VNiVERSiDAD D SALAMANCA

adAS

advance Authentication Server

Single Sing-On de la Universidad de Salamanca

Inmaculada Bravo (inma@usal.es)

Agenda

VNiVERSiDAD D SALAMANCA

1. Qué es adAS
2. Características
3. Arquitectura
4. Autenticación-Autorización
5. Integración de aplicaciones
6. adAS en funcionamiento
7. Interfaz de administración
8. Resultados

1. Qué es adAS

adAS (advanced Authentication Server) es un Servidor de Autenticación Avanzado, basado en PAPI, que realiza funciones de Proveedor de Identidad, muy flexible, sencillo de administrar y sencillo de integrar aplicaciones

- El proyecto adAS se ha diseñado como herramienta de Single Sign-On para la **Universidad de Salamanca.**
- Desarrollada por la empresa española
- Software Libre: se encuentra a disposición de la comunidad para su utilización, desarrollo de mejoras y nuevos aportes.

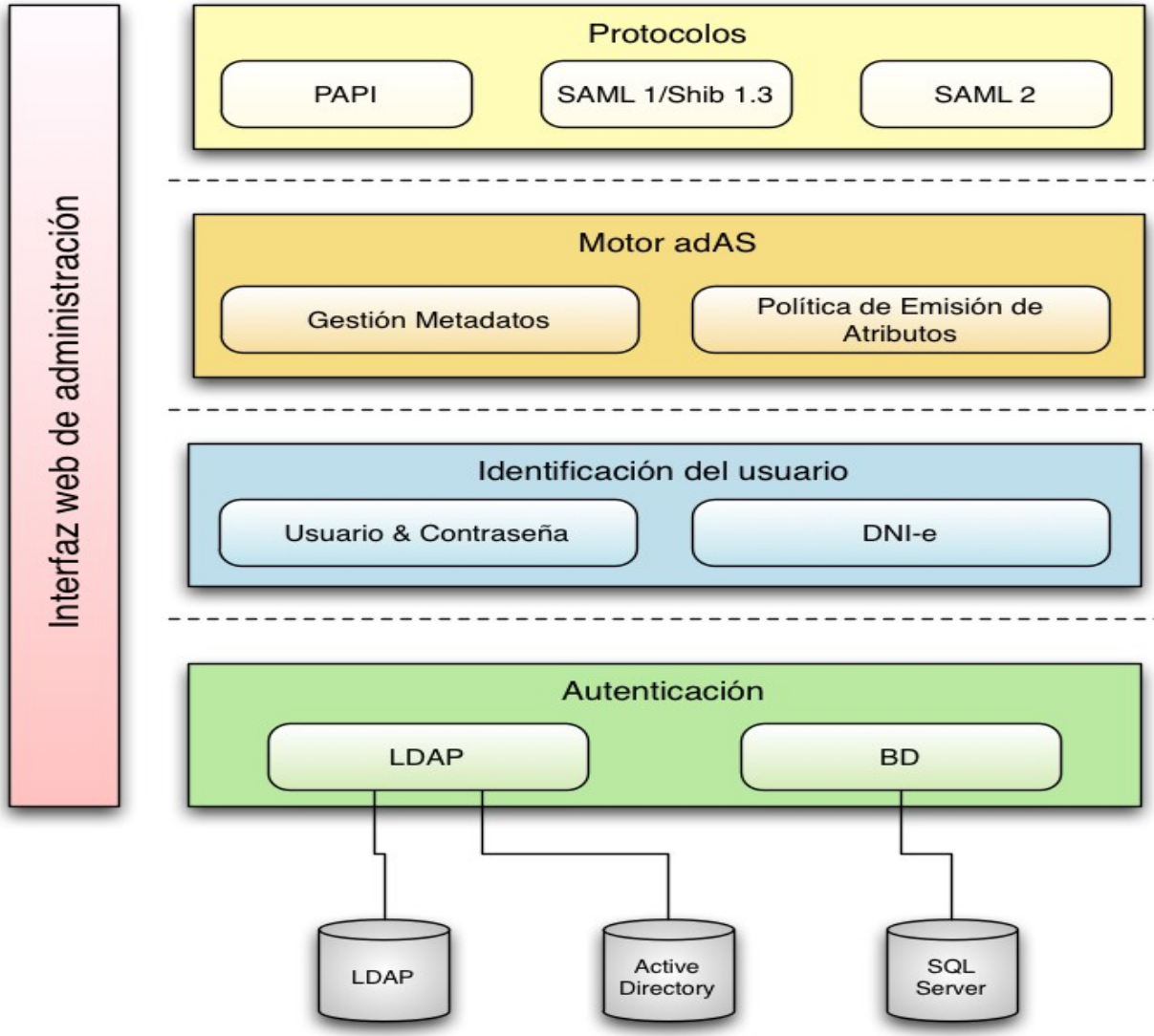
http://www.adas-sso.com

2. Características

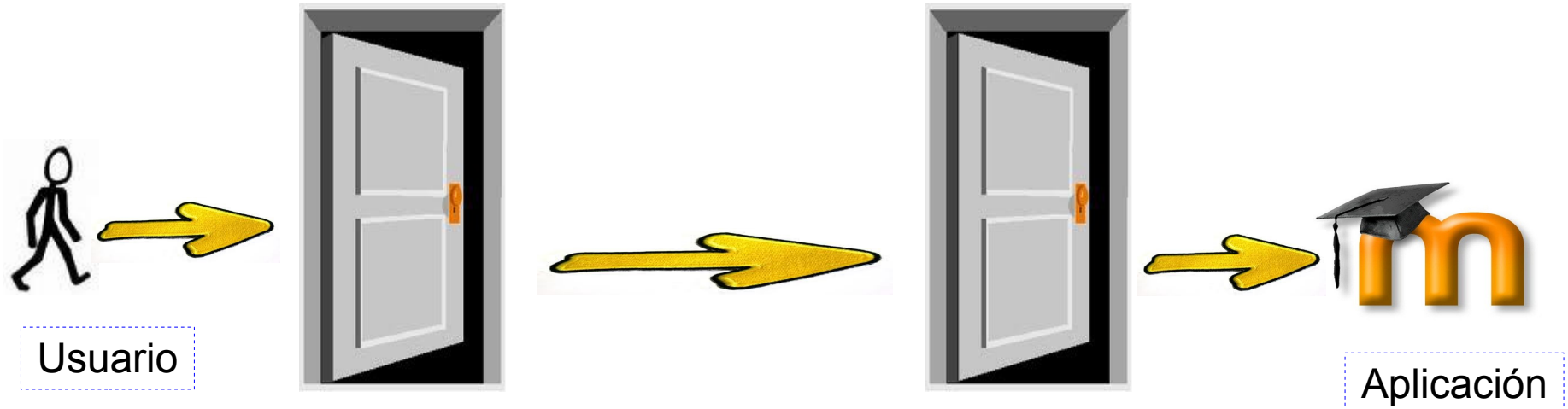
VNiVERSiDAD D SALAMANCA

1. **Multiprotocolo:** PAPI v1, SAML 1.1/Shibboleth 1.3 y SAML 2.0.
2. Gestión de los recursos a través de **metadatos**.
3. **Credenciales**: usuario/contraseña y/o DNI electrónico.
4. Diversas **fuentes de datos** para autenticar u obtener atributos.
5. **Administración** del sistema a través de una aplicación **web**.
6. Gestión avanzada de la **política de emisión de atributos**.
7. **Informes gráficos** sobre estadísticas de uso.
8. Fácil integración con sistemas de alta disponibilidad o balanceadores de carga.

3. Arquitectura



4. Autenticación-Autorización



Autenticación

Autorización

Inmaculada Bravo (inma@usal.es)

4. Autenticación-Autorización

VNiVERSiDAD D SALAMANCA

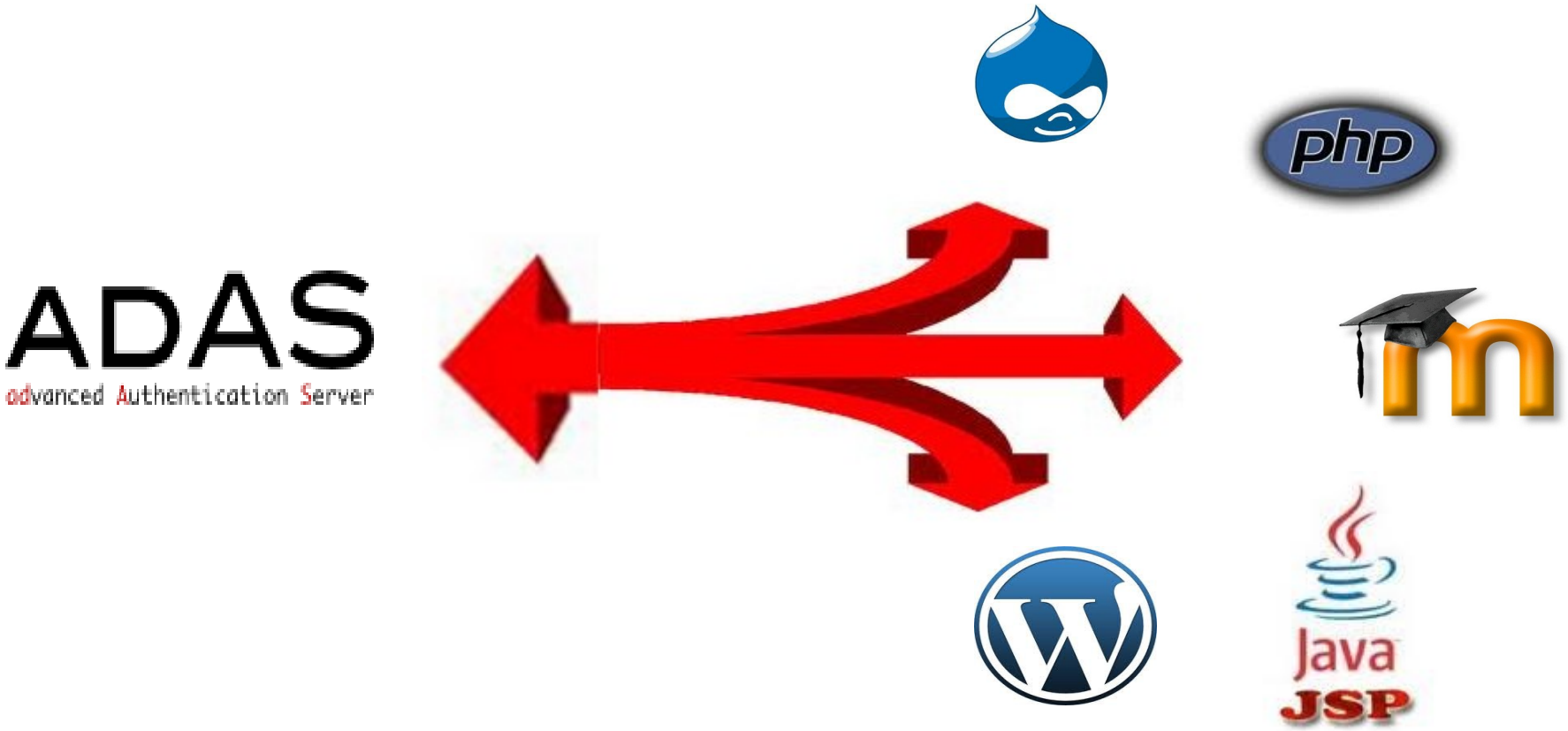
Autenticación:

- Método
  - usuario/contraseña
  - DNI-e
- Fuentes
  - LDAP
  - Bases de datos

Autorización:

- Cómo
  - Basada en atributos de usuario
  - Recolección de varias fuentes
  - Emisión especifica de attr. a cada SP
  - **Funciones callback**
- Dónde
  - En adAS
  - En el Punto de Acceso
  - En la propia aplicación

5. Integración de aplicaciones



Inmaculada Bravo (inma@usal.es)

5. Integración de aplicaciones

VNiVERSiDAD D SALAMANCA

Multitud de conectores para integrar cualquier aplicativo

Aplicación	Conector
Apps propias en php	phpPoA
Apps propias en jsp	papiFilter
Proteger directorios desde apache	papiPoA mod_papi
Apps estándar con módulos saml Drupal, Moodle, WordPress, DocNET, ect	simpleSAMLphp

Conectores en desarrollo:

- Conector para Oracle SSO (aplicaciones OCU)
- Conector .NET

5. Integración de aplicaciones

VNiVERSiDAD D SALAMANCA

Acciones en adAS:

- Incluir metadatos
- Definir política de atributos
  - Fuentes de datos
  - Atributos

Acciones en el SP:

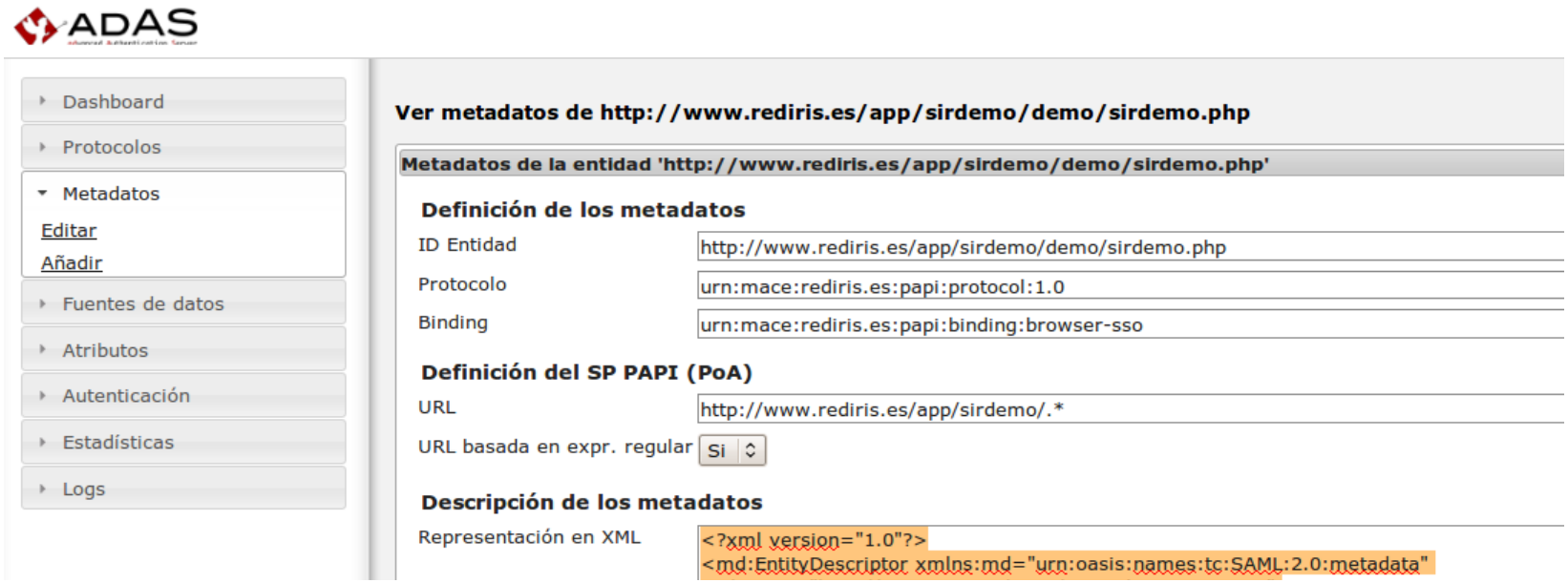
- Configurar el conector
- Incluir código para comprobar si el usuario está autenticado y para recuperar sus atributos.

Inmaculada Bravo (inma@usal.es)

5. Integración de aplicaciones

Incluir metadatos

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:papi="urn:mace:rediris.es:papi:metadata" entityID="http://www.rediris.es/app/sirdemo/demo/sirdemo.php">
      <md:RoleDescriptor xsi:type="papi:PoADescriptorType" protocolSupportEnumeration="urn:mace:rediris.es:papi:protocol:1.0">
         <papi:PoAService Binding="urn:mace:rediris.es:papi:binding:browser-sso" RegExpLocation="true"
Location="http://www.rediris.es/app/sirdemo/.*"/>
      </md:RoleDescriptor>
</md:EntityDescriptor>
```



5. Integración de aplicaciones

VNiVERSiDAD D SALAMANCA

Definir fuentes de datos

Editar fuentes de datos

Configuración fuente de datos

Definición

ID fuente	LDAP
Clase PHP	HookDB_LDAP

Opciones

ldap_server_uri	ldap://ldap.usal.es/
ldap_port	389
bind_dn	cn=adas-user,dc=usal,dc=es
bind_password	••••••••••••••••
attr_id_user	alias
scope	one
base_dn_search	dc=personas,dc=usal,dc=es

Inmaculada Bravo (inma@usal.es)

5. Integración de aplicaciones

VNiVERSiDAD D SALAMANCA

Especificar atributos

Inmaculada Bravo (inma@usal.es)

5. Integración de aplicaciones

VNiVERSiDAD D SALAMANCA

Funciones de callback

```
function desc_unidad($attributeValue) {
        $attrs = HookDB_Manager::hookDB('LDAP_unidades',
                                array_pop($attributeValue), 'usaldescripcion');
        return $attrs;
}


function rol($attributeValue) {
      //buscamos el rol
      $cat_princ = substr($attributeValue,1,1);
      switch ($cat_princ){
         case 1:
         case 2: $rolUser="staff"; break;
         case 5:
         case 3: $rolUser="student"; break;
         default: $rolUser="member"; break;
      }
     return $rolUser;
}
```


Inmaculada Bravo (inma@usal.es)

5. Integración de aplicaciones

VNiVERSiDAD D SALAMANCA

Acciones en el SP:

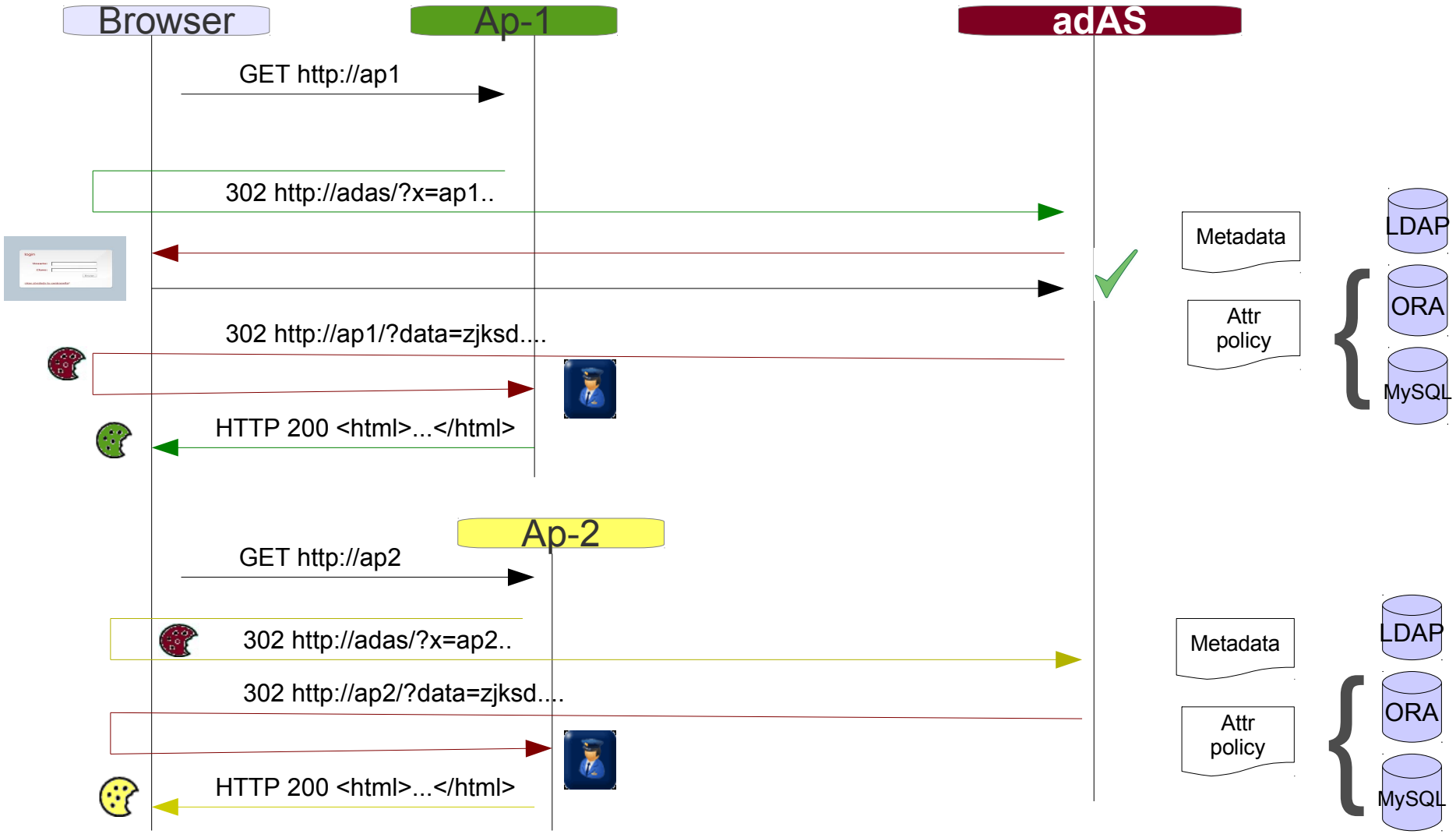
1. Copiar y configurar el conector phpPoA

```
GPoA_Pub_Key = /usr/local/papi/etc/KEYS/_GPoA_pubkey.pem
GPoA_URL = https://identidad.usal.es/adas/papiPoA
```

2. Incluir código para comprobar si el usuario está autenticado y para recuperar sus atributos.

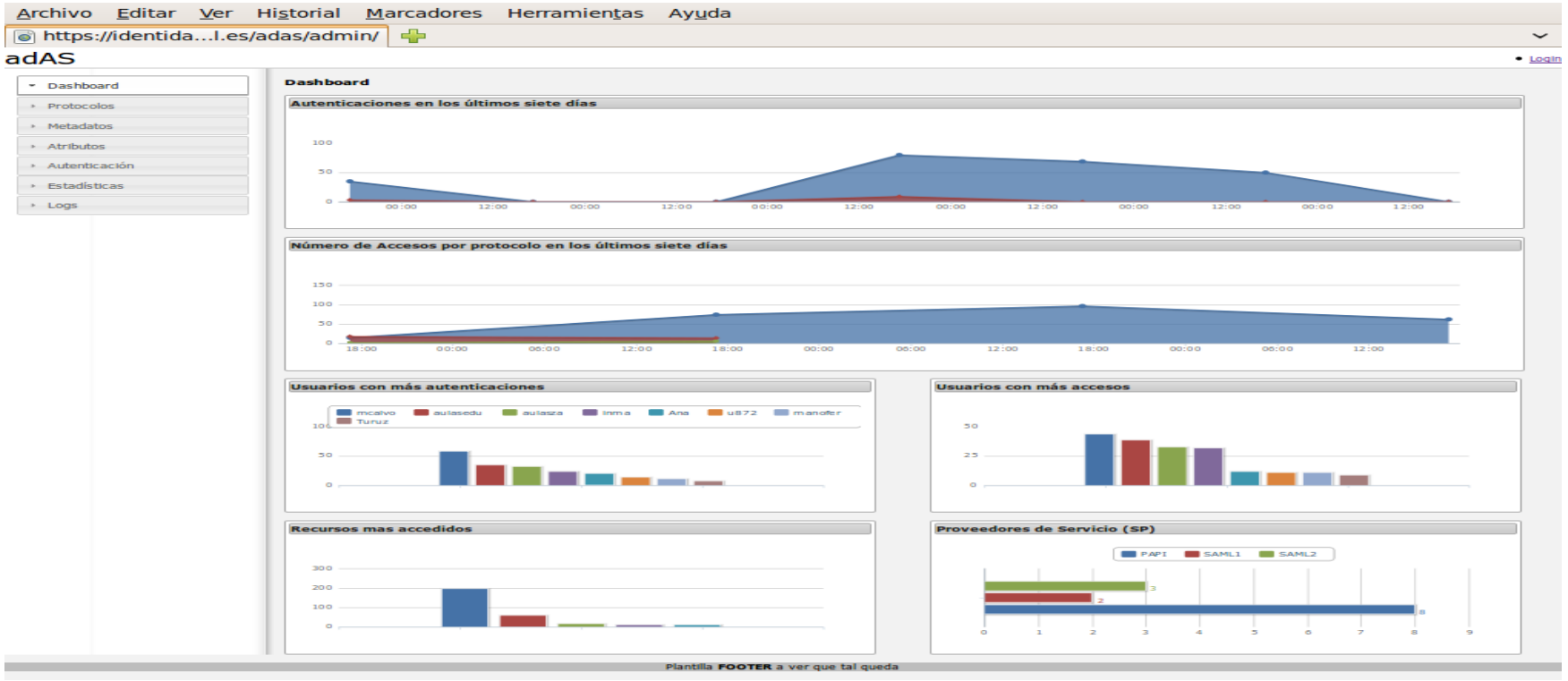
```
<?php
        include 'PoA.php';
        $poa = new autoPoA('admin');
        $userData = $poa->check_Access();

        foreach $userData as $key => $value) {
                echo "$key =$value <br />";
        }
?>
```

6. adAS en funcionamiento



Inmaculada Bravo (inma@usal.es)

7. Interfaz de administración



Demo

8. Resultados

- **Beneficios para los usuarios**
  Evitandoles logins

- **Beneficios para los desarrolladores**
  Acceso a varios repositorios, evitandoles https

- **Beneficios para la dirección**
  Utilización real de aplicativos -> planificación de recursos
  Un solo punto de acceso que auditar ->Facilitar el cumplimiento del Plan Nacional de Seguridad

- **Beneficios para los administradores del directorio**
  Herramienta potente y flexible y sobretodo fácil de administrar
  Evitar accesso al directorio por aplicaciones no controladas
  Trazabilidad de las acciones de los usuarios

VNiVERSiDAD D SALAMANCA

Muchas gracias por vuestra atención.

Inmaculada Bravo García
Servicios de Red
Universidad de Salamanca
inma@usal.es