Personalización de Araí-Usuarios para uso de SSO externo

Universidad Nacional de Córdoba

Situación en UNC

- Se cuenta con un autenticador centralizado (SSO)
- El SSO permite autenticar diferentes sistemas con diversos protocolos de autenticación

Ejemplos de sistemas:

- GDE
- Proxy
- Eduroam
- Guaraní
- Google
- Moodle
- Drupal
- Sistemas desarrollados en la UNC

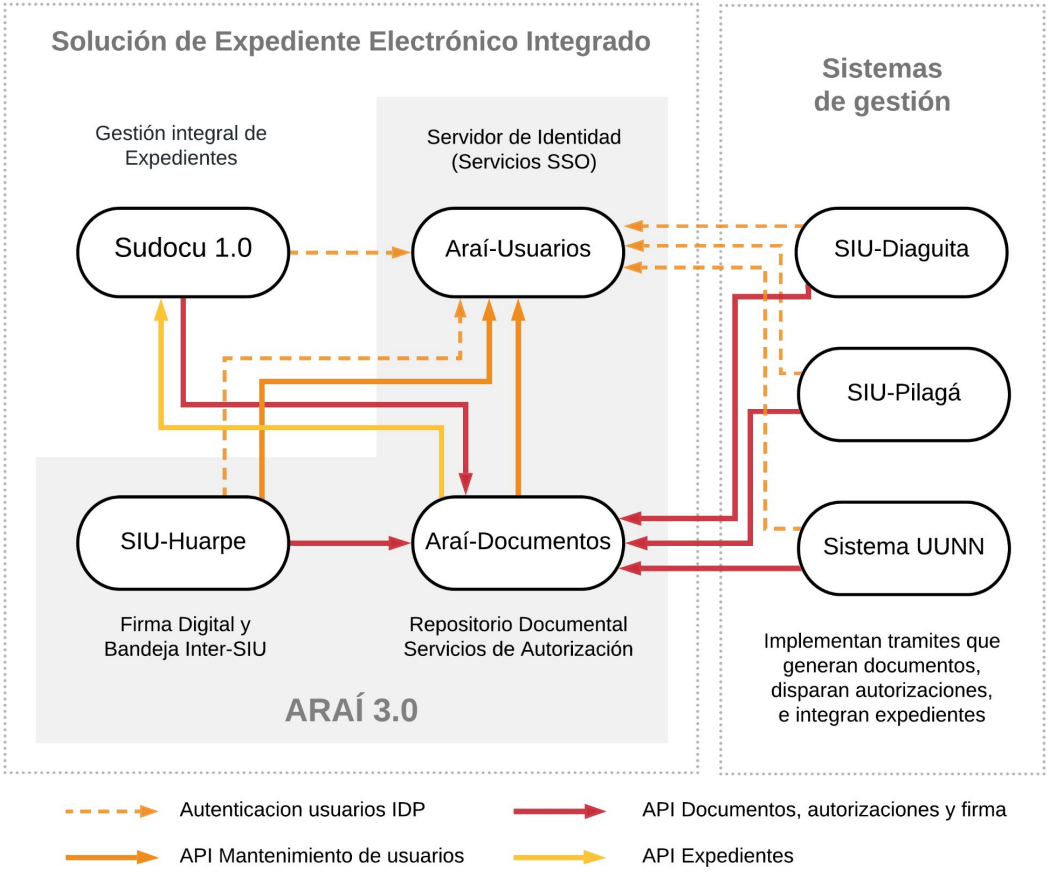
Ejemplos de protocolos:

- CAS
- OAuth
- SAML
- OpenID Connect
- Radius

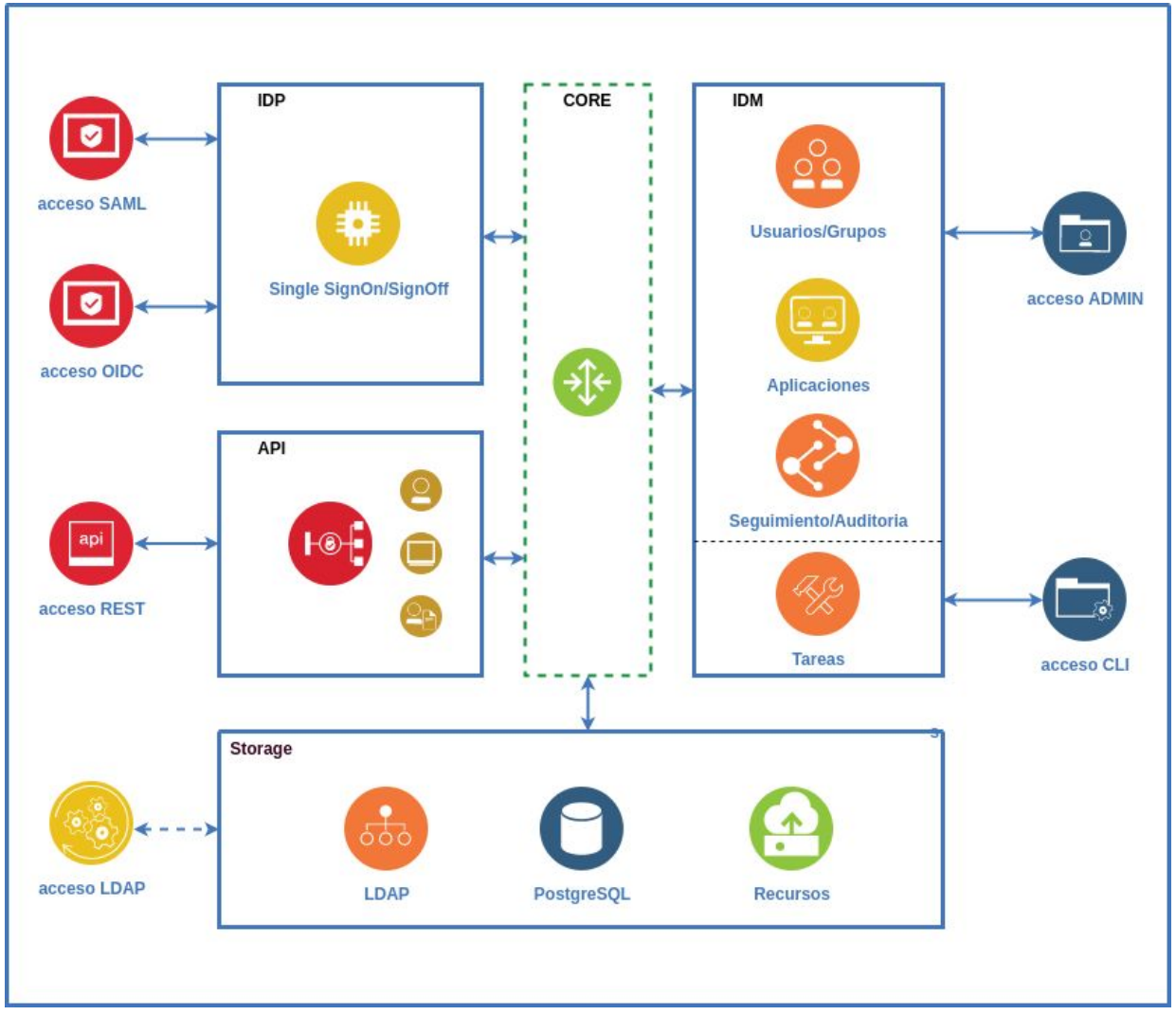
Necesidad

- Autenticar los diversos sistemas SIU por medio de algún protocolo con el autenticador de la UNC (SSO)
- Contar con un gestor o administrador de usuarios descentralizado.

¿Qué ofrece SIU?



Araí Usuarios



¿Qué estrategias de integración brinda SIU?

- Adopción exclusiva del SSO del SIU
  - La universidad ya cuenta con un SSO por lo cual no se desea mantener otro SSO.
  - El SSO de SIU brinda soporte al protocolo SAML

- Integración híbrida
  - Requiere un mecanismo de sincronización de datos entre SSO de la universidad y Arai-Usuarios.

- Desarrollar la personalización para integrar con Arai-Usuarios
  - Requiere modificaciones específicas en el SSO propio:
    - Personalizar el token SAML con atributos adicionales que son esperados por los módulos SIU.
    - Mapear atributos del token con datos del backend del IDM en caso que los valores se encuentren almacenados con otra estructura

Fuente: https://documentacion.siu.edu.ar/usuarios/docs/next/cache/estrategia-integracion/

Solución implementada

Hacer que Araí funcione como un **Proxy IdP**, es decir:

- trabajar como IdP (del protocolo SAML) para los sistemas SIU y
- trabajar como un SP para el SSO de la Universidad.

Deshabilitar la posibilidad de cambiar la contraseña en Huarpe

Contar con un endpoint que permita dar de alta usuarios con un uid determinado.

Pasos - Araí usuarios IDP

1. Copiar código fuente de arai-usuarios
2. Crear los siguientes archivos php en el proyecto idp para que arai-usuarios delegue el proceso de autenticación en el SSO de la universidad

```
|-- idp
    |-- /simplesamlphp-module-arai/lib/Auth/Source/AraiProxyAuth.php
    |-- /config/simplesamlphp/
        |-- authsources.php
        |-- saml20-idp-hosted.php
        |-- saml20-idp-remote.php
```

Pasos - Araí usuarios IDP

3. Crear archivos **AraiProxyAuth.php** para sobrescribir los métodos de autenticación y logout usados por Araí, a fin de delegar el proceso al “nuevo” IdP (SSO de la universidad).

Pasos - Araí usuarios IDP

4. Editar archivo **authsources.php**.

Éste es el archivo de configuración de la librería SimpleSAMLphp que establece qué sistemas de autenticación y autorización pueden ser utilizados.

Pasos - Araí usuarios IDP

```
<?php

$config = array(

    'usuarios_arai' => array(
        //'arai:AraiAuth' // Authentication source used by default by Araí
        'arai:AraiProxyAuth' // Authentication source used by UNC to deletage flow to SSO
     ),

    // Authorize with SSO UNC, doing IdP bridging
    'sso_unc' => array(
        'saml:SP',
        'idp' => 'https://sso.unc.edu.ar/idp',

        // Using the same keys for IdP and SP
        'privatekey' => 'certificado_idp.key',
        'certificate' => 'certificado_idp.crt'
    ),

);
```

Pasos - Araí usuarios IDP

5. Editar archivo **saml20-idp-remote.php**

Este archivo contiene la metadata del IdP usado por Araí para delegar las autenticaciones.

Pasos - Araí usuarios IDP

6. saml20-idp-hosted.php

Este archivo ya existe y se encuentra correctamente configurado en Araí.

Ya que Araí funciona como IdP para los sistemas SIU.

Pasos - Araí usuarios IDP

7. Crear Dockerfile:

```
FROM hub.siu.edu.ar/siu/expedientes/arai-usuarios/idp:v3.1.10 as idp

COPY AraiUNCAuth.php idp/simplesamlphp-module-arai/lib/Auth/Source/AraiProxyAuth.php

COPY authsources.php idp/config/simplesamlphp/authsources.php

COPY saml20-idp-remote.php idp/config/simplesamlphp/saml20-idp-remote.php
```

Pasos - Araí usuarios IDP

8. Mapeo de usuarios del SSO de la universidad y Araí Usuarios

Araí Usuarios utiliza una base de datos LDAP para mantener un registro de sus usuarios, y un mapeo de cada usuario con su respectiva cuenta en los distintos sistemas SIU. De los atributos almacenados en dicha base, uno de los más importantes es el **uid**, usado por Araí para reconocer usuarios.

Cuando se delega la autenticación de los usuarios en el SSO de la universidad, Araí espera que este le pase en la respuesta el atributo uid para poder identificar de qué usuario de su base de datos se trata.

Para que se puedan autenticar usuarios existentes en en el sistema de usuarios de la UNC a la hora de acceder a Araí, es necesario crear usuarios en la base LDAP de Araí cuyo uid se corresponda con un id de usuario del sistema de usuarios de la UNC

Pasos - Huarpe

9. Deshabilitar el cambio de contraseña en Huarpe

Se asigna el valor cero a la variable de entorno BUNDLE_USUARIOS_UPDATE_PWD para el contenedor de huarpe

Pasos - Araí usuarios API

10. Se agrega un nuevo recurso a la API de Arai usuarios para realizar el alta de usuarios aceptando el formato de dato que se le envía como uid. También se elimina la solicitud de email y password.

Uso de la Araí usuarios API

11. Se crea Dockerfile:

```
FROM hub.siu.edu.ar/siu/expedientes/arai-usuarios/api:v3.1.10 as api

COPY recurso_usuarios.php
api/src/SIU/AraiUsuarios/API/Endpoints/v2/unc/recurso_usuarios.php

COPY UsuariosManager.php core/src/SIU/AraiUsuarios/Core/UsuariosManager.php
```

Demo

Gracias!

Contacto UNC: desarrollo@informatica.unc.edu.ar