Pasarela Cl@ve de RedIRIS: un enfoque dual

Francisco Aragó
Gabinet de Planificació i Prospectiva Tecnològica
Universitat Jaume I (Castellón)

Introducción

Proyecto de **RedIris** para la **CRUE:**

- Para emplear **Cl@ve como IdP**
- Para **mediar entre los SP universitarios** y el MINHAP
  - Simplifica la gestión de entidades.

¿Qué es Cl@ve?

- Unifica los métodos de autenticación de la Administración
  - **Cl@ve PIN** [PIN24H de la AEAT]
  - **Cl@ve Permanente** [Seguridad social]
  - **DNIe y certificados** [@Firma]
  - **Ciudadanos europeos** [STORK]

¿Qué es Cl@ve?

- Ventajas:
  - **Autenticación única** para el ciudadano
  - Interfaz única y estándar de acceso
  - **Integración sencilla**
  - Mantenimiento delegado

- **Solución técnica: basada en STORK**

STORK

- Dos LSPs financiados por la CE (entre 2008 y 2015)
- Diseñar y pilotar una **infraestructura de autenticación** y autorización pan-europea.
- Necesidades funcionales y legales muy específicas.
- Genera un **perfil SAML extendido**

El perfil SAML-STORK

- **Perfil de atributos** propio.
- **Metadatos no estándar** (y el SP no genera).
- **Firma** de tokens obligatoria.
- Binding **HTTP-POST**.
- **SLO no estándar.**

El perfil SAML-STORK

- **No emplea el name ID** (ID por atributo).
- Identificador de entidad (**providerName** en vez de issuer).
- Extiende el protocolo SAML
  - **Lista de atributos en la AuthnReq**
  - Nivel de calidad en la autenticación (**QAA**)
  - Otros

El perfil Cl@ve

- Operaciones
  - **Single Sign On** (HTTP-POST, firmada)
  - **Single Log Out** (SP-initiated)

- **Atributos** soportados (basado en STORK):
  - eIdentifier
  - givenName
  - Surname
  - inheritedFamilyName
  - adoptedFamilyName
  - citizenQAAlevel
  - afirmaResponse
  - isdnie
  - registerType

El perfil Cl@ve

- **Nivel de autenticación QAA** (2-4)
  - 2 → PIN24H, Clave GISS
  - 3 → Clave GISS + SMS, @firma (certificados SW)
  - 4 → @firma (DNIe y certificados HW)
- **Personalizar el selector de autenticación** (POST):
  - idpList
  - idpExcludedList
  - forcedIdP
- Autenticación de **personas jurídicas**
  - allowLegalPerson → islegalperson, oid

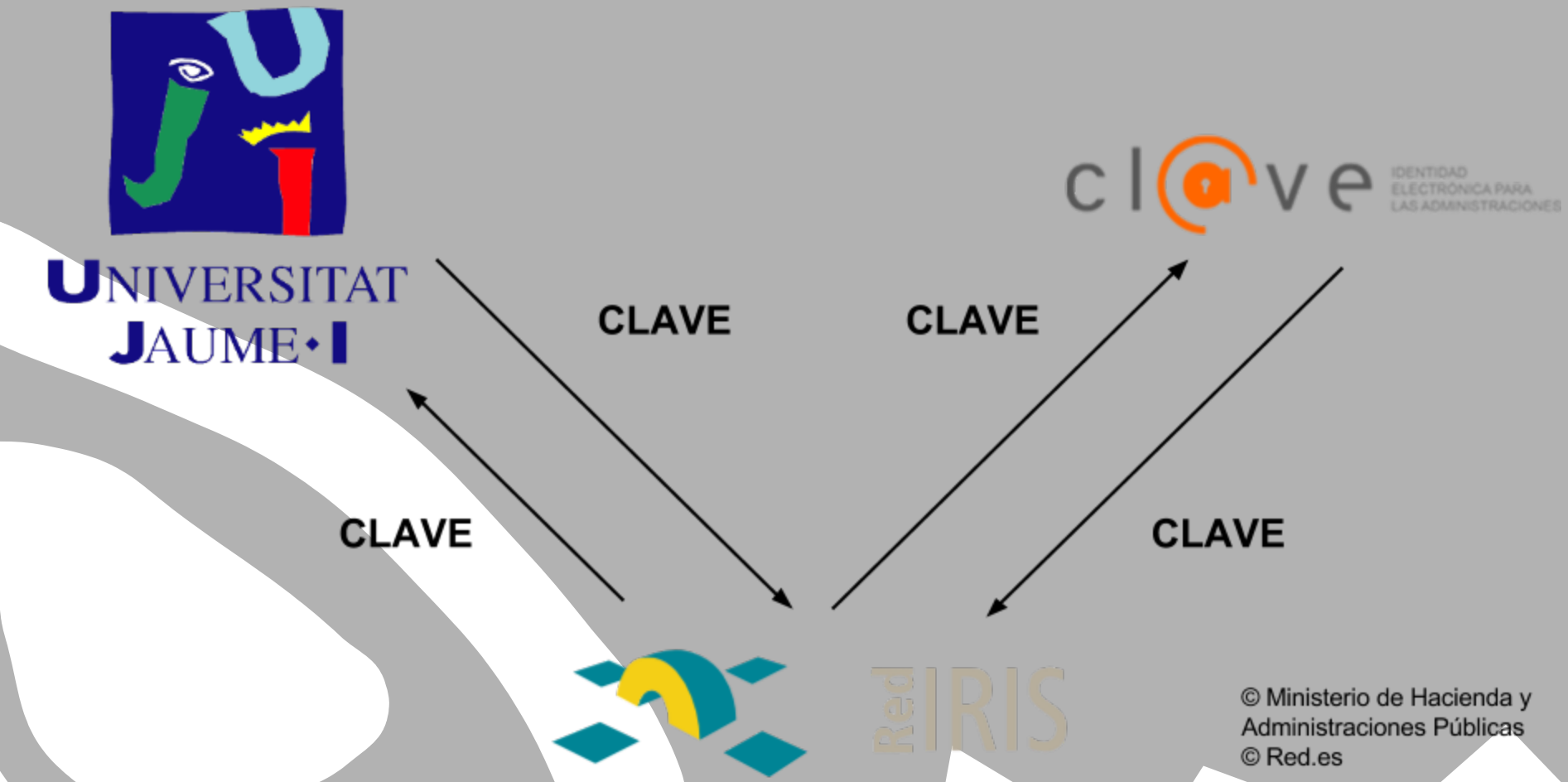
El perfil Cl@ve

- Especificaciones del Single Log Out
  - HTTP-POST, firmado
  - **Parámetros POST no estándar**
    - samlRequestLogout
    - samlResponseLogout
  - **entityID del SP** → en el nameID
  - **returnAddress del SP** -> en el Issuer (porque no hay metadata de SP)

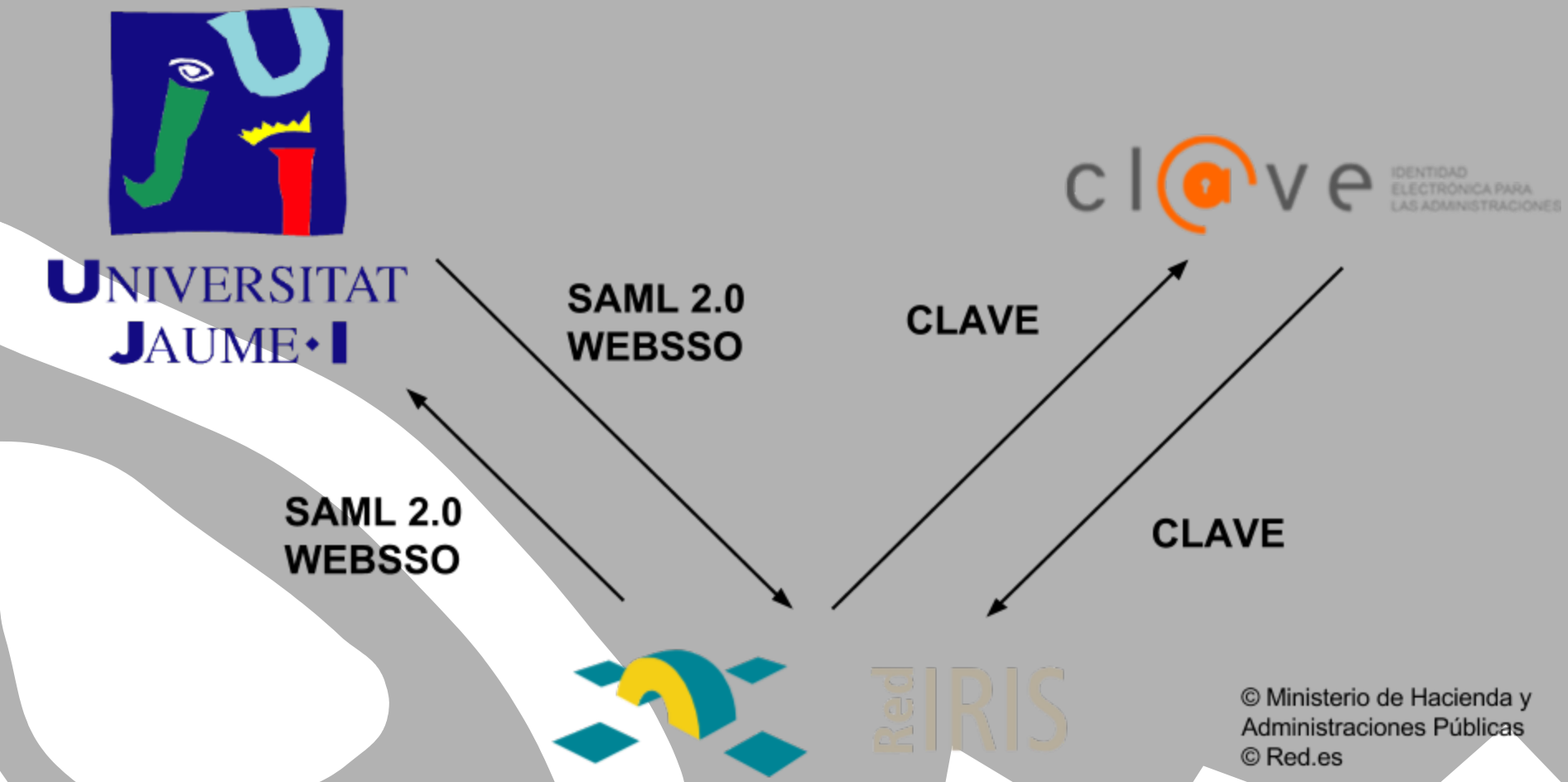
Dos pasarelas

- Cl@ve **diverge de SAML 2.0** WEB-SSO
- Caso de uso más frecuente:
  - **Autenticación con lista estática** de atributos
- Puede ser **traducido al estándar**
- **Dos pasarelas**:
  - una Cl@ve
  - una SAML2.0 WEBSSO

Pasarela Cl@ve-Cl@ve



Pasarela SAML-Cl@ve



Diseño

- Basado en **SimpleSamlPHP**.
- **Módulo**.
- Dos IdP, configuración compartida.
- Autorización de SP, compartida o separada.

Pasarela Cl@ve-Cl@ve

- No genera sesión
- **No publica metadatos**
- Retransmite:
  - Lista de atributos (autorizados)
  - Parámetros POST (autorizados)
  - Extensiones STORK
- Se puede **enmascarar globalmente** ciertas opciones.

Pasarela SAML-Cl@ve

- No genera sesión
- **Publica metadatos estándar**
- Configurable por SP (se puede enmascarar globalmente ciertas opciones):
  - Lista de atributos
  - Extensiones STORK
  - Parámetros POST
- Parámetros POST de la respuesta → **devueltos como atributos**

Integración

SAML	Cl@ve
• Software comercial. • **Mantenibilidad**, seguridad. • **Esfuerzo** de integración **bajo**.	• **Lista** de atributos **dinámica**. • Extensiones STORK. • **Envío de datos** en la petición.

Metadatos del SP

Metadato	SAML	Cl@ve
EntityID	✓	✓
Assertion Consumer Service	✓	
Certificado de firma	✓	✓
Lista de atributos	✓	
Lista de fuentes de autenticación (a mostrar/ocultar/forzar)	✓	
Aceptar autenticación de persona Jurídica	✓	

¿Qué pasarela integrar?

	SP SAML ya implantado	SP SAML no disponible
Sin requisitos especiales (Auth básica)	SAML	CLAVE?
Puede beneficiarse de las mejoras de protocolo	SAML?	CLAVE

Trabajo futuro

- Soporte para funcionalidades STORK2
  - Nuevos atributos
  - Aserciones múltiples (consulta de APs)
  - Firma de documentos
  - Validación de firmas
  - Poderes sobre personas jurídicas
- Integrar generación de nameID
- Integración en el HUB de SIR2
- Traducción de perfil de atributos (eduPerson?)

UNIVERSITAT JAUME I
DES DE 1991
25 ANYS

Gracias por vuestra atención