



Middleware for collaborative Applications and Global vIrtual Communities

WP2 AAI - Federación de Identidades

F E N I X



Magic

Middleware for collaborative Applications
and Global virtual Communities



CONACYT

Consejo Nacional de Ciencia y Tecnología

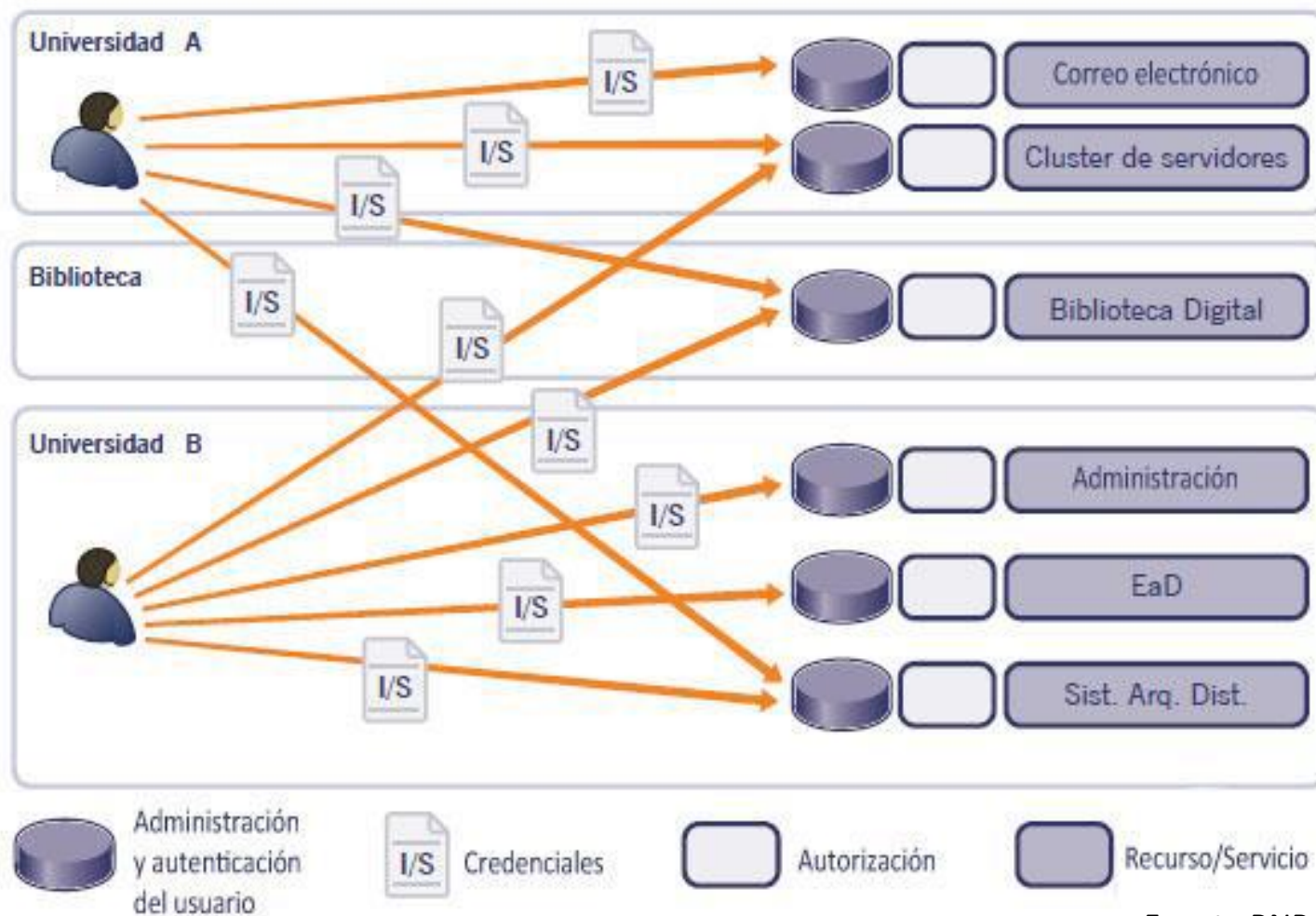
Objetivo del despliegue de AAI

- Crear una Infraestructura de **A**utorización y **A**utenticación para servicios y procesos académicos, de las RNIE's de África, Asia, el Caribe y América Latina.
- Impulsar la creación de sus **propias Federaciones de Identidad**, facilitando la integración con iniciativas Europeas haciendo posible la unión de servicios **inter-federados**.

Federación de Identidad

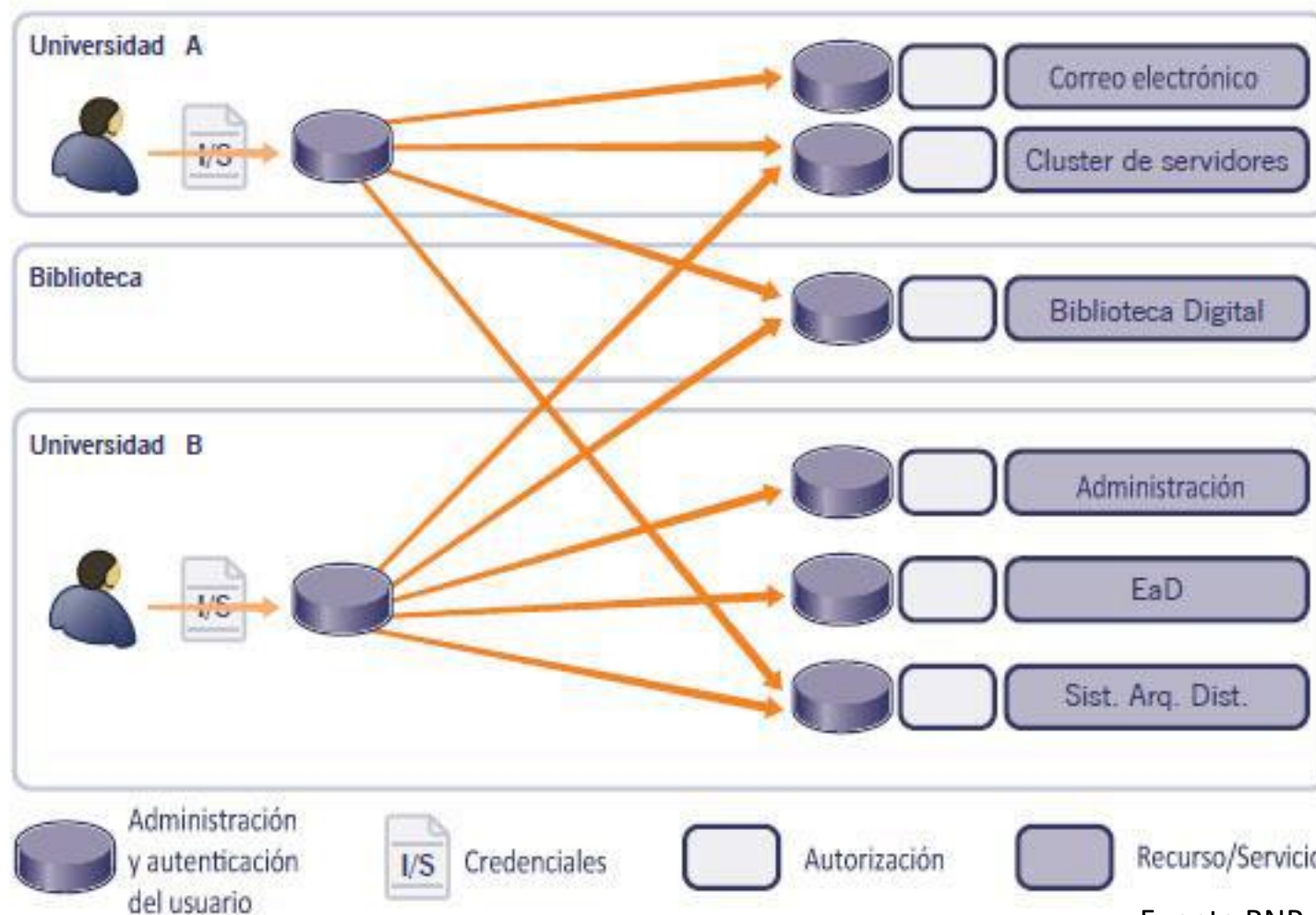
- Es una red de confianza que implementa un método de autenticación manteniendo la interoperabilidad.
- Funciona a través de un acceso seguro basado en Web, que autoriza a un usuario, para que a través de una sola firma pueda utilizar un conjunto de recursos digitales ofrecidos por una federación.
- Estos recursos pueden ser de su propia Institución y/o de otras, con las que la federación tenga convenio.

Sistema tradicional



Fuente RNP

Sistema federado



Fuente RNP

Elementos de una federación

- Proveedor de Identidad (IdP), almacena y gestiona la información de los usuarios.
- Proveedor de Servicio (SP), ofrece un servicio restringido a un grupo de usuarios.
- Servicio de Descubrimiento (DS / WAY), elemento que centraliza, la información sobre los IdP's.

Actores de una federación

- Usuario, persona vinculada a la institución, que quiere hacer uso de un recurso restringido.
- Proveedor del recurso, una aplicación asociado a un componente de proveedor de servicio.
- Institución del usuario, que tiene al proveedor de identidad y lleva a cabo la autenticación del usuario.

Servicio de Descubrimiento

- El proveedor de servicio permite el acceso de usuario de diferentes instituciones, a través de DS/WAYF la federación centraliza la información sobre los proveedores de identidad, para que el selección la institución a la que pertenece y la cual validará sus credenciales para que tenga acceso al recurso que protege el SP.

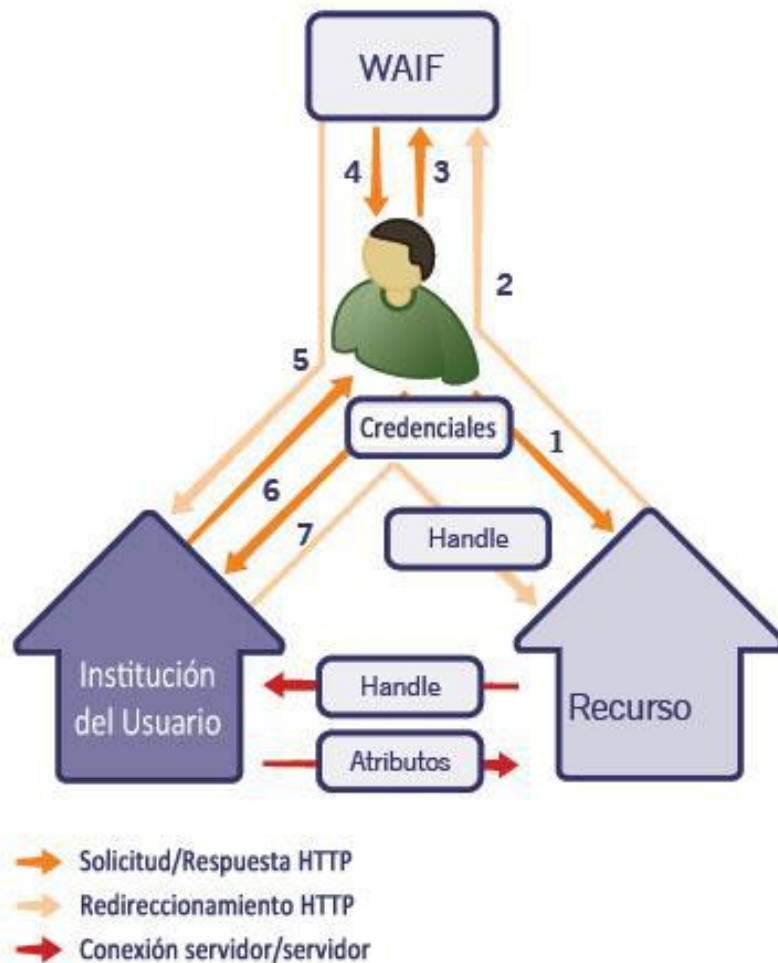
Proveedor de Identidad

- Implementa una política interna de gestión de identidad.
 - Atributos de los usuarios: Nombre, fecha nacimiento, cargo, ID.
- Metodo de autenticación.
 - Login / contraseña, certificados digitales, etc.
- Otorga un identificador único para cada usuario de la institución.

Proveedor de Servicio

- Implementa los servicios que deben estar disponibles para los usuarios de las instituciones y requieren:
 - Autenticación, identificación de los usuarios
 - Autorización, atributos adicionales que garantizan ciertos privilegios de acceso.
- Su enfoque está en la implementación del servicio y no en el mantenimiento de los registros de los usuarios.

Interacción entre elementos de una FI



Fuente RNP

- 1: El usuario accede al proveedor de servicio (SP)
- 2: El servicio presenta opciones del DS/WAYF centralizado.
- 3: El usuario selecciona su institución de origen.
- 4: El usuario es redirigido hacia su (IdP).
- 5: El IdP autentica al usuario con el método elegido por la institución.
- 6: El SP recibe la garantía de autenticación del usuario de parte del IdP.
- 7: El SP pide atributos adicionales de ese usuario al IdP; para garantizar la privacidad del usuario, sólo se entregan atributos previamente acordados entre el IdP y el SP.
- 8: El proveedor de servicio decide sobre las autorizaciones y proporciona el servicio al usuario.

Ejemplos de federaciones

- <http://www.rediris.es/sir/>
- <https://www.rnp.br/servicos/servicos-avancados/cafe>
- <http://cofre.reuna.cl/index.php/es/>
- <http://www.incommon.org/federation/>
- <http://services.geant.net/edugain/Pages/Home.aspx>

Antecedentes en México

- Creación en 2014 de un primer piloto de un Federación de Identidades Mexicana - **FldMex**.
- Afiliación de FldMex con una Federación Europea <https://gridp.garr.it>
- Impartición de dos Talleres de Capacitación, uno con la Universidad de Colima y con la Dirección Gral. De Tecnológicos en el D.F., y otro con algunos campus de la Universidad Autónoma Metropolitana.
- Creación en 2015 de la Federación Mexicana de Identidades **FENIX**, liderada por CUDI.

Propósito de Fenix

- Crear una Infraestructura Nacional de Autenticación y Autorización que permita la integración con **eduGAIN**.
- Fortalecer las comunidades en las instituciones, facilitándoles el acceso a recursos nacionales e internacionales en línea.
- Compartir los beneficios de las confederaciones con las instituciones miembros de CUDI.

Participantes y actividades

- Hasta ahora tenemos 9 instituciones miembros CUDI, sumadas al proyecto **FENIX**:
- BUAP, CICESE, CINVESTAV, IPN, ITESM, UAM, UCOL, UDG, UNAM.
- Las 9 instituciones han firmado una carta de intención para pertenecer a FENIX
- Asistencia al taller técnico sobre Federación de Identidades.

¿Hacia donde vamos?

- **Para 2016:**
 - Tener 5 a 8 servicios federados de las instituciones miembros CUDI.
 - Invitar a más instituciones para que participen en FENIX.
- **Para 2017**
 - Tener cuando menos un servicio federado por cada una de las instituciones afiliadas a FENIX.
 - Tener acuerdos de Interfederación en EDUGAIN
 - Invitar a más instituciones para que participen en FENIX.

¿Preguntas?

Fernando Aranda

faranda@cudi.edu.mx

PROYECTO Magic

Middleware for collaborative Applications and Global
virtual Communities

WP2 - AAI – Federación de Identidades