Servicio de autenticación centralizado y gestión de identidades en la Universidad de la República

Marzo 2017

SERVICIO CENTRAL DE INFORMÁTICA

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

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 tecnologías. Diseño de varios aspectos de la solución, pruebas. Contacto con Facultad de Ingeniería.

Participación en Workshops de IdM y federaciones de identidad académicas, organizado por ELCIRA (TICAL 2014) y MAGIC (TICAL 2016).

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

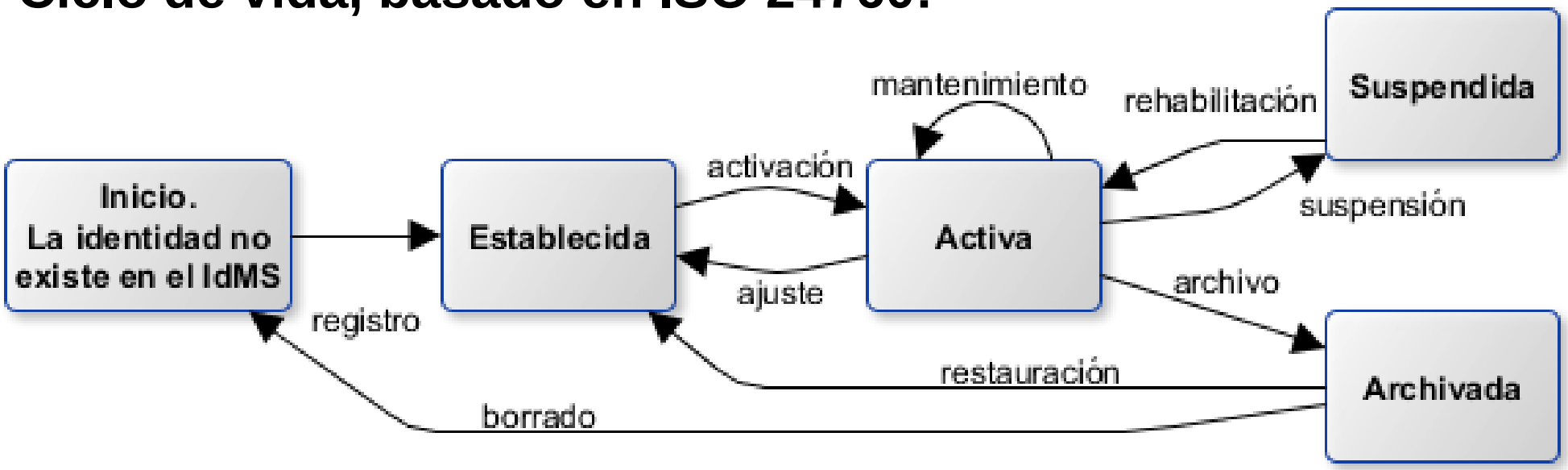
Technologies de l'information — Techniques de sécurité — Cadre pour la gestion de l'identité —

Partie 1: Terminologie et concepts

Identity lifecycle

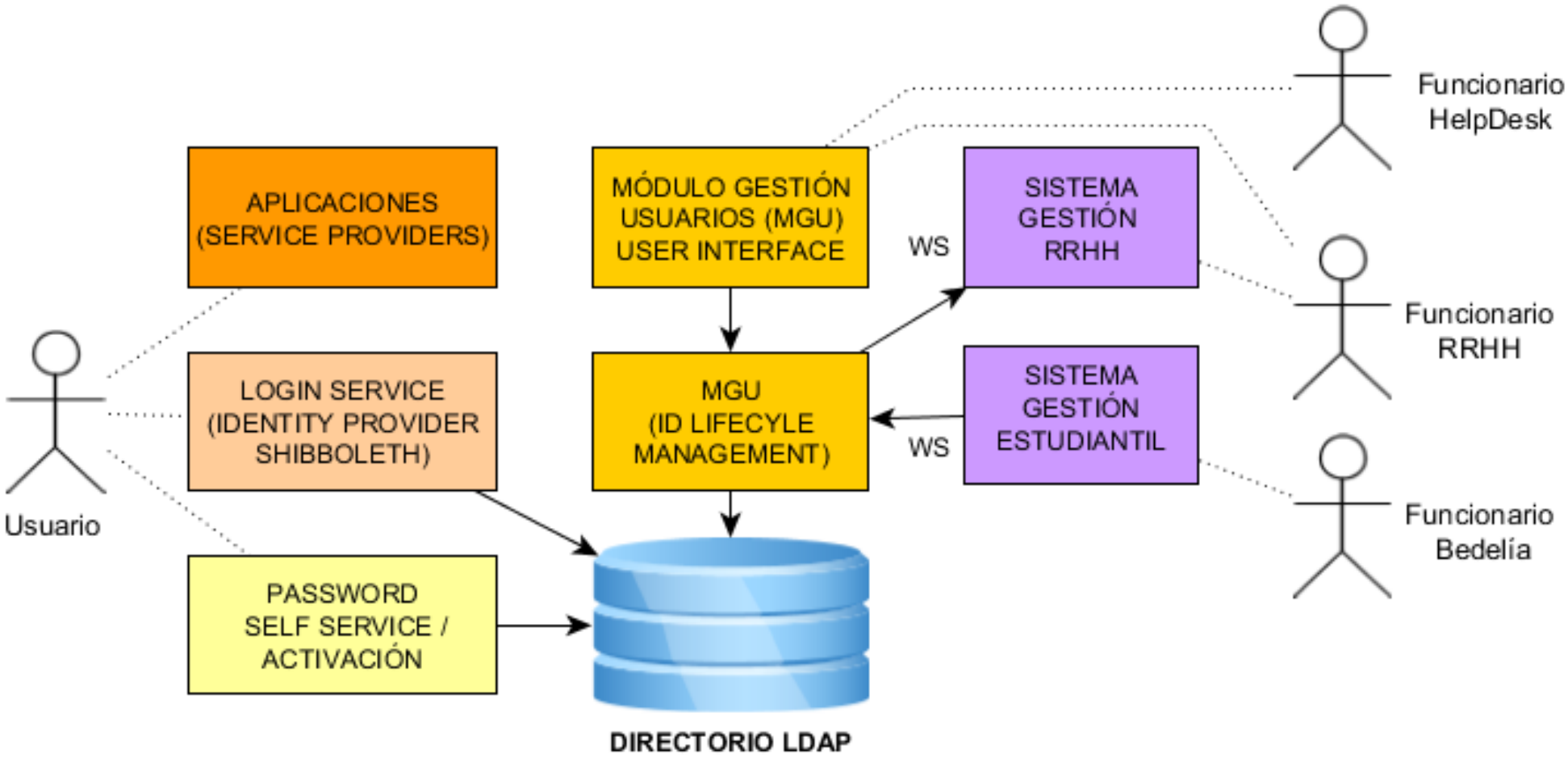
La gestión de identidades considera el ciclo de vida de la información de identidad (Identity Lifecycle) desde el registro inicial hasta el archivo o borrado y esto implica gobernanza, políticas, procesos, datos, tecnología y estándares

Ciclo de vida, basado en ISO 24760:



Módulo de gestión de usuarios

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

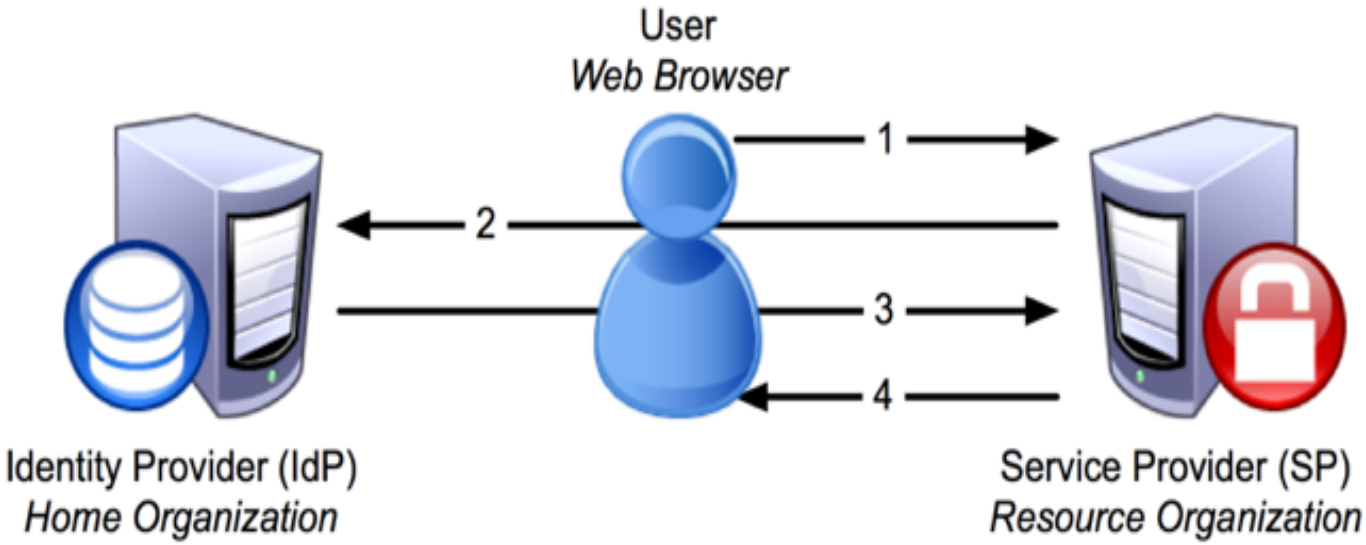


Registro de usuarios

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 utiliza tarjeta (smart-card) con certificado x509 para acceso a ciertos sistemas sensibles, la información también se gestiona en esta infraestructura.

Proveedor de Identidad

- **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"**



Proveedor de identidad

- Para la implementación del IdP se utilizó Shibboleth IdP (open source).
- La identidad federada permite que información de identidad de usuarios en un dominio de seguridad sea provista a otras organizaciones que formen parte de la federación. Esto permite Single Sign On entre distintos dominios y elimina la necesidad de que quienes proveen contenido deban mantener cuentas de usuarios y contraseñas.
- Los proveedores de identidad (IdP) autentican y prooveen información sobre los usuarios y los proveedores de servicio (SP) consumen esta información y controlan el acceso a contenido que requiera autenticación.

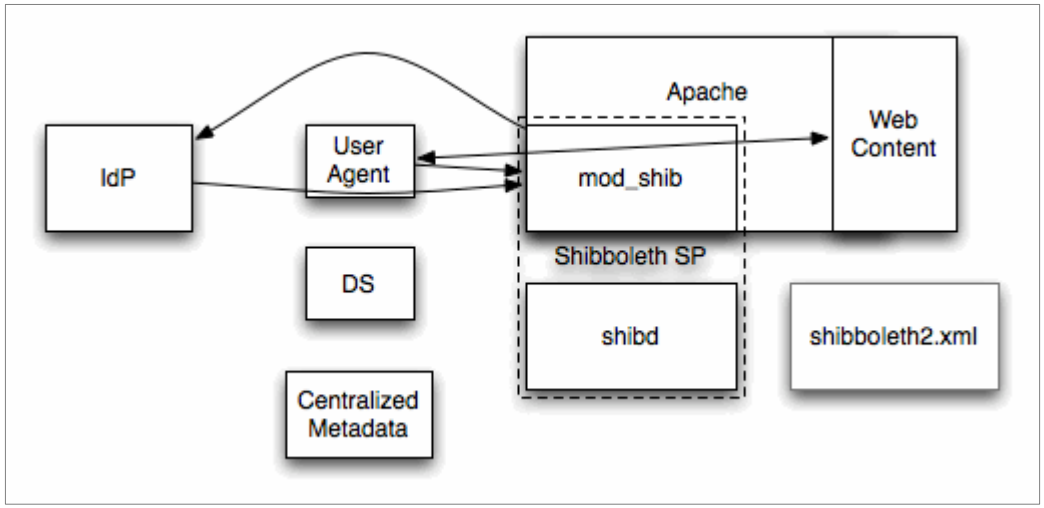
Proveedor de identidad

- **SAML: Especificación con: Protocolo de comunicación (SAML Protocol) y formato para intercambio de información de autenticación, y atributos (SAML Assertion)**
- **SAML 101: Introducción a SAML como cloud security standard: https://www.youtube.com/watch?v=gUmMcecHN9s**

- **Antecedentes: EduGAIN: red mundial académica con 1500 proveedores de identidad SAML similares (inter-federación).**
- **https://www.youtube.com/watch?v=x1YhuFPxMz8**

Proveedores de servicios

- **Se utiliza un módulo en el servidor web (Shibboleth SP) para facilitar la integración de aplicaciones. El módulo realiza el manejo de SAML. Redirige al IdP si no hay una sesión activa. Si la autenticación es exitosa, comunica información de autenticación y atributos a las aplicaciones que protege.**
- **La autorización queda en manos de la aplicación.**



Atributos

- **Documento: <pais>-<tipo>-<número>**
- **Ejemplo: UY-DO-12345678 (incluye digito verificador)**
- **Nombre completo**
- **Dirección de email**
- **Afiliación en formato estandarizado (esquema eduPerson): staff, faculty, student**
- **Afiliación incluyendo servicio: ejemplo student@011**
- **Una cuenta de usuario puede no tener afiliación, por ej. un docente que cesa en su cargo.**

Integración de aplicaciones

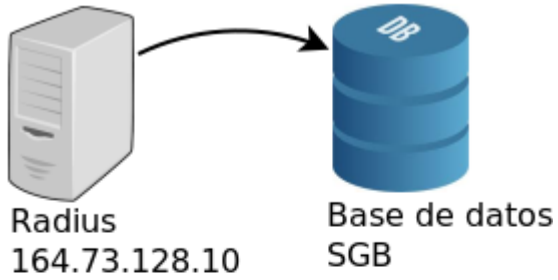
Experiencia en el primer año:

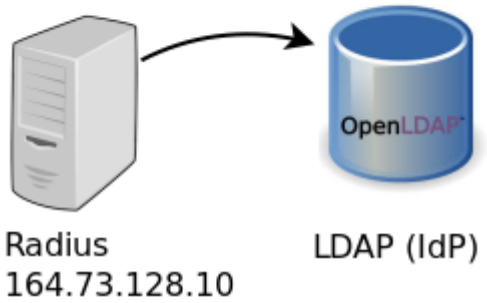
- Desarrollo de nuevas aplicaciones que utilizan IdP para autenticar
- Adaptación de aplicaciones existentes
- Integración de distintas tecnologías: Java, PHP Genexus, Oracle PLSQL
- Capacitación a equipos de desarrollo
- Pruebas de software existente que soporta integración con SAML / shibboleth (ej: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

Radius

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

Radius


DB
Radius
164.73.128.10
Base de datos
SGB


OpenLDAP
Radius
164.73.128.10
LDAP (IdP)

Radius

Controles sobre la cuenta

- Pertenece al realm consultado
- Activa (en el caso de estudiantes implica haber realizado proceso de activación de la cuenta y tener alguna actividad en los últimos 5 años)
- No tiene password bloqueado (la clave se bloquea luego de cierta cantidad de intentos fallidos)

Radius

Cambios en la autenticación

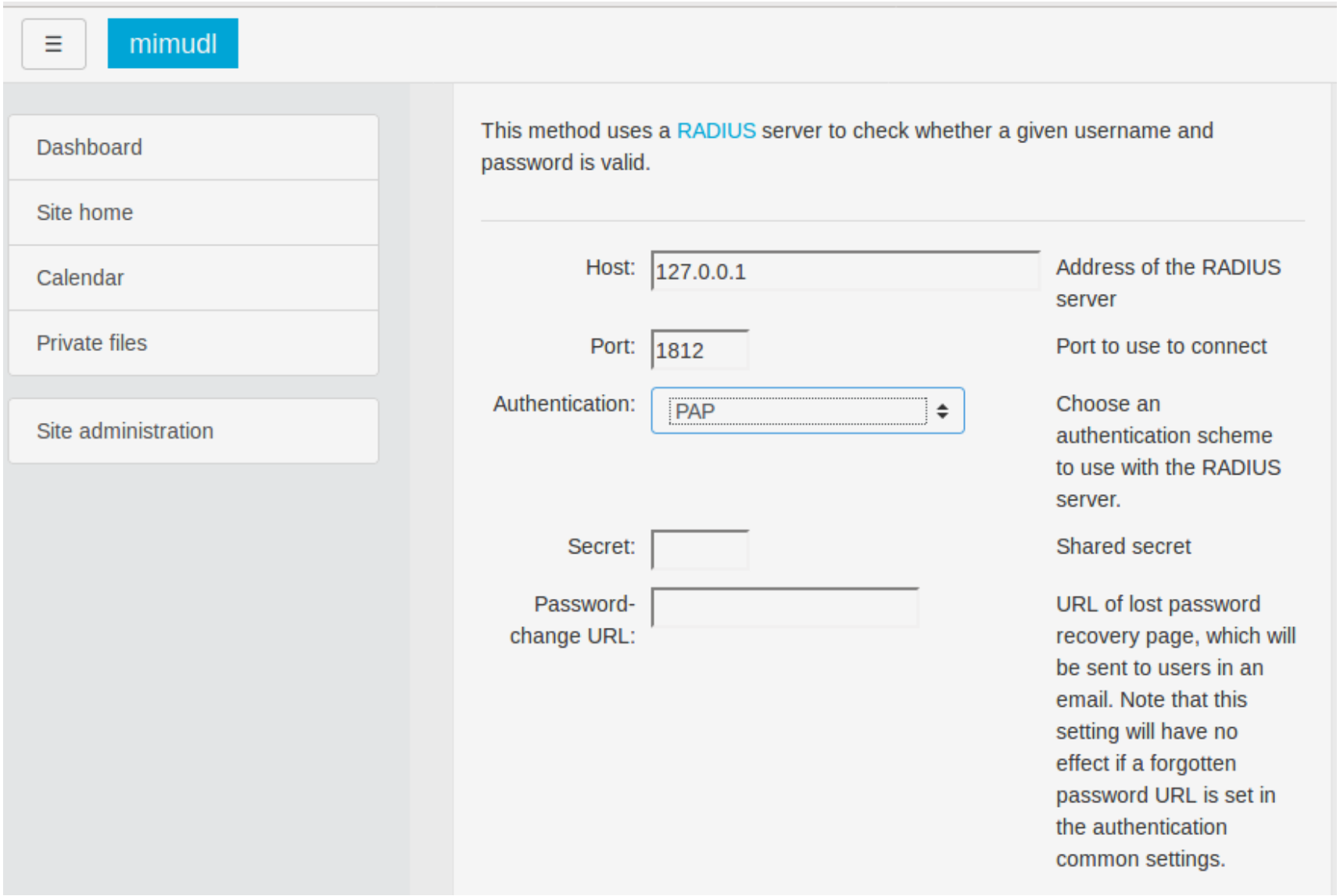
- En el 99 % de los casos el identificador del estudiante no cambia. Ej: estudiante de Facultad de Derecho con **C.I.:1234567-8** se autentica en Radius con **1234567@fder**

- En el caso de los estudiantes extranjeros que ahora se identifican con un documento extranjero, se ve afectado el identificador utilizado. Ej: estudiante extranjero de Facultad de Derecho inscripto en SGAE con documento real **BR-PA-12345** y representado en SGB con documento ficticio **9000001**, en Radius, pasa de autenticarse de la forma **9000001@fder** a **BR-PA-12345@fder**

- En el caso de los estudiantes extranjeros inscriptos por SGB(anteriores a 2016) se migran al LDAP con el identificador ficticio del tipo 9000000. Ej: estudiante extranjero de Facultad de Derecho inscripto en SGB con **9000002**, luego de la migración sigue autenticándose en Radius con **9000002@fder**

Radius

Ejemplo de configuración Moodle



Radius

FORMULARIO DE ENCUESTA SERVICIO RADIUS

Facultad o Servicio:

Contacto
- Nombre:
- Teléfono:
- Correo electrónico:

Aplicación o servicio que accede a Radius:

En el caso de ser una aplicación web, utiliza HTTPS en la página de ingreso de la clave?
SI NO

Servidores activos que se conectan al Radius

Servidor 1
- IP:
- Nombre:

Servidor 2
- IP:
- Nombre:

Servidor 3
- IP:
- Nombre:

Radius

- Aplicaciones web que necesiten autenticar con la base central de usuarios → IdP
- Otros servicios que necesiten autenticar con la base central de usuarios → Radius
- Para el caso de aplicaciones web que actualmente utilizan Radius para autenticar estudiantes → utilizar HTTPS en la página de ingreso de la clave

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
- 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
- Moodle - Autenticación con Shibboleth https://docs.moodle.org/32/en/Shibboleth

[Sitios web accedidos el 30 de junio de 2016]

Muchas gracias

Más información: https://proyectos.seciu.edu.uy/

mesadeayuda@seciu.edu.uy