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

Emilio Penna, Mariela De León

Servicio Central de Informática Universitaria, Universidad de la República
Colonia 2066, Montevideo, Uruguay
emilio.penna@seciu.edu.uy, mariela.deleon@seciu.edu.uy

Resumen. El Servicio Central de Informática de la Universidad de la República ha trabajado en los últimos dos años en la implementación de un servicio de autenticación centralizada, basada en un proveedor de identidad Shibboleth, y en una solución para gestión de identidades unificada. La gestión de identidades considera el ciclo de vida de la identidad (tomando como referencia la norma ISO 24760) y se implementó en forma integrada con los sistemas centrales de gestión, lo que permite que el sistema de gestión de identidades cuente con información actualizada y consistente.

Se trabajó con énfasis en aspectos de seguridad de la solución, considerando desde los procesos administrativos de registro y verificación de identidad, hasta la implementación de mecanismos de autenticación fuerte con certificados x509 de cliente y smart-cards. Por otra parte, considerando los avances en las federaciones de identidad académicas, se eligieron estándares, tecnologías y modelos de datos que permitieran una buena integración con estas federaciones.

Actualmente estos servicios se encuentran en producción y se han integrado con éxito varias aplicaciones y servicios que son utilizadas por toda la universidad, desde aplicaciones de autogestión para los funcionarios, hasta el servicio de autenticación utilizado para eduroam. En este artículo se describen las características principales de la solución, las mejores prácticas relevadas, los resultados obtenidos y los próximos pasos que se pretenden dar en el proyecto.

Palabras clave: Autenticación, Federación de Identidades, Identity Management, SAML, eduGAIN, Shibboleth, Single Sign On, eduroam

1 Introducción

La Universidad de la República (Udelar) es la principal institución de educación superior y de investigación del Uruguay. Es una institución pública, autónoma y cogobernada por sus docentes, estudiantes y egresados. La Udelar cuenta actualmente con aproximadamente 100.000 estudiantes activos y 15.000 funcionarios (docentes y no docentes). Administrativamente se compone de 22 unidades, entre facultades, centros universitarios y servicios centrales. La mayor cantidad de facultades se ubican en distintos puntos de la capital, Montevideo, y también existen centros universitarios en otros departamentos del país.

La Udelar cuenta con un Servicio Central de Informática Universitaria (SeCIU), que es responsable de asesorar a las autoridades universitarias sobre esta temática, así como de desarrollar y gestionar la infraestructura informática de la Udelar relacionada con los emprendimientos institucionales y de brindar asesoramiento y apoyo informático a todos los servicios universitarios.

En el año 2013, se plantearon una serie de necesidades que dieron lugar a la formación de un grupo de trabajo para buscar soluciones que mejoraran los procesos de autenticación y gestión de identidades para toda la Udelar. En ese momento se contaba con un mecanismo de autenticación para los estudiantes que necesitaba ser actualizado, y por otra parte, para los funcionarios y docentes, no se contaba con un mecanismo de autenticación central. A partir de ese momento, SeCIU trabajó

investigando antecedentes, estándares, tecnologías y mejores prácticas que pudieran aplicarse para brindar una solución adecuada [1][2]. Por un lado se puso especial foco en la seguridad de estos aspectos, y por otra parte se pretendía mejorar la experiencia de sus usuarios, facilitando el acceso a recursos, aplicaciones, y servicios.

En la búsqueda de soluciones similares, se observó con mucho interés el desarrollo de las federaciones de identidad en educación e investigación a nivel regional y global, y las posibilidades actuales de interfederación, posibilitadas por la infraestructura global de autenticación eduGAIN[3]. Intentando aprender de estas experiencias, miembros de SeCIU participaron en el taller de federaciones realizado en el marco del proyecto ELCIRA en el TICAL 2014, y posteriormente se continuó el contacto con miembros de eduGAIN y también en listas de correo como la de REFEDS (Research and Education Federations) [4]. Considerando este contexto, se orientó el trabajo para que el proyecto de gestión de identidades de Udelar fuera compatible con eduGAIN, de forma de ampliar las posibilidades de colaboración y acceso a recursos de los miembros de la institución.

En el año 2014 se comenzó con el diseño y la implementación de varios componentes de la solución y en el año 2015 se aprovechó la oportunidad de un censo de funcionarios, para completar la primer versión de la solución e implantar la misma en toda la universidad. Esta solución permitió tener una identidad unificada para cada miembro de la Udelar, e implicó la implementación de un nuevo directorio global y la generación de cuentas para todos los funcionarios (docentes y no docentes). Esto se realizó junto con la implantación de dos nuevas aplicaciones a las cuales acceden de manera autenticada todos los funcionarios: la aplicación del censo y el Módulo de Autogestión de Personal (MAP), en el cual los funcionarios pueden consultar vía web sus recibos de sueldo, certificados para declaraciones de impuestos y realizar solicitudes de certificaciones médicas.

Un componente central de la solución es un Proveedor de Identidad (Identity Provider, IdP) que brinda un servicio central de autenticación. En este modelo, cuando un usuario intenta ingresar a un recurso o aplicación que requiere autenticación, se redirige al mismo al IdP, donde se autentica y luego se le da acceso al recurso solicitado. El IdP también permite realizar Single Sign On (inicio único de sesión, lo cual habilita al usuario para acceder a varios sistemas con una sola instancia de autenticación). Este proveedor utiliza el estándar SAML[5] alineado con la infraestructura global de autenticación eduGAIN, lo cual permite la autenticación federada, con el objetivo de que los usuarios puedan también acceder a recursos de otras instituciones con su identidad digital de Udelar. Para lograr esto último, el grupo del proyecto de gestión de identidades trabaja en conjunto con el área que administra la Red Académica del Uruguay (RAU) para la formación de la federación nacional de identidad académica. También se ha trabajado con la RAU para integrar esta solución de identidad unificada con eduroam (REF), de forma de que los miembros de Udelar puedan acceder a eduroam con el mismo nombre de usuario y contraseña que utilizan en el proveedor de identidad central.

2 Gestión de identidades

En el comienzo del proyecto se planteó la necesidad de una solución de autenticación, lo cual requiere al menos un repositorio de identidades con sus correspondientes credenciales. Esto introduce la problemática de cómo gestionar de manera adecuada esta información de identidades (considerando la creación, verificación, mantenimiento, modificación y eliminación de la información), y considerar los procesos, políticas y sistemas que puedan estar involucrados con dicha gestión.

Esta temática es abordada en una disciplina llamada gestión de identidades (Identity Management, IdM). Se intentó relevar y considerar buenas prácticas existentes para encarar esta tarea. En primer lugar se puede mencionar a la norma ISO 24760 “Information technology - Security techniques - A framework for identity management”[6]. En esta norma se define a la gestión de identidades como los “*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”.*

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. La implementación de un registro de identidades debe

considerar este ciclo de vida y en esto intervienen aplicaciones y herramientas para el mantenimiento y uso adecuado de la información. En esta actividad resulta relevante el cuidado de la integridad, confidencialidad y disponibilidad de la información, y en particular deben considerarse las normas de protección de datos personales que puedan aplicar. También es vital considerar el riesgo de robo de la información de identidad, y las medidas que puedan aplicarse para mitigarlo.

Otra referencia destacable en esta temática es una guía de mejores prácticas en gestión de identidades para instituciones de educación superior del Reino Unido (IdM Toolkit [7]). Esta guía brinda amplia información del tema, desde conceptos, gobernanza, componentes y sistemas hasta recomendaciones para gestión de proyectos de este tipo.

Ciclo de vida de las identidades

En la figura siguiente se muestran distintos estados y transiciones que pueden observarse en el ciclo de vida de una identidad en un Sistema de Gestión de Identidades (Identity Management System, IdMS), según ISO 24760-1.

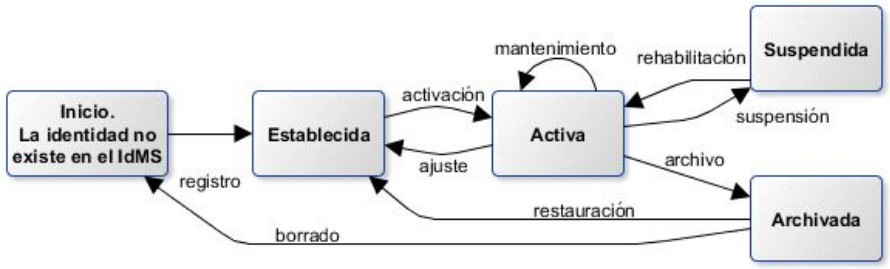

Ilustración : Ciclo de vida de una identidad, basado en ISO 24760-1

Inicialmente una entidad es desconocida, no existe en el IdMS y no se posee información de la misma en el repositorio de identidades. Cuando se realiza el registro o inscripción de una entidad, se crea la identidad en el IdMS, y se registra la información necesaria en el repositorio de identidades (realizando previamente las verificaciones que correspondan). También se generan identificadores y se provee al usuario de algún tipo de credencial inicial. La identidad queda en estado "Establecida", la información está presente en el IdMS pero la entidad todavía no está habilitada para acceder a los recursos y servicios del dominio. En la universidad esto sucede por ejemplo cuando se inscribe un estudiante por primera vez o cuando ingresa un nuevo funcionario o docente.

Posteriormente debe realizarse la activación de la identidad, para que la entidad pueda acceder a recursos e interactuar con servicios provistos por la institución. En el proceso implementado en la Udelar, los usuarios deben realizar la activación de su cuenta para poder acceder a los servicios disponibles.

Durante el tiempo que la identidad está activa, es posible que se actualice información de la misma, en un proceso de mantenimiento. Es posible en algunos casos que la modificación o ajuste requiera reactivar la cuenta.

En algunas situaciones es posible que deba suspenderse temporalmente la cuenta, para evitar que la entidad pueda utilizar los recursos del dominio o institución. La cuenta queda en estado "Suspendida" hasta que se rehabilite y vuelva a estar activa.

Una identidad podría ser archivada, en este estado la información de identidad de una entidad sigue presente en el registro de identidad, aunque la entidad no es reconocida en el dominio. Eventualmente, en una re-inscripción de la entidad, la información archivada podría ser usada para restaurar la identidad en el IdMS. La información archivada también queda disponible para fines estadísticos, históricos o de auditoría. Por último, una identidad podría ser borrada del repositorio de identidades (en la implementación de Udelar las identidades no se borran, sino que quedan archivadas).

Sistemas para gestión de identidades, 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

Existen varios productos que implementan algunas de estas funcionalidades [8]. El IdM Toolkit brinda consideraciones a tener en cuenta a la hora de elegir estos productos. En el caso de Udelar, se utilizaron productos open source (proveedor de identidad y aplicación para autogestión de cuenta) y se optó por hacer un desarrollo propio del módulo que mantiene la información del repositorio de identidades. En esta decisión influyó la disponibilidad de un equipo de desarrollo que contaba con experiencia previa en la implementación de aplicaciones integradas con los sistemas centrales de gestión. Los principales componentes de la solución son:

Repositorio de identidades implementado con un directorio LDAP. Se utilizó OpenLDAP[9] versión 2.4. También se utiliza el módulo provisto por OpenLDAP para definición e implementación de políticas de contraseñas.

Servicio de autenticación que incluye un Proveedor de Identidad SAML y servidores Radius[10] (se describen en el capítulo siguiente).

Sistema que gestiona la información del directorio (Módulo de Gestión de Usuarios, MGU), integrado con los sistemas centrales de gestión de la institución. Se maneja la gestión del ciclo de vida para los distintos tipos de identidades. Actualmente la implementación maneja cuentas de docentes, funcionarios y estudiantes.

Aplicación para gestión de la cuenta por parte del usuario (servicio de tipo “Password Self Service”) Esto incluye activación de cuenta, cambio y recuperación de contraseña mediante preguntas de seguridad. Se utilizó un producto open source: PWM Password Manager [11]

Con respecto a la autorización, el IdP emite atributos que pueden ser utilizados por las aplicaciones para realizar control de acceso. Para algunos sistemas centrales de gestión se almacena en el directorio un valor en cierto atributo que indica que un usuario tiene permiso para acceder al sistema.

También existe un servicio de autorización donde se manejan roles y permisos de usuarios, pero es utilizado únicamente para aplicaciones internas de gestión. Actualmente la solución no brinda herramientas para la gestión de grupos.

El sistema que maneja el ciclo de vida de las identidades (MGU), se integra con los sistemas de gestión de dos formas: obteniendo información o recibiendo información de los mismos a través de una API propia. El mecanismo aplicado en cada caso es:

Integración con el Sistema de RRHH (este sistema es provisto por un proveedor externo). MGU brinda una interfaz gráfica web para el funcionario de RRHH, para buscar al usuario (funcionario o docente), y mediante Web Services se obtiene información del sistema de RRHH, que luego se almacena en el directorio.

Integración con el Sistema de Gestión Estudiantil (Sistema de Gestión y Administración de la Enseñanza, SGAE). Este sistema se desarrolló en la Udelar, y por tanto se tuvo posibilidad de adaptar el mismo para notificar al MGU (vía Web Services) de nuevas identidades estudiantiles y cambios en la información de las mismas, lo cual actualiza el directorio.

Se incluyen procesos de mantenimiento periódicos, para mantener sincronizada la información con los sistemas de gestión (por ejemplo detectar cuando un funcionario ya no está activo).

Por otra parte, también se brindan algunas funcionalidades avanzadas para la Mesa de Ayuda (HelpDesk) central de la Udelar, para poder brindar asistencia en casos excepcionales. Próximamente se prevé incorporar funcionalidades para facilitar la gestión de certificados x509 de usuarios, que generalmente se usan en smart-cards para acceso a sistemas que lo requieran.

Un requerimiento primario es que la fuente principal (autoritativa) de la información son los sistemas centrales de gestión. El repositorio de identidades (directorio) debe tomar de estas fuentes la información, y mantener la coherencia con los mismos. En la Figura siguiente se ilustran los componentes y actores que interactúan actualmente con el directorio.

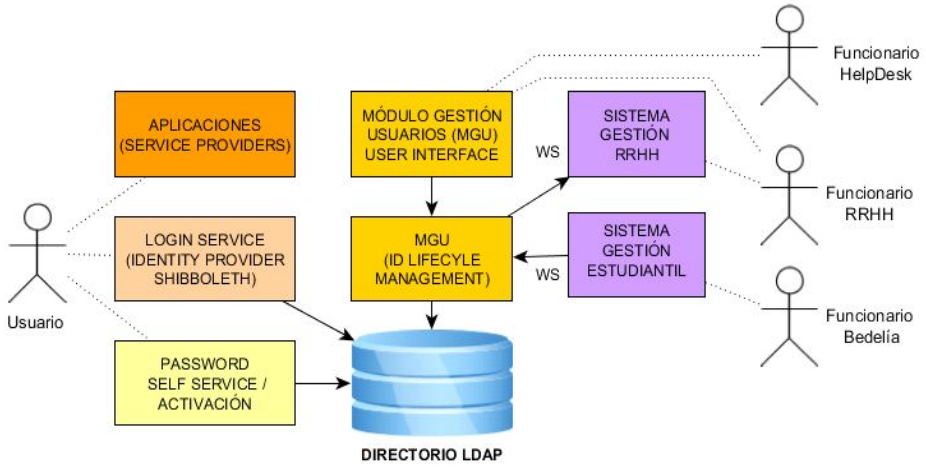

Ilustración : Componentes y actores que interactúan con el directorio.

Procedimiento de registro de nuevo usuario

Para los funcionarios, docentes y estudiantes, se exige una validación presencial de la identidad para la entrega del código inicial que permite acceder a la cuenta de usuario y a las aplicaciones integradas. El procedimiento en el caso de los funcionarios, a grandes rasgos, consiste en:

El usuario concurre presencialmente a la oficina de RRHH, y presenta documento de identidad para solicitar su cuenta de usuario.

El funcionario de la oficina de RRHH verifica la identidad y busca al usuario por documento en el módulo de gestión de usuarios (el cual está integrado al sistema de RRHH, y obtiene datos del mismo). Se genera un código de activación y se entrega al usuario, junto con las condiciones de uso e instrucciones para activar su cuenta. El usuario firma la aceptación de estas condiciones. El módulo almacena la información correspondiente en el directorio LDAP.

El usuario posteriormente debe realizar la activación de su cuenta (puede hacerlo en su casa). En la activación se envía un correo electrónico con un vínculo al que debe acceder (de esta forma se verifica que tenga acceso a dirección de correo declarada). Posteriormente debe elegir una contraseña que cumpla con las políticas de contraseña definidas. Por último, puede responder a una serie de preguntas de seguridad que sirven como mecanismo de recuperación de contraseña en caso de olvido.

Capacitación para las oficinas de RRHH

En 2015, SeCIU realizó una capacitación para los funcionarios de las oficinas de RRHH de más de 20 facultades de la institución sobre los procedimientos relacionados a la gestión de identidades, poniendo énfasis en la importancia de la correcta ejecución de los procedimientos para garantizar la confiabilidad de la información y poder establecer con un mayor nivel de certeza que una identidad digital es utilizada únicamente por la persona que corresponde.

Modelado de la información de identidad.

En el nuevo directorio global, una persona tiene una única entrada, y en caso de tener múltiples afiliaciones (vínculos) con la institución (por ejemplo funcionario y estudiante), se registran múltiples valores en un atributo que indica la afiliación.

El identificador en el directorio es el documento, el cual es una terna formada por pais, tipo y código (número de documento nacional en el caso de los ciudadanos uruguayos). Por razones de privacidad, el documento solamente se comunica a las aplicaciones internas. También se utiliza un identificador único, no reasignable (generado cuando se genera la cuenta del usuario) y se emite dicho valor como identificador para los sistemas externos.

Los esquemas LDAP y los principales atributos utilizados son:

inetOrgPerson y person [12]: se utilizan atributos para almacenar el nombre, direccion de email, password.
EduPerson [13]: se utilizan atributos para almacenar la afiliación (eduPersonAffliation), el identificador único (eduPersonUniqueId).
Esquema con información para autogestión de contraseña (por ejemplo, respuestas de seguridad), propio de la aplicación utilizada (PWM).
udelarPerson: esquema personalizado creado para almacenar otra información.

Algunos atributos definidos en el esquema personalizado (udelarPerson) son:
Afliación extendida que indica con qué unidad organizacional de la universidad tiene vínculo la persona. Se almacena el tipo de afiliación y el código de la unidad. El atributo permite múltiples valores.
Tipo de cuenta y tipo de validación de la identidad realizada (por ejemplo, si fue presencial).
Estado de la cuenta
Información del certificado x509 del usuario (en caso de que utilice)
Si accede a sistemas centrales de gestión, se indica el código del sistema al cual tiene permitido acceder.

También se tiene un registro de eventos relevantes en la entrada del usuario, indicando el origen del evento (dirección IP, hora, operador).

Con respecto a la baja o archivado de las cuentas, se aprovecha la integración con los sistemas de gestión. Se ejecutan procesos que detectan cambios en la afiliación de los usuarios, y si es necesario actualizan el directorio. Si un usuario ya no tiene afiliación, se mantiene la cuenta (sin afiliación) durante un período establecido y luego se archiva. También se utiliza una fecha de expiración.

3 Proveedor de Identidad y Autenticación

La solución cuenta con un proveedor de identidad (IdP) que brinda un servicio central de autenticación. El proveedor de identidad utiliza la especificación SAML 2.0, lo cual permite realizar inicio de sesión único web (Single Sign On, SSO), y provee de información de autenticación y atributos a las aplicaciones integradas.

Se utiliza el perfil más habitual (“Web Browser SSO profile”) de la especificación SAML[5] para

SSO. Dado que existen varias formas posibles de realizar SSO con SAML, se decidió ajustarse a lo establecido por el "SAML interoperability profile" [14], con el objetivo de prepararnos para lograr la mejor interoperabilidad posible a la hora de que los usuarios de Udelar accedan a servicios de otras instituciones en el contexto de una federación e interfederación.

Flujo de acceso a un recurso protegido

En la figura se muestra un diagrama con los principales pasos en el flujo de acceso a un recurso protegido.

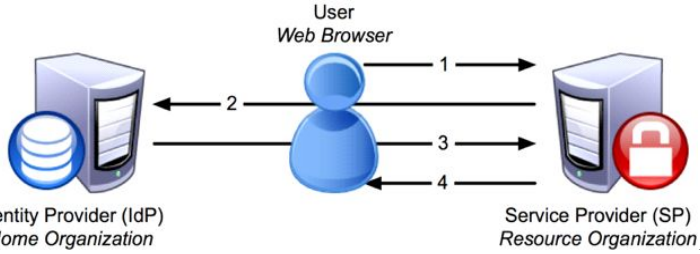

Ilustración : Flujo de acceso a un recurso protegido[15]

El usuario intenta acceder con su navegador web (Web Browser) a una aplicación o recurso protegido (que requiere autenticación) en el Proveedor de Servicio (Service Provider, SP).
El SP intercepta el pedido y redirige al usuario al IdP, en la redirección incluye un pedido de autenticación. El usuario se autentica en el IdP de su institución (Home Organization).
Si la autenticación es exitosa, el IdP redirige al usuario al SP. En esta redirección se incluye un mensaje SAML que contiene datos de la autenticación y algunos atributos del usuario.
El SP verifica la respuesta del IdP y si la misma es válida, el SP retorna el recurso solicitado originalmente por el usuario.

Implementación:

Para implementar este servicio se utilizó Shibboleth IdP [16] en su nueva versión (versión 3). La experiencia con este IdP ha sido muy positiva y podemos comentar varios puntos fuertes:

Open Source, con desarrolladores de muy alto nivel y una comunidad muy activa.
Uno de los mejores productos disponibles, maduro y de amplio despliegue a nivel mundial (se utiliza en el 75% de los IdP registrados en eduGAIN [17]).
Muy buen nivel y rapidez de respuesta ante las dudas planteadas en su lista de usuarios.
Muy configurable y adaptable.

Integración con el directorio LDAP

Shibboleth IdP trae por defecto la posibilidad de integración con directorios LDAP. La integración con OpenLDAP no presentó ningún inconveniente. Una mejora de la versión 3 es la posibilidad de integración con el módulo de políticas de contraseñas de OpenLDAP (ppolicy [18]) lo cual se puede realizar ajustando la configuración [19].
La integración del IdP con OpenLDAP ppolicy permite que se pueda informar al usuario en la misma página de inicio de sesión de que la autenticación ha fallado a causa de que la cuenta está bloqueada o la contraseña expirada, o incluso poder dar una advertencia de que la contraseña está

próxima a expirar.

Autenticación con certificados x509 de cliente.

Shibboleth IdP permite el uso simultáneo de distintos módulos de autenticación. Incluso un SP particular puede indicar el tipo de autenticación que desea. En Udelar se utiliza la autenticación con contraseña, y actualmente está en etapa de pruebas la autenticación con certificados x509 de cliente (se cuenta con un prototipo que funciona correctamente). En la versión 2 de Shibboleth se requería un módulo adicional para este tipo de autenticación, pero en la versión 3 lo trae incluido y es suficiente hacer un ajuste en la configuración [20].

En Udelar se utilizan smart-cards con certificados x509 de cliente para el acceso a sistemas que requieren mayor protección, como por ejemplo sistemas financieros centrales. Actualmente se utilizan smart-cards para el acceso a algunos sistemas web y para esto se utiliza un módulo agregado a Apache que se integra directamente con el directorio LDAP [21]. Este módulo no está actualizado para las últimas versiones de Apache y se prevé utilizar el IdP para brindar esta funcionalidad.

Infraestructura y performance

El proveedor de identidad ejecuta en una plataforma con las siguientes características:
Máquina virtual VMWare con 2 GB de RAM y 4 cores.
Sistema Operativo Debian 8
Oracle Java 1.8, Apache Tomcat 8
Apache HTTP Server 2.4 como reverse proxy.
OpenLDAP 2.4

La performance ha sido buena, y de acuerdo a la documentación existe la posibilidad de escalar si es necesario [22]. Hay estudios de performance disponibles, contribuidos por otras universidades [22], incluyendo tests Jmeter [REF] ya preparados, que pueden descargarse y ejecutarse [22]. En Udelar se utilizó uno de estos test (utilizando la configuración de “unsolicited login”) para realizar pruebas de carga sobre la infraestructura mencionada. En la figura siguiente se muestran los tiempos de respuesta a lo largo del tiempo de la prueba.

En la prueba se realizaron 10000 inicios de sesión (100 hilos, con 100 iteraciones cada hilo). El tiempo total que insumió esta prueba fue 1:54 minutos, lo que corresponde a un throughput de 87 inicios de sesión por segundo.

Cada inicio de sesión de la prueba involucra dos pedidos HTTP: un GET y luego un POST. Con esta cantidad de hilos la latencia para la gran mayoría de estos pedidos se ubica entre 300 y 900 ms. Esto se considera aceptable para el uso esperado del IdP, considerando la cantidad de hilos concurrentes. En situaciones de menor carga, se han observado latencias por debajo de los 100 ms.

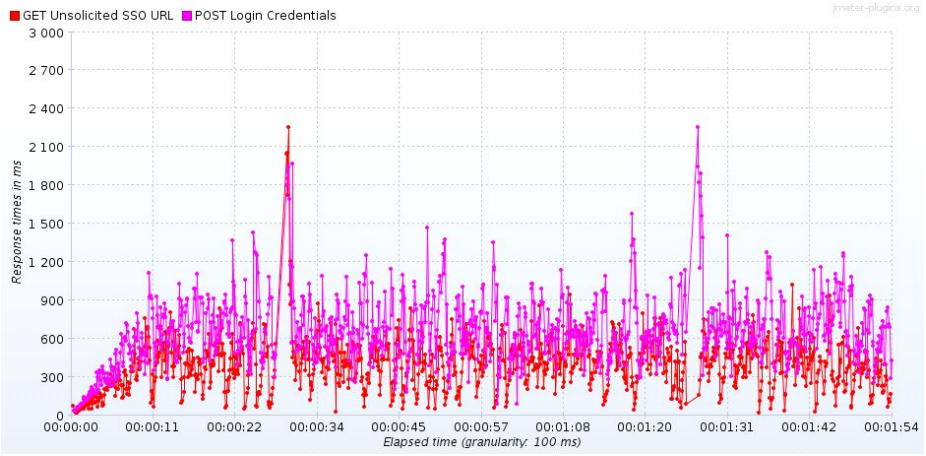

Ilustración : Tiempos de respuesta en la prueba de carga

Traducción al español

Shibboleth IdP versión 3 por defecto incluye únicamente mensajes en inglés (textos que se muestran al usuario en las páginas del IdP), pero existe la posibilidad de traducir estos mensajes. En la Udelar se realizó la traducción al español de los mensajes. En octubre de 2015, en la comunidad de Shibboleth surgió la iniciativa de contar con un repositorio de traducciones, y Udelar contribuyó con la traducción al español, de forma que otros usuarios de habla hispana del IdP puedan descargarla y utilizarla [23]. Posteriormente se ha mantenido esta traducción, adaptándola ante los cambios de versión que incluyen nuevos mensajes. Cabe agregar que los desarrolladores de Shibboleth han manifestado que es posible que se agreguen estas traducciones al paquete principal del IdP en una próxima versión.

Atributos

El proveedor de identidad puede comunicar atributos del usuario autenticado a las aplicaciones (Service Providers, SP). En este punto, es importante considerar reglamentaciones de protección de datos personales que puedan aplicar. Shibboleth IdP permite controlar esta emisión de atributos en varios niveles. En su versión 3 trae incluido un módulo de consentimiento, en el cual el usuario puede aprobar (o no) que se entregue cierta información a una aplicación. También es posible definir reglas de filtrado de atributos en el IdP, e indicar qué atributos se pueden emitir a cada SP. Un ejemplo de uso es el filtrado del documento de identidad del usuario, que se emite únicamente a aplicaciones internas de la Udelar.

A nivel internacional, en las federaciones de educación e investigación, se ha planteado el problema de la emisión de atributos de manera segura en relación a la protección de datos. En este sentido, es relevante el concepto de la categoría “Research and Scholarship Entity Category” [24] que permite de manera segura emitir un pequeño conjunto de atributos preestablecido a Service Providers que han probado que requieren estos atributos para fines de educación e investigación. Shibboleth IdP permite la implementación de estas categorías, lo cual también facilita la configuración del filtrado de atributos a mayor escala.

Shibboleth IdP también puede actuar como autoridad emisora de atributos, en forma independiente de la autenticación. En la especificación de SAML se define un formato estandarizado para las consultas de atributos (AttributeQuery). Un ejemplo de uso es cuando una aplicación (SP) utiliza un IdP para la autenticación, pero luego requiere atributos de un segundo IdP. En Udelar se han probado prototipos de este escenario, y un uso previsto es que sistemas de algunas facultades que utilizan otro tipo de autenticación propio, puedan hacer consultas de atributos al IdP.

Atributos recomendados para eduGAIN

Con el objetivo de maximizar las posibilidades de interoperabilidad y colaboración en un contexto de interfederación, eduGAIN recomienda que los IdP de las federaciones participantes puedan emitir un conjunto determinado de atributos que son los más requeridos por los Service Providers a nivel internacional. Esta recomendación se expresa en el "eduGAIN attribute profile" [25].

En el diseño del directorio de la Udelar se tuvo en cuenta la conveniencia de la compatibilidad con eduGAIN, y actualmente el IdP puede emitir todos los atributos recomendados en este profile. En resumen, los atributos principales son:

Nombre y correo (atributos displayName, commonName y mail)
Afiliación (eduPersonAffiliation y eduPersonScopedAffiliation)
Nombre de usuario (eduPersonPersonPrincipalName) En este caso se utiliza un identificador del usuario opaco, único y persistente del tipo 20120508@udelar.edu.uy, que sólo se utiliza en el sistema de gestión de identidad. No se emite el documento de identidad.
Identificador dirigido (eduPersonTargetedID/persistentID) Es un identificador único, persistente y opaco, distinto para cada SP, lo cual brinda la posibilidad de mayor privacidad al no permitir correlacionar actividad del usuario en distintos SP [13]. A nivel técnico, el IdP de Udelar puede emitir identificadores de tipo "persistent" y "transient", cumpliendo con el criterio recomendado en el SAML interoperable profile [14]. Esto puede agregarse en el IdP mediante configuración. En concreto se agregó a la configuración por defecto un generador de identificadores persistentes [26].

4 Integración de aplicaciones y servicios

En el modelo de SAML, se utiliza el termino "Service Provider" o "SP" para referirse a la aplicación, servicio o recurso que se ofrece al usuario y que se integra con el IdP para realizar la autenticación. El SP es responsable por la protección de un recurso y consume información provista por el IdP. También se utiliza el término "Relying Party", pues el SP es la parte que confía en la autenticación realizada por el IdP, y en los atributos que le informa.

Este modelo de confianza entre SP y IdP requiere un intercambio inicial de certificados para que estas entidades puedan utilizar firma digital y encriptación en los mensajes que intercambian. A nivel técnico, cuando se integra un nuevo SP se realiza un intercambio de metadata SAML[5] que contiene la información necesaria para esta interacción (certificados x509, URLs, protocolos soportados, etc.).

La solución de Udelar utiliza Shibboleth SP, que consiste en un módulo que se agrega al servidor web (Apache o IIS), y realiza el manejo de los mensajes SAML, permite configurar la forma de control de acceso y simplifica la integración de las aplicaciones. En la configuración del servidor web se pueden definir los recursos que se quiere proteger y de qué forma. En caso de un intento de acceso a un recurso protegido, el módulo se encarga de interceptar el pedido, preparar un pedido de autenticación y redirigir al usuario al IdP. En caso de una autenticación exitosa, el módulo recibe y procesa el token SAML emitido por el IdP, realiza varios chequeos de seguridad, y si el pedido es válido permite el acceso del usuario al recurso solicitado. El módulo también carga en variables de entorno o headers HTTP los atributos informados por el IdP, para que sea sencillo para las aplicaciones acceder a esta información.

En Udelar se realizó con éxito la integración de varias aplicaciones implementadas en distintos lenguajes. Se integraron aplicaciones Java (ejecutando en servidores de aplicaciones Apache Tomcat y JBoss), PHP, GeneXus [27] e incluso aplicaciones web legadas implementadas con Oracle PL/SQL (implementadas hace más de 20 años). Cabe agregar que muchas aplicaciones y servicios existentes permiten autenticación con Shibboleth, desde CMS y LMS hasta servicios cloud [28].

La integración al IdP de algunas aplicaciones ya existentes (desarrolladas en Udelar), requirió

cambiar la forma de autenticación de las mismas. En esta experiencia el proceso fue sencillo y requirió poco esfuerzo, incluso se puede decir que se simplificó la implementación del inicio de sesión de las mismas. Por otra parte, con el IdP se facilitó parte de la implementación de nuevas aplicaciones, al no requerir en las mismas el manejo de identidades y autenticación. Esto ha posibilitado la implementación en menores tiempos de nuevas aplicaciones que requieren acceso autenticado.

Este modelo también plantea ventajas en cuanto a la seguridad, pues por ejemplo se evita que las aplicaciones deban implementar mecanismos de autenticación, manejo y almacenamiento de identidades y contraseñas, lo cual presenta riesgos de seguridad si es implementado pobremente.

Accesos registrados y perspectivas

En Udelar se comenzó a utilizar el IdP en agosto de 2015 con una aplicación denominada "Módulo de Autogestión de Personal". El uso de esta aplicación ha ido en aumento y actualmente se observan más de 1000 ingresos diarios. Por otra parte, en setiembre de 2015 se realizó un censo de funcionarios (autenticados con el IdP), y completaron el mismo más de 15000 funcionarios. En abril de 2016 se incorpora la certificación médica vía web. Los próximos pasos en el corto plazo son:

En setiembre de 2016 se comenzará a utilizar el IdP para autenticar a los estudiantes de Udelar, y se integrará una nueva aplicación de autogestión estudiantil (permite por ejemplo la inscripción a cursos y exámenes).
Está en camino la incorporación de aplicaciones desarrolladas fuera del Servicio Central de Informática, lo que abre la posibilidad para que entidades externas aprovechen la autenticación del IdP
Está en etapa de pruebas la incorporación de sistemas financieros, utilizando autenticación fuerte en el IdP con smart-cards.

Eduroam y Radius

La Red Académica Uruguaya (RAU) ha trabajado para el despliegue de eduroam [29][30] en Uruguay y en la Universidad, lo cual se ha concretado recientemente. El servidor Radius utilizado para eduroam en la Udelar se ha integrado con el directorio del IdP, lo cual permite que los usuarios puedan utilizar eduroam, con la misma contraseña que utilizan en el IdP web.

Udelar también brinda un servicio de autenticación Radius. Este servicio se ha utilizado desde hace años en las facultades para autenticar estudiantes y es utilizado en aplicaciones web, gestores de contenido educativo, y en algunos casos en el login de sistemas operativos. Este servicio utiliza desde sus inicios una base de datos como backend de autenticación. En setiembre de este año se prevee migrar estas cuentas de usuario (manteniendo el servicio Radius) e integrarlo con el directorio del IdP, lo cual permitirá centralizar y unificar las identidades, y que los usuarios utilicen la misma contraseña para las distintas aplicaciones. Para las migraciones de datos se ha utilizado con éxito una herramienta open source (Talend [31]).

6 Federación de identidades

Una Federación de Identidad es una asociación de organizaciones, las que se unen para intercambiar información, tanto de sus usuarios como de sus recursos, de acuerdo a ciertas políticas, con la finalidad de permitir la colaboración. Estas federaciones son creadas con el fin de facilitar y simplificar la introducción de servicios compartidos a través de la federación. Esto se logra usando tecnologías federadas como SAML, las que permiten extender el alcance de una identidad digital emitida por un miembro de la federación y que esta sea válida en toda la federación.

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. Se ha trabajado en contacto con integrantes de eduGAIN y se ha avanzado en las políticas de la federación y los demás requerimientos para la incorporación [32]. Se prevé completar este trabajo en los próximos meses.

Referencias

[1]E. Bertino y K. Takahashi, Identity Management: Concepts, Technologies, and Systems. Boston: Artech House, 2010.
[2]P. J. Windley, Digital Identity, 1st edition. Sebastopol, CA: O'Reilly Media, 2005.
[3]eduGAIN. [En línea]. Disponible en: http://services.geant.net/edugain/Pages/Home.aspx [Accedido: 30-jun-2016].
[4]REFEDS – The Voice of Research and Education Identity Federations. https://refeds.org/ [Accedido: 30-jun-2016].
[5]SAML Specifications | SAML XML.org. [En línea]. Disponible en: http://saml.xml.org/saml-specifications [Accedido: 30-jun-2016].
[6]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 [Accedido: 30-jun-2016].
[7]Identity Management infoKit / Home. https://www.identity-project.org [Accedido: 30-jun-2016].
[8] Top Identity Management Software Products http://www.capterra.com/identity-management-software/ [Accedido: 30-jun-2016]
[9]OpenLDAP, Main Page. http://www.openldap.org/ [Accedido: 30-jun-2016].
[10]FreeRADIUS: The world's most popular RADIUS Server. http://freeradius.org/ [Accedido: 30-jun-2016].
[11]Proyecto PWM, GitHub. https://github.com/pwm-project/pwm [Accedido: 30-jun-2016].
[12]Definition of the inetOrgPerson LDAP Object Class. https://tools.ietf.org/html/rfc2798 [Accedido: 30-jun-2016].
[13]eduPerson & eduOrg | Internet2. http://www.internet2.edu/products-services/trust-identity/eduperson-eduorg/ [Accedido: 30-jun-2016].
[14]The (SAML2Int) Interoperable SAML 2.0 Profile.http://saml2int.org/. [Accedido: 30-jun-2016].
[15]Shibboleth Concepts https://wiki.shibboleth.net/confluence/display/CONCEPT/Home [Accedido: 30-jun-2016].
[16]Shibboleth. https://shibboleth.net/ [Accedido: 30-jun-2016].
[17] Global Shibboleth IdP Deployments https://spaces.internet2.edu/display/InCFederation/Global+Shib+IdP+Deployments [Accedido: 30-jun-2016].
[18]OpenLDAP Software 2.4 Administrator's Guide: Overlays. http://www.openldap.org/doc/admin24/overlays.html [Accedido: 30-jun-2016].
[19]LDAPAuthnConfiguration - Identity Provider 3. https://wiki.shibboleth.net/confluence/display/IDP30/LDAPAuthnConfiguration [Accedido: 30-jun-2016].
[20]X509AuthnConfiguration - Identity Provider 3.https://wiki.shibboleth.net/confluence/display/IDP30/X509AuthnConfiguration. [Accedido: 30-jun-2016].
[21]ARESU - Architecture réseaux, expertise, services unités. https://aresu.dsi.cnrs.fr/spip.php?rubrique41 [Accedido: 30-jun-2016].
[22]Load Testing Contributed Results - Identity Provider 3. https://wiki.shibboleth.net/confluence/display/IDP30/Load+Testing+Contributed+Results [Accedido: 30-jun-2016].
[23]MessagesTranslation - Identity Provider 3. https://wiki.shibboleth.net/confluence/display/IDP30/MessagesTranslation [Accedido: 30-jun-2016].
[24] Research and Scholarship Entity Category. https://refeds.org/category/research-and-scholarship [Accedido: 30-jun-2016].
[25]eduGAIN attribute profile. http://services.geant.net/edugain/Resources/Documents/GN3-11-012%20eduGAIN_attribute_profile.pdf [Accedido: 30-jun-2016].
http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201310.html#eduPersonTargetedID [Accedido: 30-jun-2016].
[26]Persistent NameID Generation Configuration https://wiki.shibboleth.net/confluence/display/IDP30/PersistentNameIDGenerationConfiguration [Accedido: 30-jun-2016].
[27] Genexus http://www.genexus.com/
[28] Shibboleth Enabled Applications and Services https://wiki.shibboleth.net/confluence/display/SHIB2/ShibEnabled
[29]Eduroam https://www.eduroam.org/
[30]Eduroam UY http://eduroam.uy/

[31]Talend Real-Time Open Source Data Integration Software. https://www.talend.com/ [Accedido: 30-jun-2016].
[32] Join Edugain https://technical.edugain.org/joining_checklist