Implementación de un servicio de autenticación centralizado y gestión de identidades en la Universidad de la República

Emilio Penna

SERVICIO CENTRAL DE INFORMÁTICA

TICAL CONFERENCIA 2016
13 - 15 Sept. Buenos Aires, Argentina

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

Introducción

- **Institución pública, la mayor del país.**
- **Más de 100000 estudiantes activos**
- **Más de 16000 funcionarios y docentes**
- **Presencia en varios puntos del país**
- **SeCIU: Servicio Central de Informática Universitaria**

SERVICIO CENTRAL
DE INFORMÁTICA

Inicio

2013: Inicio del proyecto, principales necesidades:

1. **Unificación de información de identidad**
2. **Falta de sistema de autenticación central para funcionarios y docentes, requerida por nuevas aplicaciones.**
3. **Necesidad de actualización del mecanismo de autenticación de estudiantes**
4. **Mejoras en procesos de gestión de identidades y ciclo de vida**
5. **Mejoras de aspectos de seguridad**
6. **Mejor experiencia para el usuario**

Antecedentes

2014: Relevamiento de antecedentes, estándares y tecnologias. Diseño de varios aspectos de la solución, pruebas.

Participación en IdM Workshop organizado por ELCIRA, en TICAL 2014. Fundamental para conocer avances en federaciones de identidad e inter-federaciones.

Producción

2015 – Salida en producción con dos aplicaciones accedidas por casi todos los funcionarios y docentes

Identity Management

"Procesos y políticas involucradas en el manejo del ciclo de vida y valor, tipo y metadata opcional de los atributos de las identidades conocidas para un dominio particular" (ISO 24760)

INTERNATIONAL STANDARD **ISO/IEC 24760-1**

First edition
2011-12-15

Information technology — Security techniques — A framework for identity management —

Part 1:
Terminology and concepts

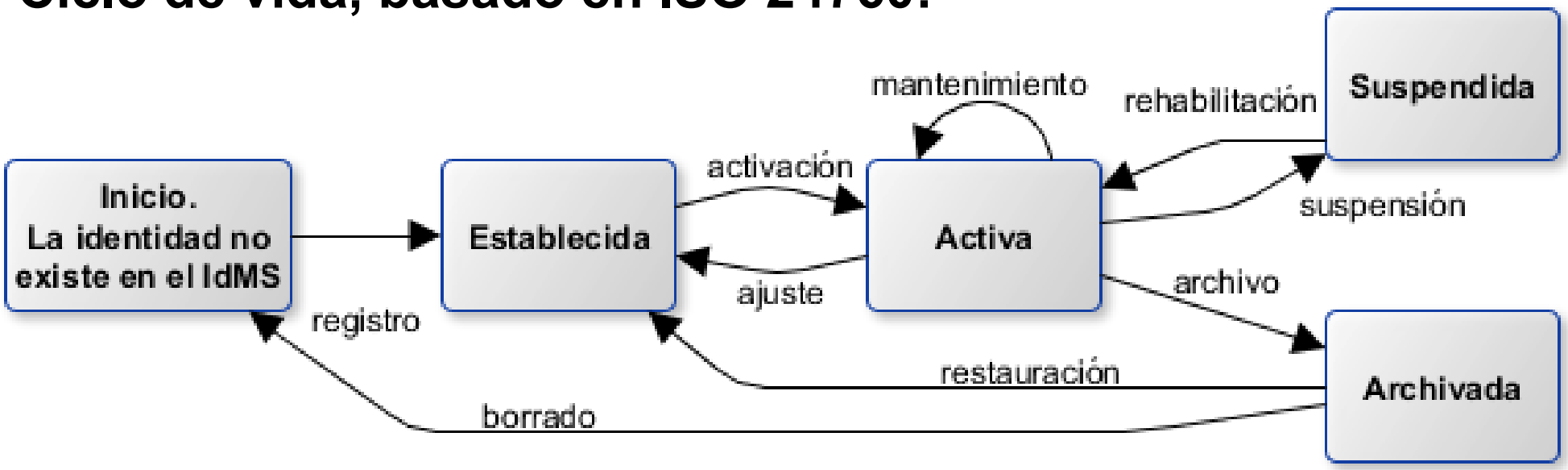
Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité —

Partie 1: Terminologie et concepts

Identity lifecycle

La gestión de identidades considera el ciclo de vida de la información de identidad (Identity Lifecycle) desde el registro inicial hasta el archivo o borrado y esto implica gobernanza, políticas, procesos, datos, tecnología y estándares

Ciclo de vida, basado en ISO 24760:



Sistemas para IdM, componentes y funciones

De acuerdo al IdM Toolkit, las funciones principales de un sistema de IdM requeridos para una institución académica son:

- **Herramientas para gestión del repositorio de identidades y manejo del ciclo de vida**
- **Servicio de autenticación**
- **Servicio de autorización**
- **Servicio de directorio**
- **Servicio de grupos**

Algunos sistemas utilizados en Udelar

Shibboleth

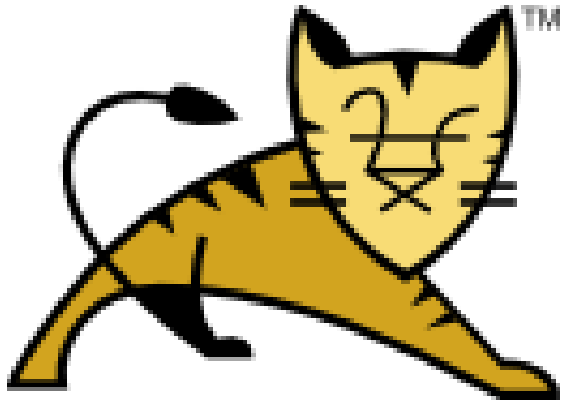
Apache HTTP SERVER

OpenLDAP™ http://www.OpenLDAP.org

FreeRADIUS The world's most popular RADIUS Server

mgu

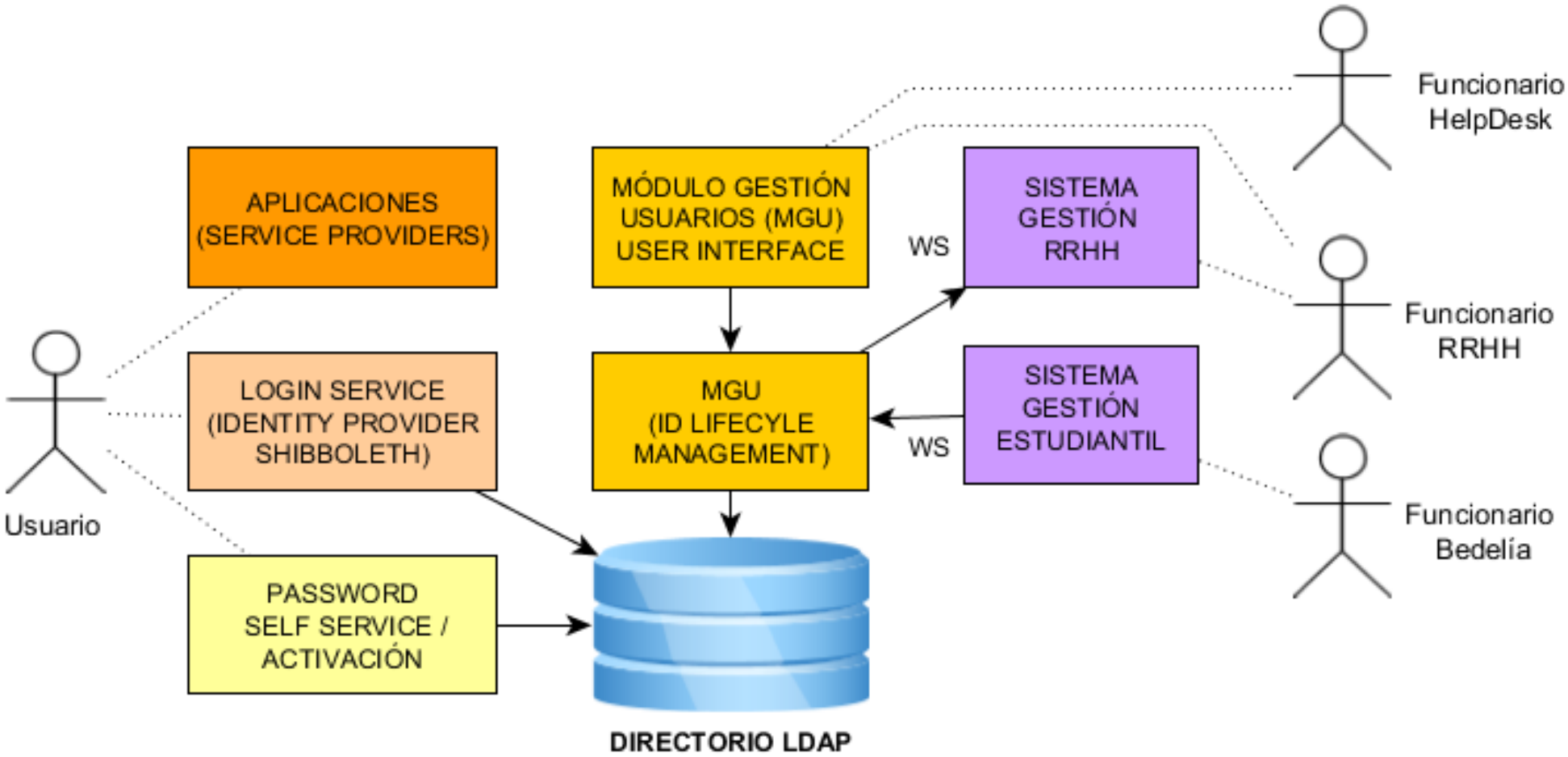
PWM
Password Manager



Apache Tomcat

Módulo de gestión de usuarios

MGU - Gestión del repositorio de identidades y manejo del ciclo de vida



Procedimiento de registro de usuarios

1. El usuario debe concurrir a la oficina de Recursos Humanos con documento de identidad
2. Verificación de identidad (validación presencial)
3. MGU toma datos del sistema de RRHH y genera cuenta en directorio LDAP
4. Aceptación de condiciones de uso
5. Entrega de código de activación
6. Activación de la cuenta (por parte del usuario)
7. Si el usuario debe utilizar ciertos sistemas sensibles, solicita smart-card con certificado x509.

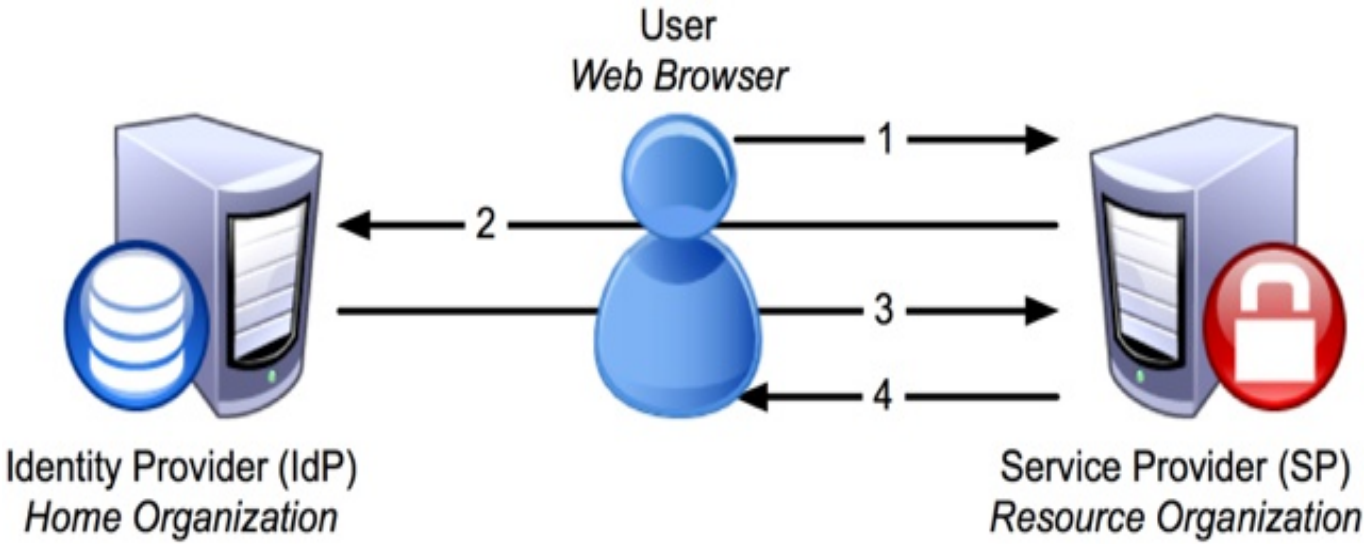
Modelado de información de identidad

Identidad única con múltiples vínculos (afiliaciones)

1. **InetOrgPerson, person: nombres, email, mobile, password**
2. **EduPerson: eduPersonAffiliation, eduPersonPrincipalName**
3. **PwmUser: pwmResponseSet**
4. **UdelarPerson: afiliación extendida (ej: staff@11), tipo de cuenta y tipo de validación, estado de la cuenta**
5. **UdelarPersonCertInfo: información de smart-cards y certificados, sistemas centrales a los que puede acceder**
6. **Identificadores: Documento de identidad (uso interno), eduPersonUniqueId, persistentId, transientId.**
7. **Actulamente el IdP emite todos los atributos recomendados en el eduGAIN attribute profile**

Proveedor de Identidad y autenticación

- Proveedor de Identidad SAML (federated identity protocol)
- Single Sign On - Web Browser SSO Profile
- Se configuró de forma alineada con el "Interoperable SAML 2.0 Profile"

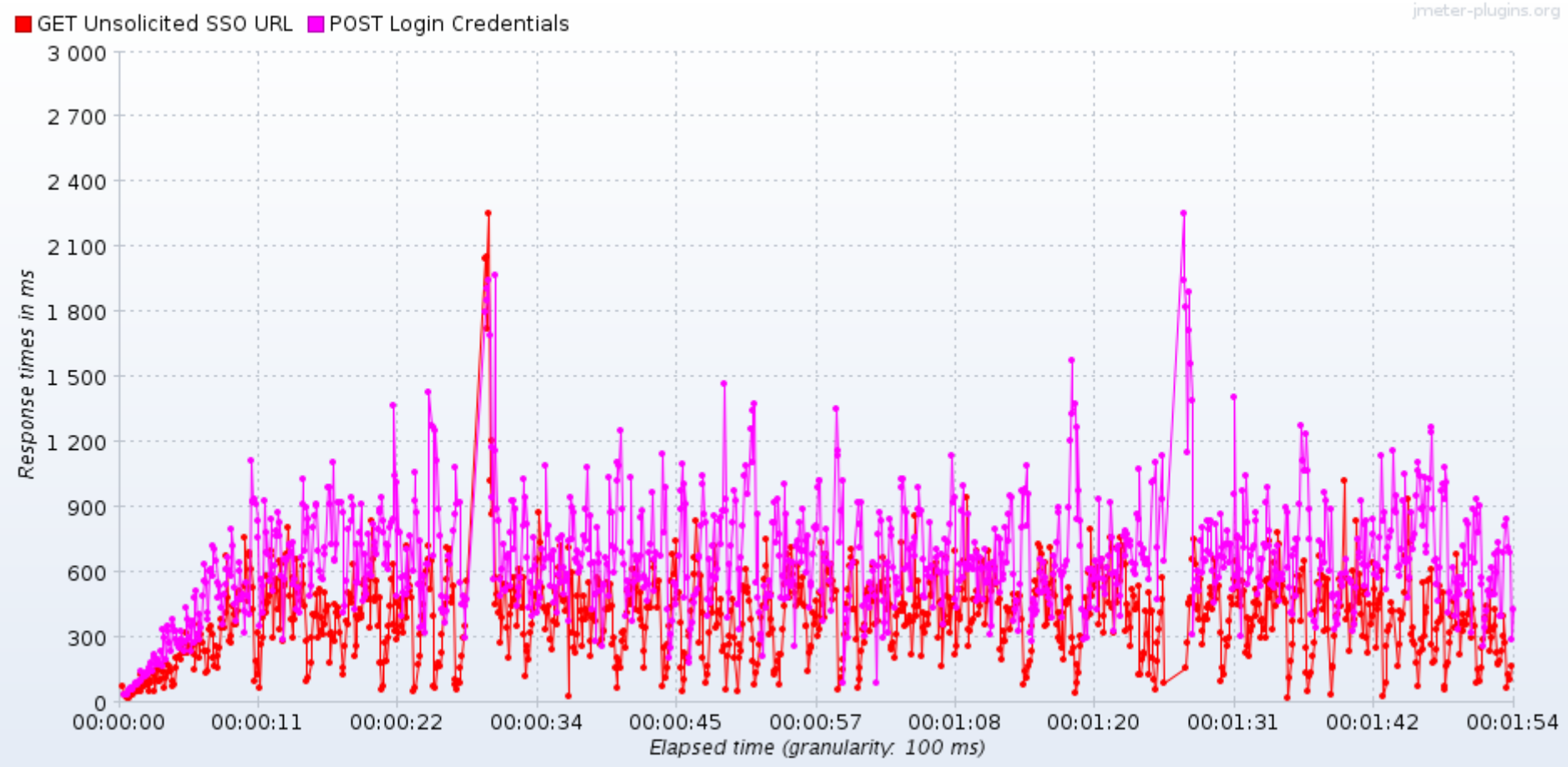


Shibboleth IdP v3 - OpenLDAP

1. Integración con OpenLDAP “out of the box”
2. Integración con módulo de políticas de contraseñas de OpenLDAP: ppolicy (solo se requiere configuración).
3. Autenticación con certificados x509 de cliente: sólo requiere configuración.

Load Test

1. Test jmeter – 10000 inicios de sesion en 1:54 min.
2. Test disponible en wiki de shibboleth, con community contributed results

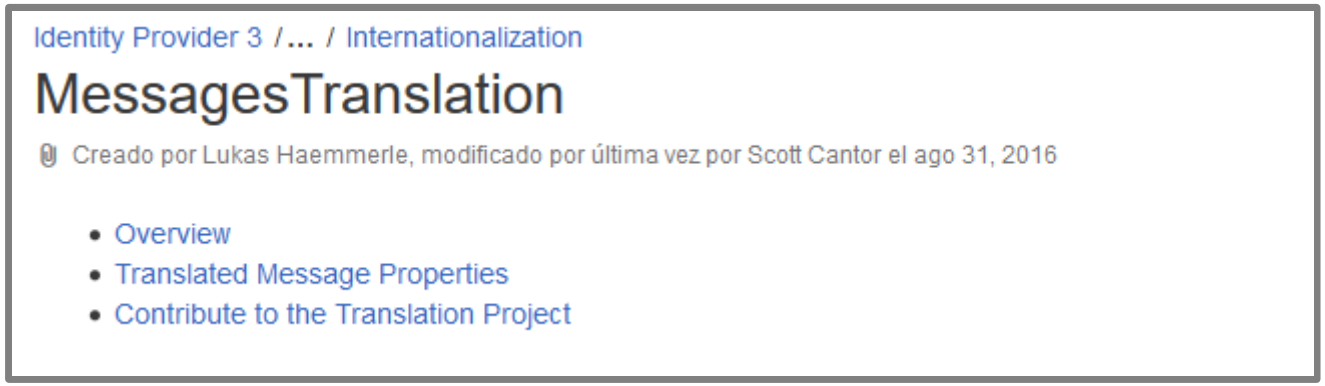


Shibboleth IdP v3 en español

Shibboleth por defecto solo incluye mensajes en inglés.

En 2015 surge proyecto de traducción, Udelar contribuye traducción al español.

https://wiki.shibboleth.net/confluence/display/IDP30/MessagesTranslation



Emisión de atributos

- Tener en cuenta regulaciones de protección de datos personales y privacidad
- Posibilidad de filtrado de atributos por SP
- Módulo de consentimiento incorporado en IdP v3
- En el contexto de federaciones son relevantes la entity-categories, en particular: “Research and Scolarship Entity Category”
- Attribute Authority

Unlocking Attributes

REFEDS work on Entity Categories is helping support the safe and secure release of attributes to services

Integración de aplicaciones

Experiencia en el primer año:

- Desarrollo de nuevas aplicaciones que utilizan IdP para autenticar
- Adaptación de aplicaciones existentes
- Integración de distintas tecnologías: Java, PHP Genexus, Oracle PLSQL
- Capacitación a equipos de desarrollo
- Software existente que soporta integración con SAML / shibboleth (ej: Moodle)
- Servicios cloud que soportan autenticación con SAML

Radius

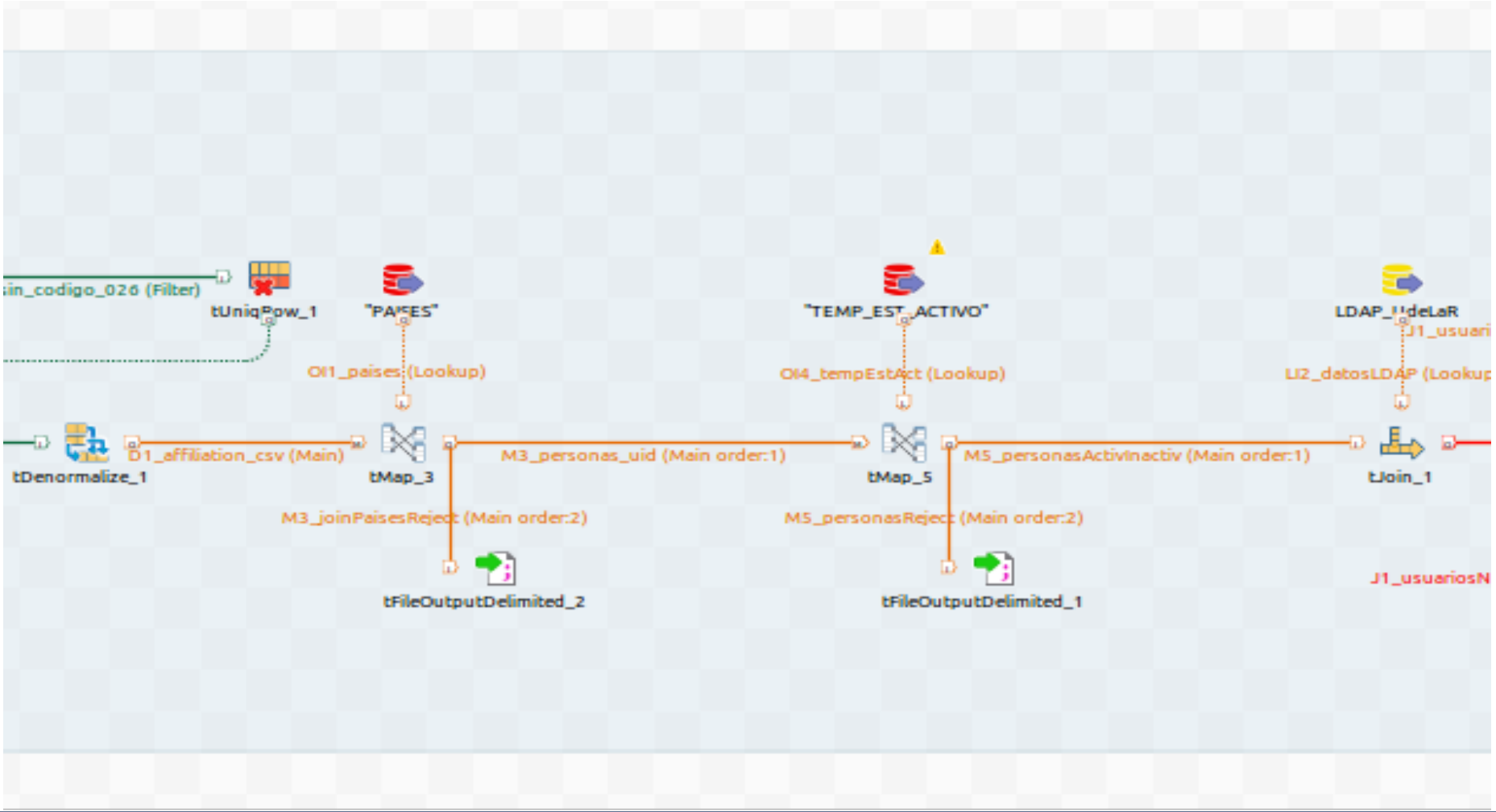
- **Próximo paso en el corto plazo: incluir estudiantes en el directorio**
- **Servicio Radius existente – se prevee integrarlo con el nuevo directorio**

eduroam

- **Integración del servidor Radius de eduroam de Udelar con el nuevo directorio global.**
- **Permite que los usuarios puedan utilizar eduroam, con la misma contraseña que utilizan en el IdP web.**

Migraciones de datos

Herramienta utilizada para migraciones de datos al directorio: Talend (Open Source ETL & Data Integration)



Federación de identidades

Actualmente el grupo del proyecto de gestión de identidades se encuentra trabajando en conjunto con el área que administra la Red Académica del Uruguay (RAU) para la formación de la federación nacional de identidad académica del Uruguay, y su incorporación a eduGAIN.

Referencias

- eduGAIN. Disponible en: http://services.geant.net/edugain/Pages/Home.aspx
- REFEDS – The Voice of Research and Education Identity Federations. https://refeds.org/
- «SAML Specifications | SAML XML.org». [En línea]. Disponible en: http://saml.xml.org/saml-specifications
- «ISO/IEC 24760-1:2011 - Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts», ISO. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=57914
- «Identity Management infoKit / Home». https://www.identity-project.org
- Top Identity Management Software Products http://www.capterra.com/identity-management-software/
- «OpenLDAP, Main Page». http://www.openldap.org/
- «FreeRADIUS: The world's most popular RADIUS Server». http://freeradius.org/
- Proyecto PWM, GitHub. https://github.com/pwm-project/pwm
- Definition of the inetOrgPerson LDAP Object Class. https://tools.ietf.org/html/rfc2798
- eduPerson & eduOrg | Internet2. http://www.internet2.edu/products-services/trust-identity/eduperson-eduorg/
- The (SAML2Int) Interoperable SAML 2.0 Profile.http://saml2int.org/.
- Shibboleth Concepts https://wiki.shibboleth.net/confluence/display/CONCEPT/Home .

Referencias

•Shibboleth. https://shibboleth.net/

•«OpenLDAP Software 2.4 Administrator's Guide: Overlays». http://www.openldap.org/doc/admin24/overlays.html

•LDAPAuthnConfiguration - Identity Provider 3. https://wiki.shibboleth.net/confluence/display/IDP30/LDAPAuthnConfiguration

•X509AuthnConfiguration - Identity Provider 3.https://wiki.shibboleth.net/confluence/display/IDP30/X509AuthnConfiguration.

•Load Testing Contributed Results - Identity Provider 3. https://wiki.shibboleth.net/confluence/display/IDP30/Load+Testing+Contributed+Results

•MessagesTranslation - Identity Provider 3. https://wiki.shibboleth.net/confluence/display/IDP30/MessagesTranslation

•Research and Scholarship Entity Category. https://refeds.org/category/research-and-scholarship

•eduGAIN attribute profile. http://services.geant.net/edugain/Resources/Documents/GN3-11-012%20eduGAIN_attribute_profile.pdf

•Shibboleth Enabled Applications and Services https://wiki.shibboleth.net/confluence/display/SHIB2/ShibEnabled

•Eduroam https://www.eduroam.org/

•Eduroam UY http://eduroam.uy/

•Talend Real-Time Open Source Data Integration Software. https://www.talend.com/

[Sitios web accedidos el 30 de junio de 2016]

Muchas gracias

emilio.penna@seciu.edu.uy
secretaria@seciu.edu.uy
www.seciu.edu.uy