La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología -ATENEA- ha implementado una plataforma de gestión de aprendizaje (LMS) de código abierto Moodle versión 4.5+ alojada en una nube pública en infraestructura de Atenea. A esta plataforma se le denomina Academia Atenea, que hará el rol de *Customer* en el esquema de interoperabilidad.

Para garantizar la interoperabilidad de Academia Atenea con sistemas externos (*provider*), se establecen los siguientes requisitos técnicos para una integración a múltiples plataformas mediante *Single Sign-On* (SSO).

1. Fichas técnicas admitidas para las plataformas del operador (*provider)*

Los proponentes deben asegurar que su plataforma soporta la integración con el IDP de ATENEA dependiendo de los siguientes escenarios

1.1 Cuando la plataforma del proponente (*provider)* es Moodle 4+

Para este escenario, se configurará será el **LTI1.3.** Este modelo de interoperabilidad es el óptimo ya que es el protocolo que usan las versiones de Moodle 4+ y ha sido probado con éxito en ATENEA en vigencias anteriores con otras instituciones. Su flexibilidad permite que el usuario pueda transitar de una plataforma a otra sin tener que realizar doble inicio de sesión.

1.2 Cuando la plataforma del operador (*provider)* no es Moodle o es una versión anterior a 4+

En caso de que la plataforma proveedora (*provider*) sea un desarrollo a la medida o sea otro tipo de LMS versión anterior a 4+, el operador necesitará exponer los datos a través de otros, tales como:

- **SAML 2.0**
- **OAuth 2.0**
- ***OpenID Connect*** (OIDC, basado en *OAuth* 2.0 para autenticación federada).

Nota: ATENEA no cubrirá los gastos del operador en desarrollo de API, Endopint, Webhook o cualquier otro método de interoperabilidad dentro de la plataforma *provider*.

2. Requisitos técnicos

Para todos los escenarios descritos, se necesita un equipo técnico administrador de la plataforma, que, mediante mesas técnicas con ATENEA sea corresponsable de los ejercicios de interoperabilidad del lado *provider,* es decir, que tenga el conocimiento técnico requerido y los permisos sobre la plataforma *provider.*

2.1 Para integración vía LTI1.3

Antes de iniciar las configuraciones, el proponente operador debe verificar los siguientes requisitos previos:

PÚBLICA

- Verificar que no haya restricciones de seguridad que impida el tráfico entre ambas plataformas (por ejemplo, reglas de firewall)
- Suministrar a ATENEA una cuenta con perfil de profesor en la plataforma *Provider*
- Verificar que el plugin de autenticación está activo
- Verificar que la opción “Publicar como herramienta LTI” esté activa

Durante la sesión de integración, es necesario que el proponente operador proporcione los siguientes parámetros que hacen parte de la configuración del protocolo:

- URL de la herramienta
- URL para la autenticación inicial
- URL JWKS
- URL enlazado profundo

Nota: En sesiones técnicas conjuntas se indicará el paso a paso para la interoperabilidad con LTI1.3

2.2 Para integración vía SAML 2.0

El proponente proveedor del servicio (*Service Provider*, SP) debe proporcionar:

- **Entity ID del SP**: Identificador único del proveedor (ej: urn:ejemplo:sp).
- **URL de *Assertion Consumer Service* (ACS)**: Endpoint donde ATENEA enviará las respuestas SAML.
- **Certificado X.509 público**: Para validar las firmas de las solicitudes SAML.
- **Algoritmo de firma**: SHA-256 (obligatorio por políticas de seguridad).
- ***Binding***: HTTP-POST (preferido) o HTTP-*Redirect*.
- **Atributos requeridos**: Como mínimo, NameID (identificador único del usuario) y atributos opcionales como email o roles.

Configuración en Moodle 4.5+:

- ATENEA actuará como ***Identity Provider* (IdP)** y compartirá los metadatos SAML (URL del SSO, certificado público y *entity* ID) con el proveedor.

2.3 Para integración vía OAuth 2.0

El proponente proveedor del servicio (*Service Provider,* SP) debe proporcionar:

- **Issuer URL**: Endpoint de autenticación (ej: https://auth.oci.ejemplo.com).
- **Client ID y Client Secret**: Credenciales proporcionadas por ATENEA para el registro del SP.
- **Scopes requeridos**: openid, profile, email (para autenticación básica).
- **Endpoints**:
- URL de autorización: https://auth.oci.ejemplo.com/oauth2/v1/authorize.

PÚBLICA

- URL de token: https://auth.oci.ejemplo.com/oauth2/v1/token.
- **JWKS endpoint**: Para validación de tokens JWT (ej: https://auth.oci.ejemplo.com/oauth2/v1/keys).

Nota: Moodle 4.5+ soporta OAuth 2.0 mediante *plugins* nativos.

2.4 Para integración vía OpenID Connect (OIDC)

Requisitos similares a OAuth 2.0, con énfasis en:

- Uso del *scope* openid.
- Validación de tokens ID mediante el *endpoint* userinfo.

3. Seguridad

- **Certificado SSL/TLS**: Todos los *endpoints* del SP deben usar HTTPS con certificados válidos.
- **IPs permitidas**: El SP debe permitir conexiones desde las IPs públicas de nube pública usadas por ATENEA (a proporcionar durante la implementación).

4. Información adicional

Para evaluar la compatibilidad técnica, el proponente debe proporcionar la siguiente información:

1. **Plataforma de alojamiento**: Detalle si el SP se hospeda en OCI, AWS, Azure, u on-premise.
2. **Restricciones de red**: Lista de puertos, IPs o firewalls que requieran configuración.
3. **Pruebas de interoperabilidad**: Capacidad para realizar pruebas en un entorno de preproducción antes del despliegue.

5. Soporte y documentación

- El proveedor debe entregar la documentación técnica detallada de su implementación SSO al finalizar el contrato.
- ATENEA proporcionará metadatos SAML o credenciales OAuth/OIDC para la integración.
- El proponente deberá disponer de recurso humano especializado o con conocimiento en funcionamiento de la plataforma con el cual se pueda interactuar técnicamente acerca de aspectos propios de interoperabilidad.

PÚBLICA