos sobre E-Autenticación
2. Validación DNI-e
3. **Problemática de usuarios adicionales**
4. Autenticación delegada
5. Autorización - Niveles de confianza (LoA)
6. Conclusiones

Usuarios Adicionales

Casos de uso

Inscripción en oposiciones

Usuarios servicios deportivos

Nuevas matrículas

Usuarios selectividad

¿Se os ocurre algún otro?

Usuarios Adicionales

¿Cómo **modelar** estos casos de uso?

¿Cuál es el **impacto** en nuestro SSO?

DNIe y fuentes adicionales de identidad

1. Conceptos sobre E-Autenticación
2. Validación DNI-e
3. Problemática de usuarios adicionales
4. **Autenticación delegada**
5. Autorización - Niveles de confianza (LoA)
6. Conclusiones

Autenticación Delegada

División de la autenticación en dos fases:

- Identificación

  Petición de autenticación a una entidad externa

- Autenticación Local

  Autenticación en base a la información recibida

Alcance

Usuarios propios y externos

Autenticación Delegada

Motivación

Consumo de métodos de autenticación de terceras partes

Reducción complejidad técnica del IdP

Usuarios externos en nuestras aplicaciones

Métodos de autenticación preferibles por los usuarios

Autenticación Delegada

AuthN Delegada vs Federación

IdP

Conocimiento de atributos recibidos

Conjunto de Sps e IdPs

Metadatos

Políticas de acceso al servicio

Políticas de atributos comunes

Autenticación Delegada

¿Cuándo una AuthN Delegada?

Aplicación **pertenece** a **nuestra** organización

Acceso usuarios de nuestra organización (pero también externos bajo condiciones)

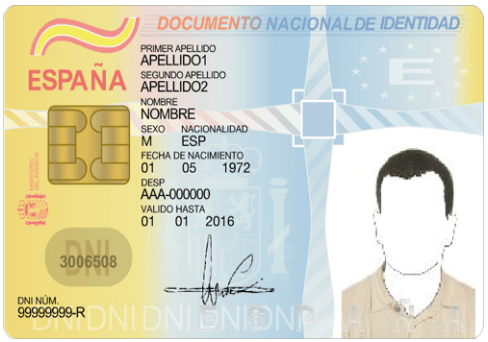
¿Cuándo una Federación?

Aplicación **no pertenece** a un IdP

Se ofrece indistintamente a uno o más IdPs

Autenticación Delegada

Usuarios con identidad digital en nuestra institución



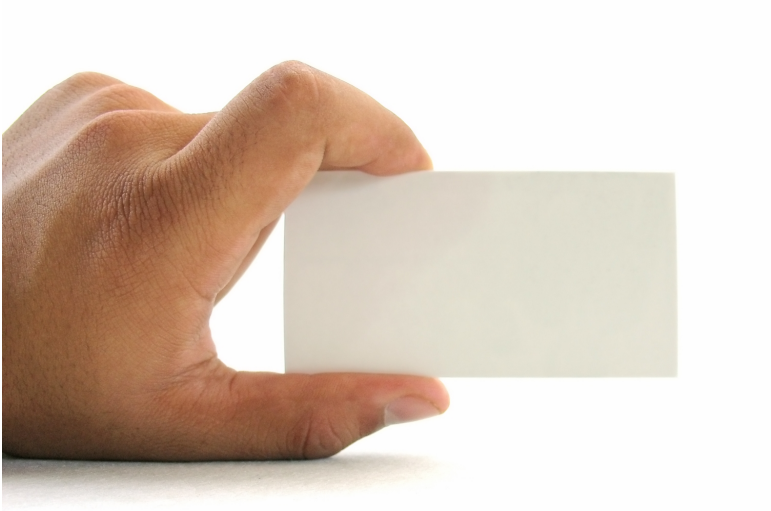
- Casos de uso:
  - Erasmus
  - Intercambio de investigadores
  - Otros métodos de autenticación (Facebook, Gmail,...)

Autenticación local

Si existe ese usuario en nuestro entorno

Autenticación Delegada

Usuarios **SIN** identidad digital en nuestra institución



- Casos de uso:
  - Alumnos/investigadores/etc invitados en un congreso
  - Usuarios de Facebook.

Autenticación local

Aunque no exista se le crea un contexto en el SSO

Autenticación Delegada en ADAS

advanced Authentication Server

Módulos PAPI

Cualquier institución que use PAPI o sea de SIR

Módulos SAML2

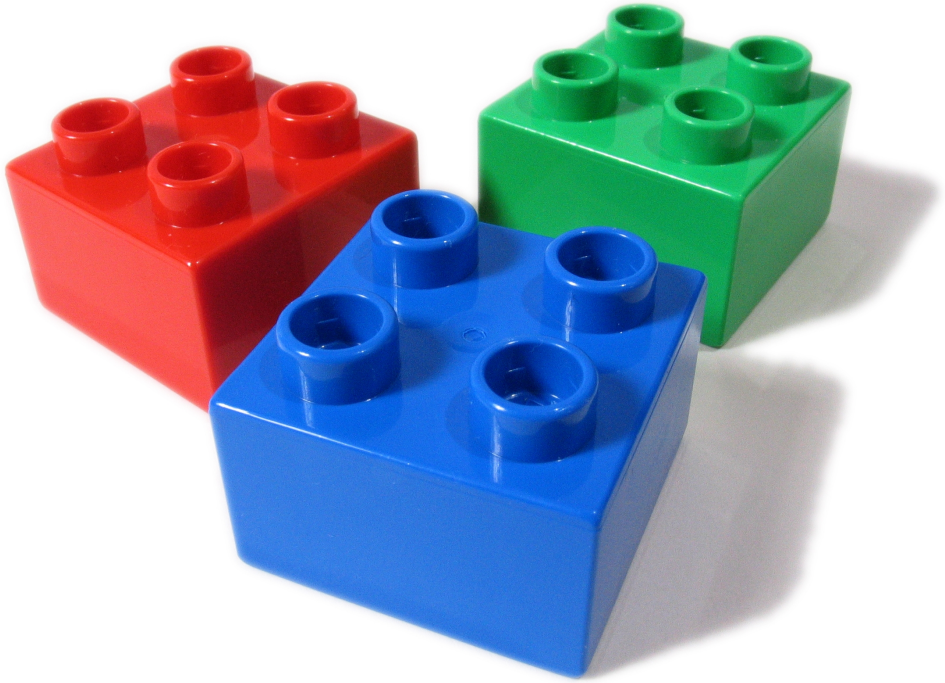
Cualquier institución que use SAML2 o sea de SIR

Módulos Facebook

Autenticación Delegada en ADAS

advanced Authentication Server

Demo



Autenticación Delegada: WAYF

Inclusión de WAYF en el Proveedor de Identidad

- Utiliza la autenticación delegada
- Objetivo: **USABILIDAD**
- Usuario sabe si pertenece a la institución

Autenticación Delegada: WAYF

AuthN Delegada vs WAYF

AuthN delegada es para usuarios que son/están en la institución

WAYF es para usuarios que no son de la institución

AuthN Delegada: WAYF en ADAS

advanced Authentication Server

Podemos definir módulos de AuthN delegada para introducirlos en el WAYF

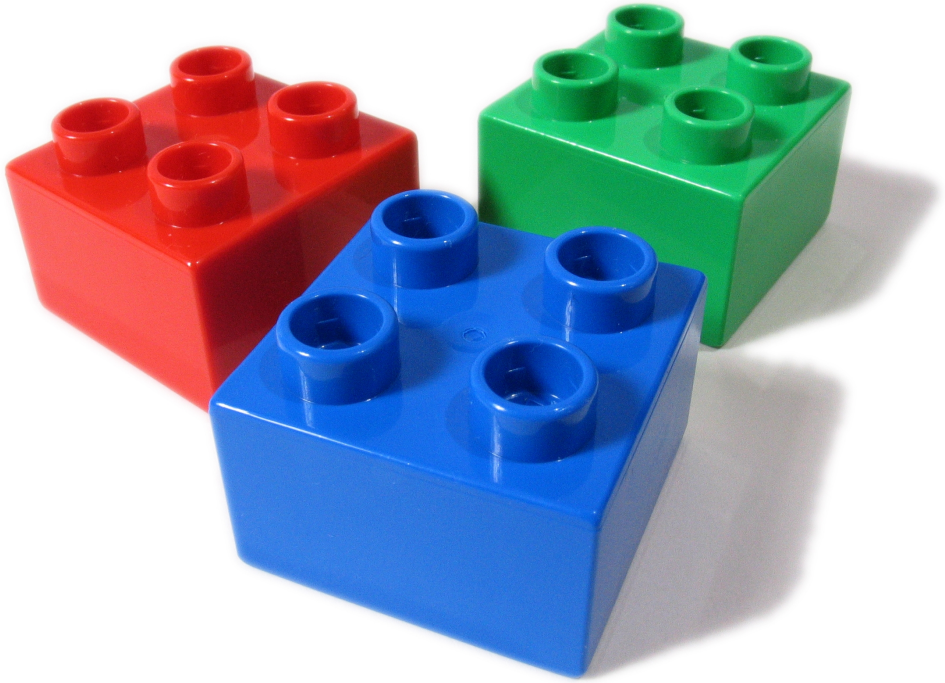
Podemos configurar Proveedores de Servicio que admitan WAYF:

WAYF para Sps determinados

AuthN Delegada: WAYF en ADAS

advanced Authentication Server

Demo



DNIe y fuentes adicionales de identidad

1. Conceptos sobre E-Autenticación
2. Validación DNI-e
3. Problemática de usuarios adicionales
4. Autenticación delegada
5. **Autorización - Niveles de confianza (LoA)**
6. Conclusiones

Autorización

“ *Level of Assurance (LoA)*
Nivel de confianza de un método de autenticación ”

Hay demasiadas formas de autenticación
(local + delegada)

1) Clasificación dependiendo del nivel de fiabilidad
2) Autenticaciones definen qué nivel cumplen
3) Aplicaciones requieren un nivel mínimo

LoAs: Guías

Existen guías que intentan cubrir todos los casos

¡ Podemos crear las nuestras !

National Institute of Standards and Technology
U.S. Department of Commerce

LoAs: Guías

Nivel	Confianza en la validez de la aserción
1	Pequeña o ninguna
2	Baja
3	Alta
4	Muy alta

Se aplican a:

- La Identidad de un usuario (Se autentica correctamente)
- Los Atributos que se emiten del mismo (Una vez autenticado podemos validar la aserción que se emite)

Definiciones abstractas, no tienen formas de uso concretas

LoAs: Guías

Utilizan niveles del NIST (1 – 4)
Relacionan impacto errores de autenticación con niveles de confianza

Potencial impacto de un error de autenticación	Niveles de Confianza			
	1	2	3	4
Daño en prestigio/reputación	Minimo	Moderado	Sustancial	Alto
Pérdidas financieras	Minimo	Moderado	Sustancial	Alto
Daño a gobiernos o intereses públicos		Minimo	Moderado	Alto
Riesgo de emisión de datos sensibles		Moderado	Sustancial	Alto
Seguridad personal			Minimo	Alto Sustancial
Actos criminales o violación derechos civiles		Minimo	Sustancial	Alto

LoAs: Definiciones de ejemplo

Nivel	Ejemplos de módulos de autenticación	Ejemplo de acceso aplicaciones
1	Facebook	Blog, Mercatus, actividades culturales, symposium, ...
2	Usuario / Contraseña	Correo, moodle, ...
3-4	FNMT, DNIe	Cambio de actas, administración de servicios críticos, ...

LoAs: Interoperabilidad

Son guías, no estándares

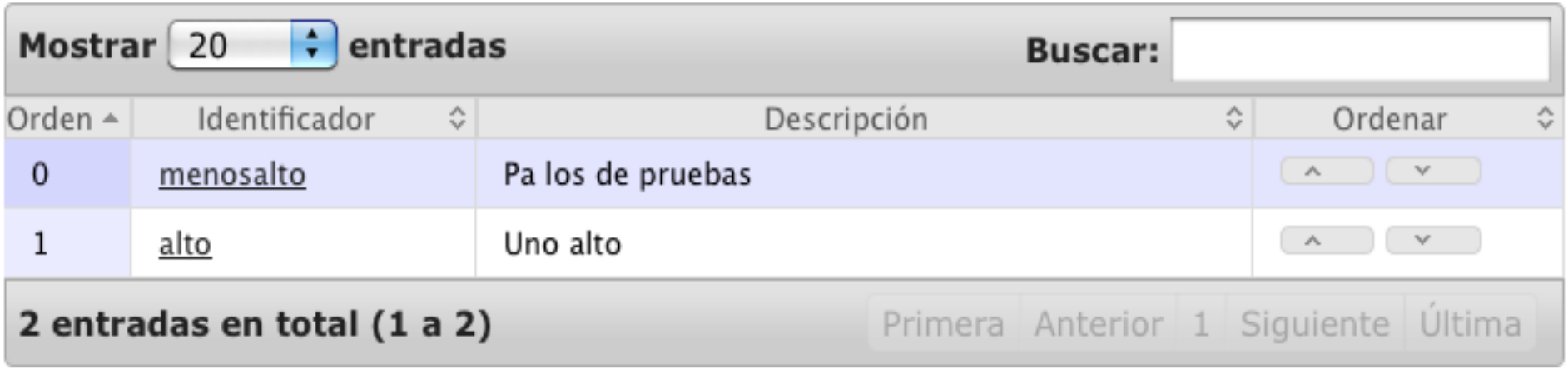
La confianza es muy subjetiva
(algo es muy confiable para un entorno,
no lo es para otro)

Tenemos que crear reglas para "convertir" las clasificaciones

LoA en ADAS

advanced Authentication Server

Editor de clasificaciones de LoA



LoA en ADAS

advanced Authentication Server

LoAs en módulos de autenticación

LoA en ADAS

advanced Authentication Server

LoAs en proveedores de servicio

Definición de los metadatos

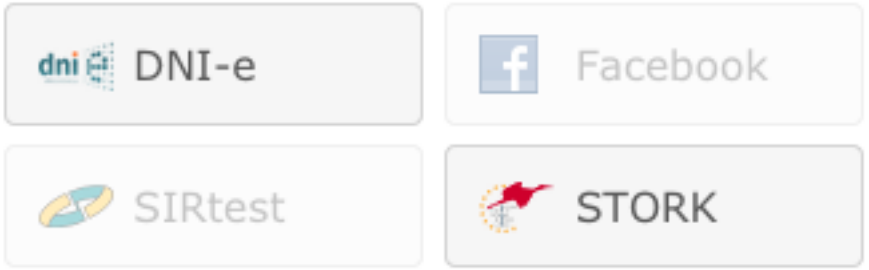
ID Entidad	http://proxy1.domain1.com
Protocolo	urn:mace:rediris.es:papi:protocol:1.0
Binding	urn:mace:rediris.es:papi:binding:browser-sso
Nivel de Confianza mínimo	LoA no definido *Nivel mínimo de confianza con el que se podrá autenticar un usuario en este SP.*
WAYF permitido	No *Indica si este Proveedor de Servicio mostrará al usuario un WAYF.*

LoA en ADAS

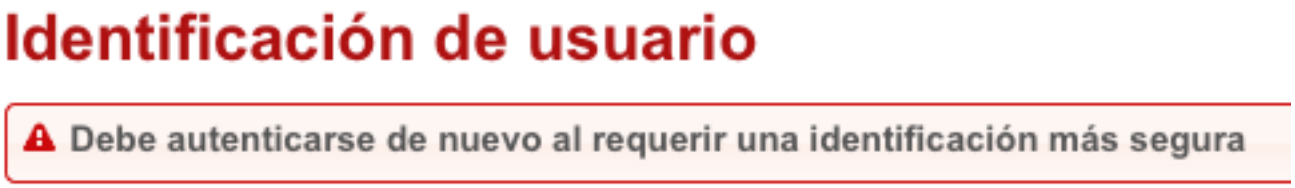
advanced Authentication Server

Página de Login => Objetivo: USABILIDAD

- Deshabilita métodos de autenticación que no cumplen LoA requerido



- Si está ya autenticado y LoA requerido es superior, requiere autenticación de nuevo



Autorización ¿IdP o SP?

IdP

Genera lista de atributos para el SP

Autoriza el envío

SP

Recibe atributos

Autoriza en función de ellos

Necesario para autorizar en zonas concretas

Autorización ¿IdP o SP? Problemática

La autorización es un proceso que complica el entorno

Coste de tiempo y personal

Mayoría de aplicaciones sólo se integran en el SSO con la autenticación

Moodle

Wordpress

...

Autorización ¿IdP o SP?
Gestión AuthZ en un SSO

Autorización en IdP

IdP emite atributo si tiene derechos de acceso

Reglas de autorización en los SP muy simples

Autorización en SP

Corte en el proceso de responder al SP si el usuario no cumple política

DNIe y fuentes adicionales de identidad

1. Conceptos sobre E-Autenticación
2. Validación DNI-e
3. Problemática de usuarios adicionales
4. Autenticación delegada
5. Autorización - Niveles de confianza (LoA)
6. **Conclusiones**

Conclusiones

A nuestro alcance...

- Federaciones no para todos los casos
- Incorporación de motor de autorización en adAS

Con cooperación de todos...

- ¿Cómo solventar problemas del DNI-e?
- Dar semántica común a los LoAs
- Definir LoAs Flexibles (Ej. Comodo)

¿preguntas?

Inmaculada Bravo
inma@usal.es

VNiVERSiDAD D SALAMANCA

Cándido Rodriguez
candido.rodriguez@prise.es

prise