



RedIRIS

Jornadas Técnicas y Grupos de trabajo de RedIRIS
v44 - 24/11/2017

Autenticación de aplicaciones nativas con AppAuth

SERGIO GÓMEZ BACHILLER
Operador del Servicio de Informática
Universidad de Córdoba

 @sgomez

 sgomez



¿Qué es AppAuth?

Client SDK for native Apps

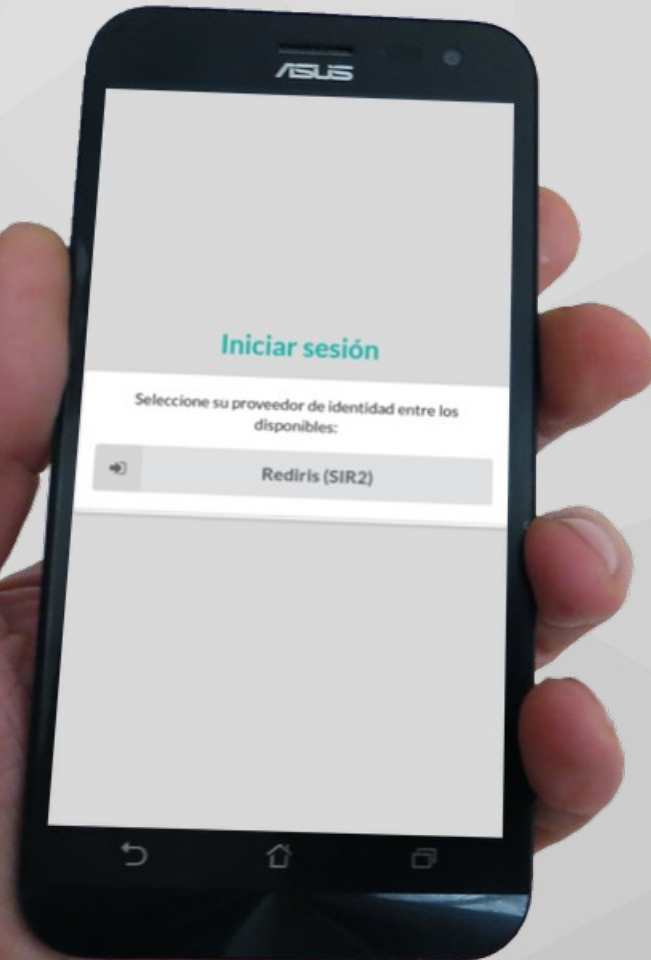


Características

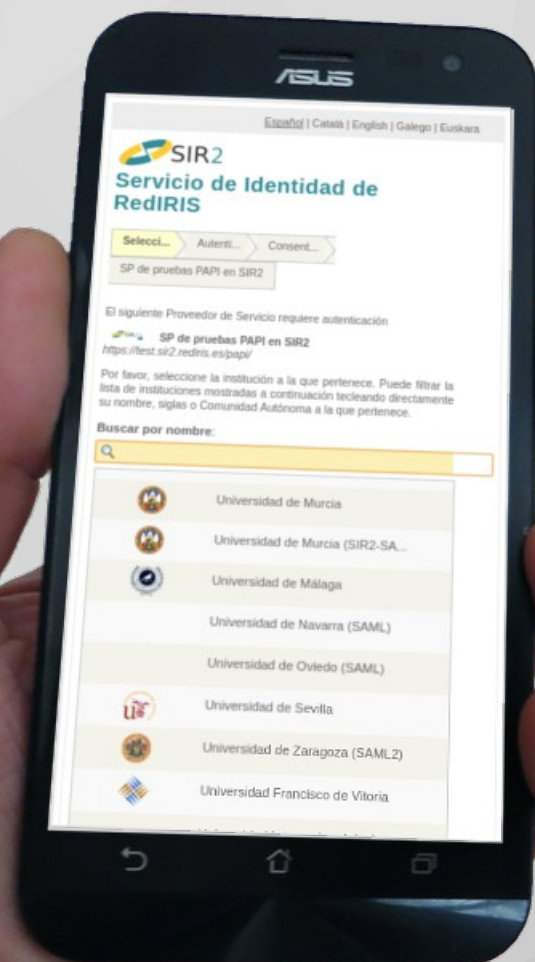
- **RFC 8252: OAuth2 for Native Apps**
- **RFC 7636: Proof Key for Code Exchange (PKCE)**
- **OAuth2**
- **OpenID Connect**



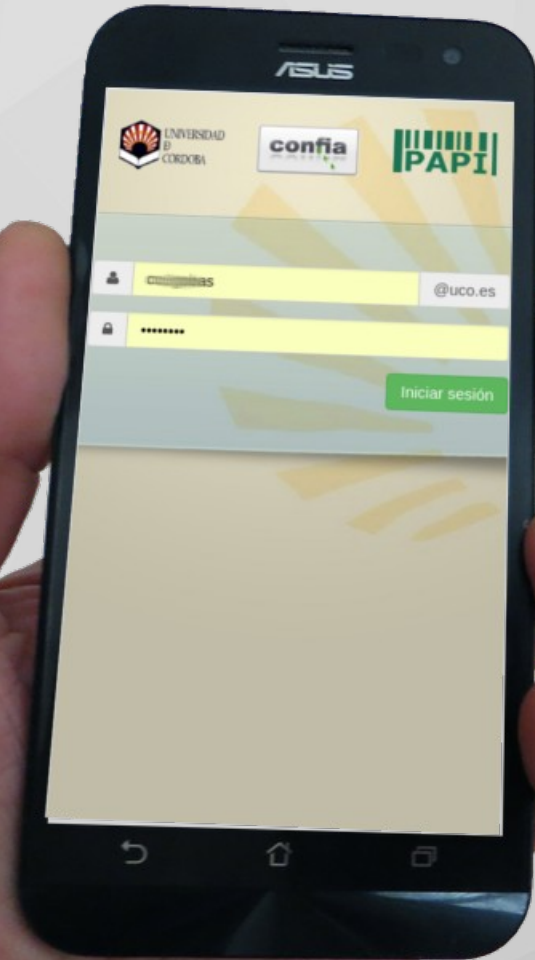
Objetivo



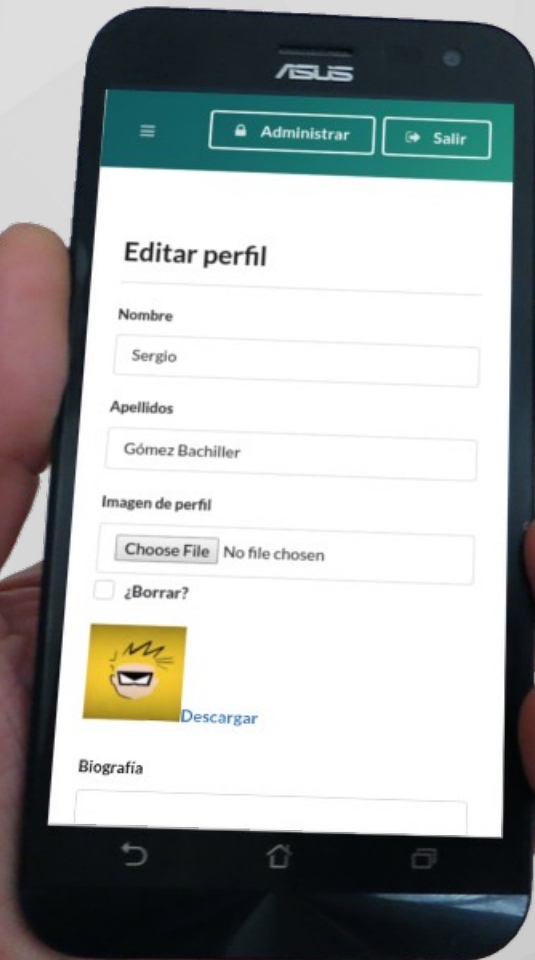
Objetivo



Objetivo



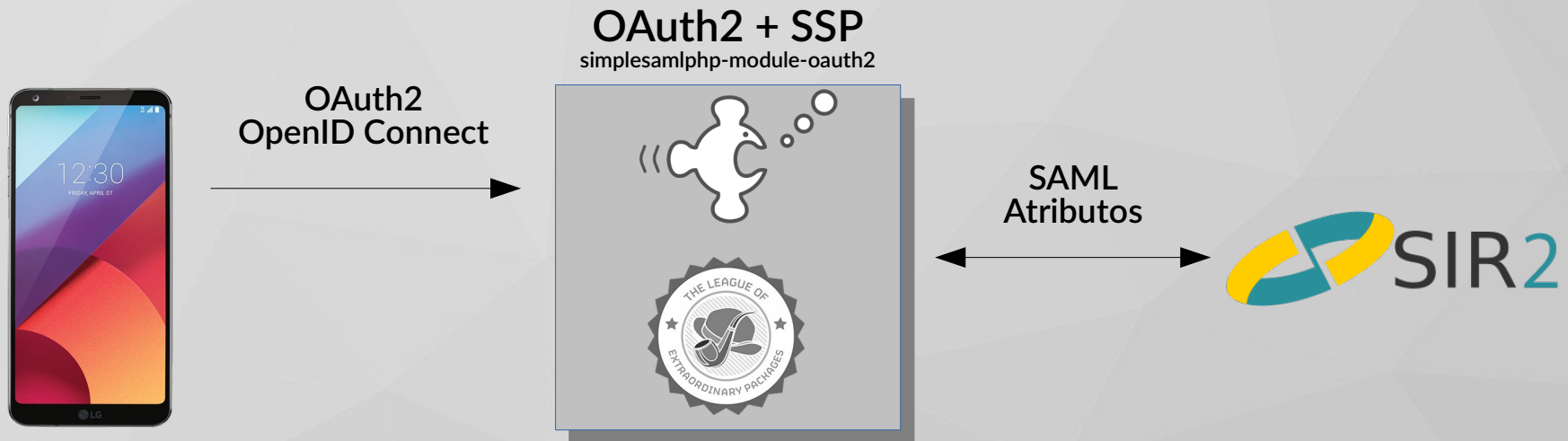
Objetivo



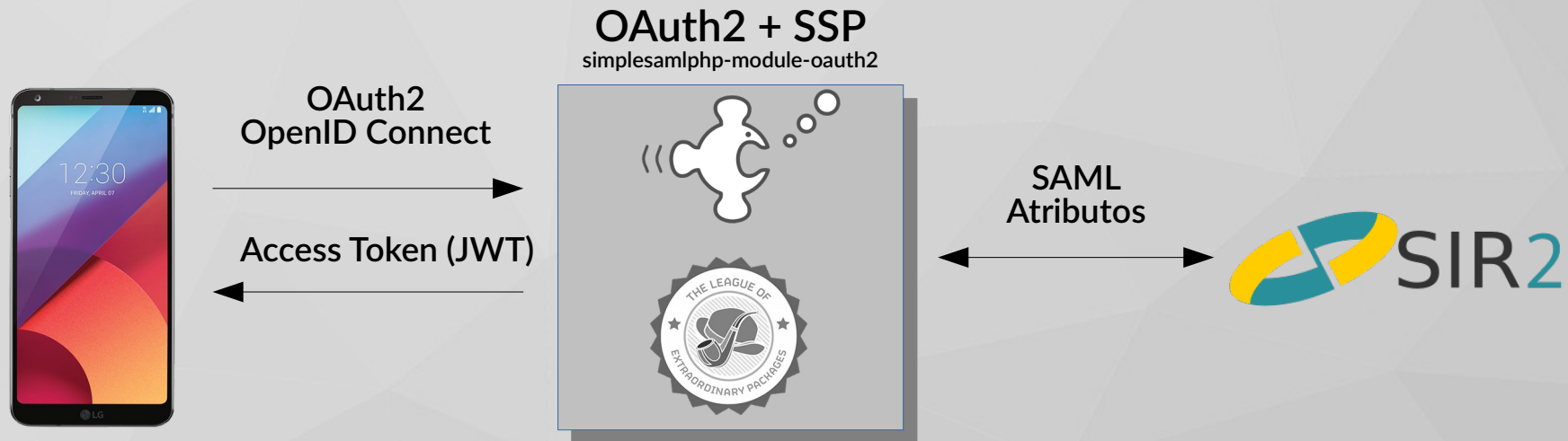
Esquema de funcionamiento



Esquema de funcionamiento



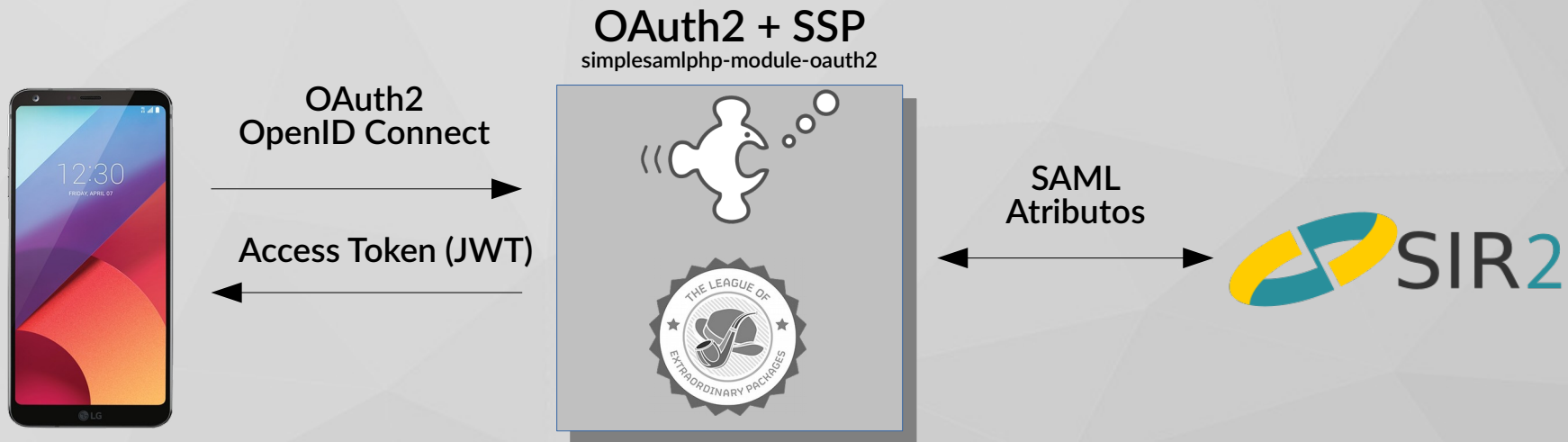
Esquema de funcionamiento



```
EyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiaXNpdCI6ImFkbGciLCJ1aWkiOiJhbnR5dWV9.TJVA95OrM7E2cBab30RMHrHDcEfxjYoYZgeFONFh7HgQ
```

```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}
```

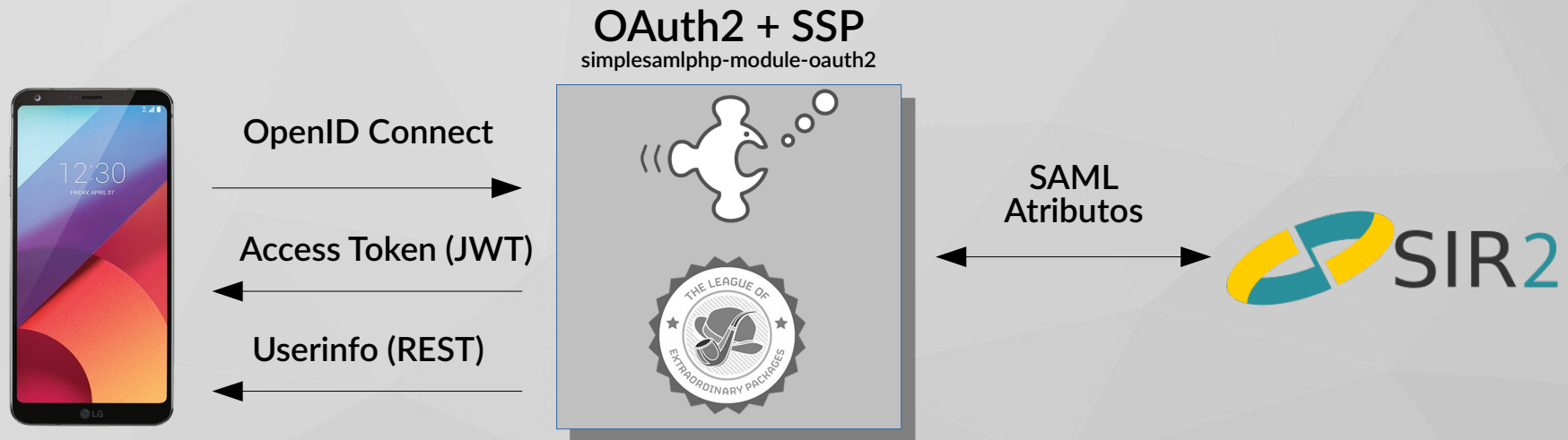
Esquema de funcionamiento



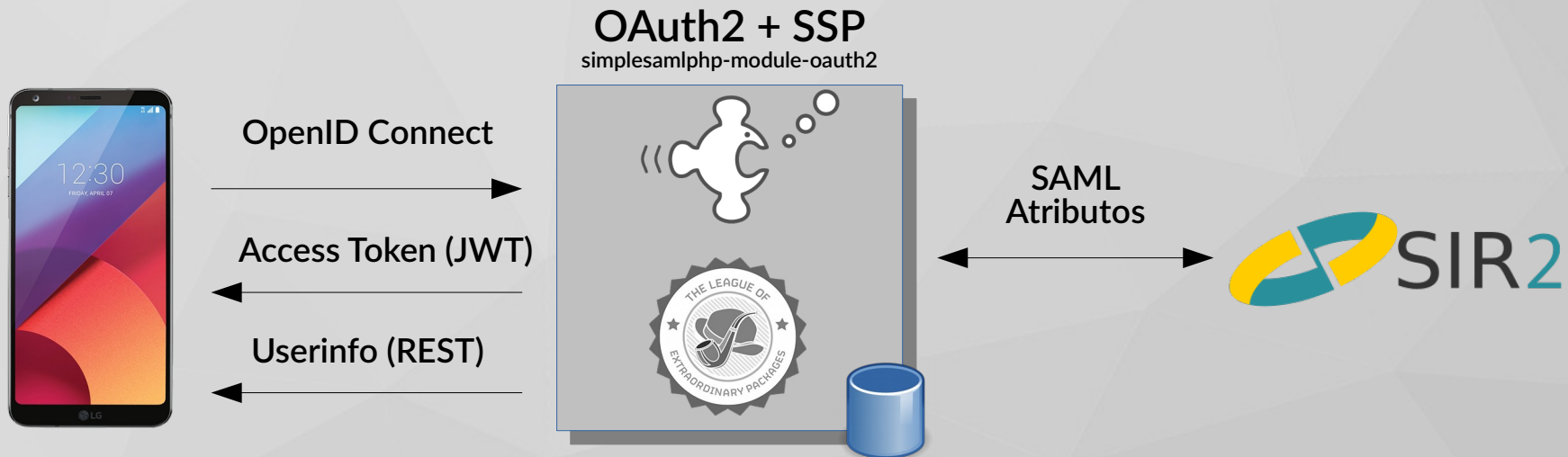
```
EyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiaXNja30gobas@uco.es", "iat": 1511927043, "exp": 1547927043
```

```
{ "sub": "cc0gobas@uco.es", "iat": 1511927043, "exp": 1547927043 }
```


Esquema de funcionamiento



Esquema de funcionamiento



```
{  
  "sub": "b822df...469490a12@uco.es",  
  "name": "John Doe",  
  "email": "j.doe@uco.es",  
  "picture": "https://img.uco.es/..."  
}
```

Configuración AppAuth

Fichero auth_config.json

```
{  
  "client_id": "c12831defa123418922023432bc0709abea0a7afd8cd312",  
  "redirect_uri": "https://appauth.demo-app.io/oauth2redirect",  
  "authorization_scope": "basic",  
  "discovery_uri": "https://.../openid-configuration.php",  
  "authorization_endpoint_uri": "",  
  "token_endpoint_uri": "",  
  "registration_endpoint_uri": "",  
  "https_required": true  
}
```

El campo *redirect_uri* debe configurarse también en el archivo AndroidManifest.xml



Configuración OpenID Connect

Esquema de discoveri_uri

```
{
  "issuer": "https://identidaddev.uco.es/",
  "authorization_endpoint": "https://.../oauth2/authorize.php",
  "token_endpoint": "https://.../oauth2/access_token.php",
  "userinfo_endpoint": "https://.../oauth2/userinfo.php",
  "jwks_uri": "https://.../jwks.php",
  "scopes_supported": [
    "basic"
  ],
  "response_types_supported": [
    "code",
    "token"
  ],
  "subject_types_supported": [
    "basic"
  ],
  "id_token_signing_alg_values_supported": [
    "RS256"
  ]
}
```



Configuración AppAuth


Esquema de jwks_uri

```
{
  "keys": [
    {
      "kty": "RSA",
      "n": "zj1MKYL8y-sS4jfeocZCvQZ2j9SU0LvzWbJAQiGEHo5
jjFKFSq9dTqPyp_UoX-jQt9doeaU3-eIV51qUXu80zK
cnUYZcB6if60fUN15H9ehRvEdjo0vuv3WQ4py_mKj7o
G_Jr_zXcBoih_PrsgPb0BAg4Q5_wKixF7_ifEwVcB8",
      "e": "AQAB",
      "use": "sig",
      "alg": "RS256"
    }
  ]
}
```



Seguridad (RFC8252)

External User-Agent
Custom Tab (Indicador SSL)



OpenID AppAuth Demo


START AUTHORIZATION

Authorization options:

Account ID (e.g. test@example.com)

The Account ID is optional. If specified, it is transmitted as a login_hint parameter in the authorization request.

Use browser:

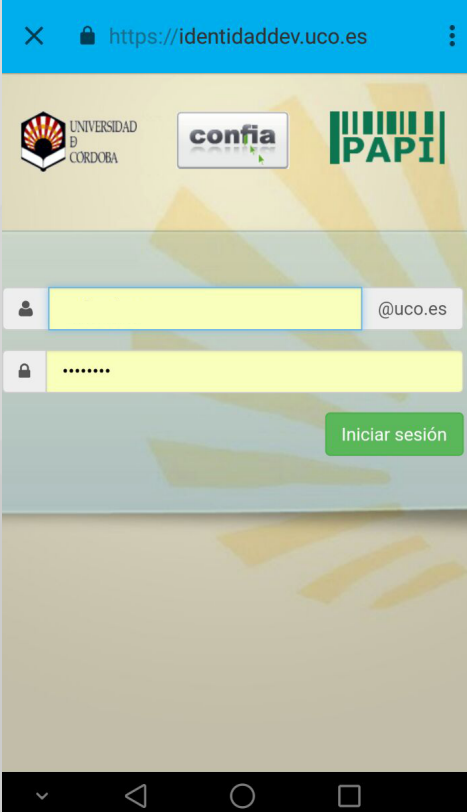
 AppAuth heuristic selection

Use PendingIntent's for completion

Authorization settings in use:

Discovered auth endpoint:
https://identidaddev.uco.es/simplesaml/module.php/oauth2/authorize.php

Static client ID:
e34122080be070945e48d428de62abca9a7afd86f

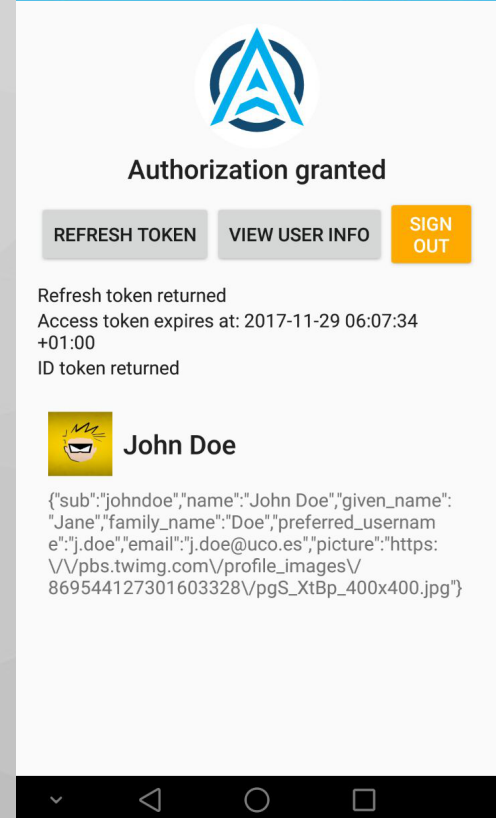


Browser address bar: https://identidaddev.uco.es

Logos: UNIVERSIDAD DE CORDOBA, confia, PAPI

Form fields: @uco.es, Password


Iniciar sesión



Authorization granted

REFRESH TOKEN **VIEW USER INFO** **SIGN OUT**

Refresh token returned
Access token expires at: 2017-11-29 06:07:34 +01:00
ID token returned

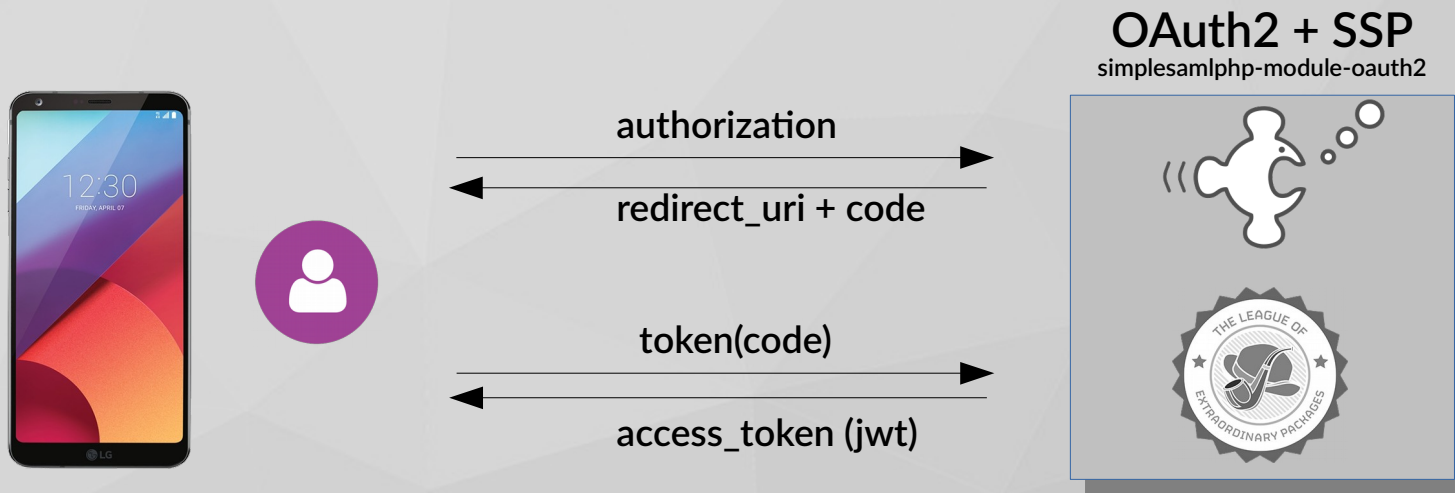


John Doe

```
{"sub":"johndoe","name":"John Doe","given_name":"Jane","family_name":"Doe","preferred_username":"j.doe","email":"j.doe@uco.es","picture":"https://pbs.twimg.com/profile_images/869544127301603328/pgS_XtBp_400x400.jpg"}
```

Seguridad (PKCE)

OAuth2/OpenID Connect sin PKCE



Configuración AppAuth

Fichero auth_config.json

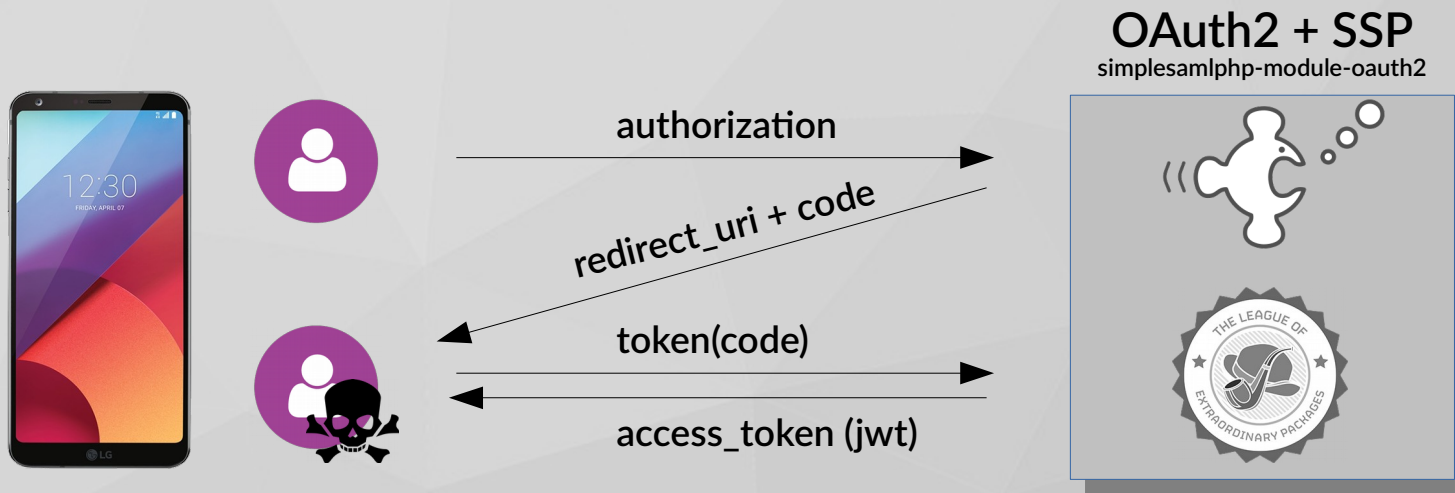
```
{  
  "client_id": "c12831defa123418922023432bc0709abea0a7afd8cd312",  
  "redirect_uri": "https://appauth.demo-app.io/oauth2redirect",  
  "authorization_scope": "basic",  
  "discovery_uri": "https://.../openid-configuration.php",  
  "authorization_endpoint_uri": "",  
  "token_endpoint_uri": "",  
  "registration_endpoint_uri": "",  
  "https_required": true  
}
```

El campo *redirect_uri* debe configurarse también en el archivo AndroidManifest.xml



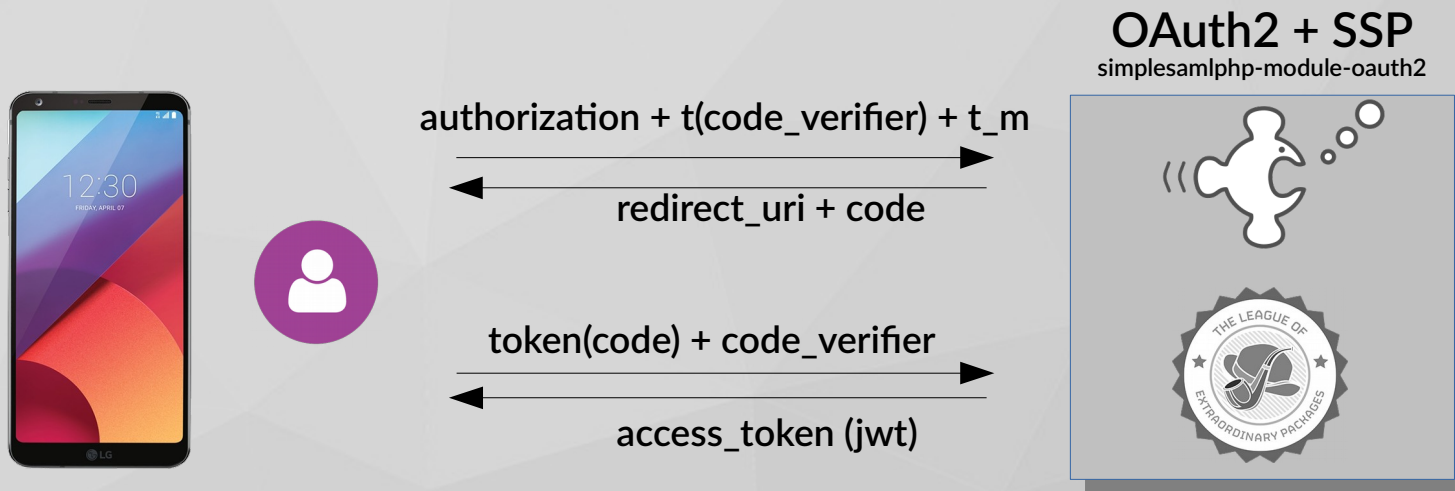
Seguridad (PKCE)

OAuth2/OpenID Connect sin PKCE



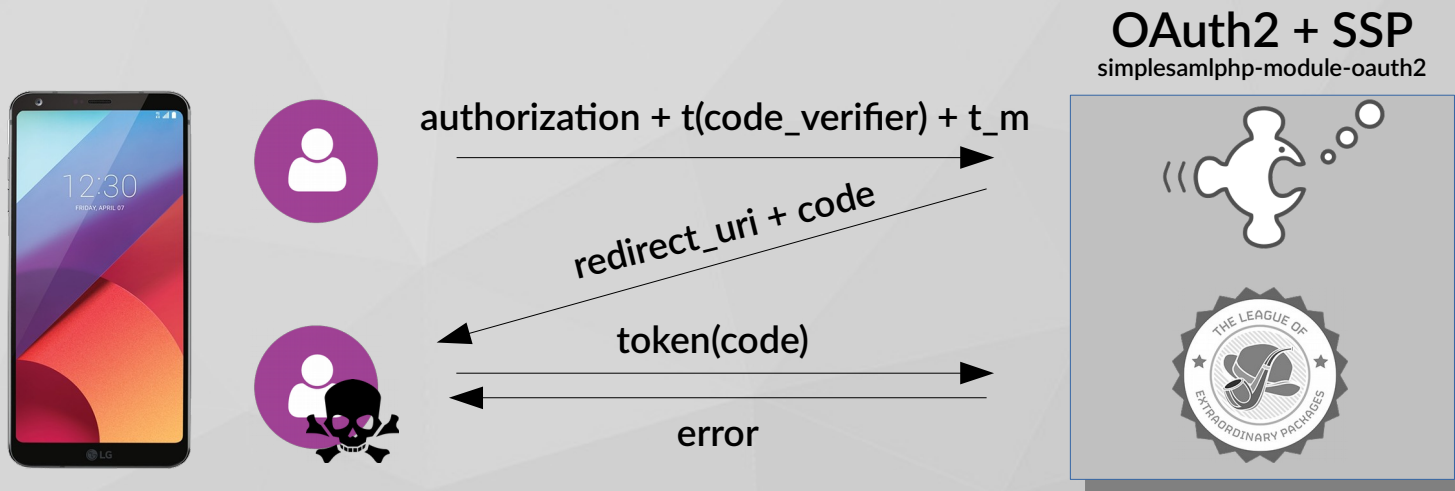
Seguridad (PKCE)

OAuth2/OpenID Connect con PKCE



Seguridad (PKCE)

OAuth2/OpenID Connect con PKCE



Seguridad (PKCE)

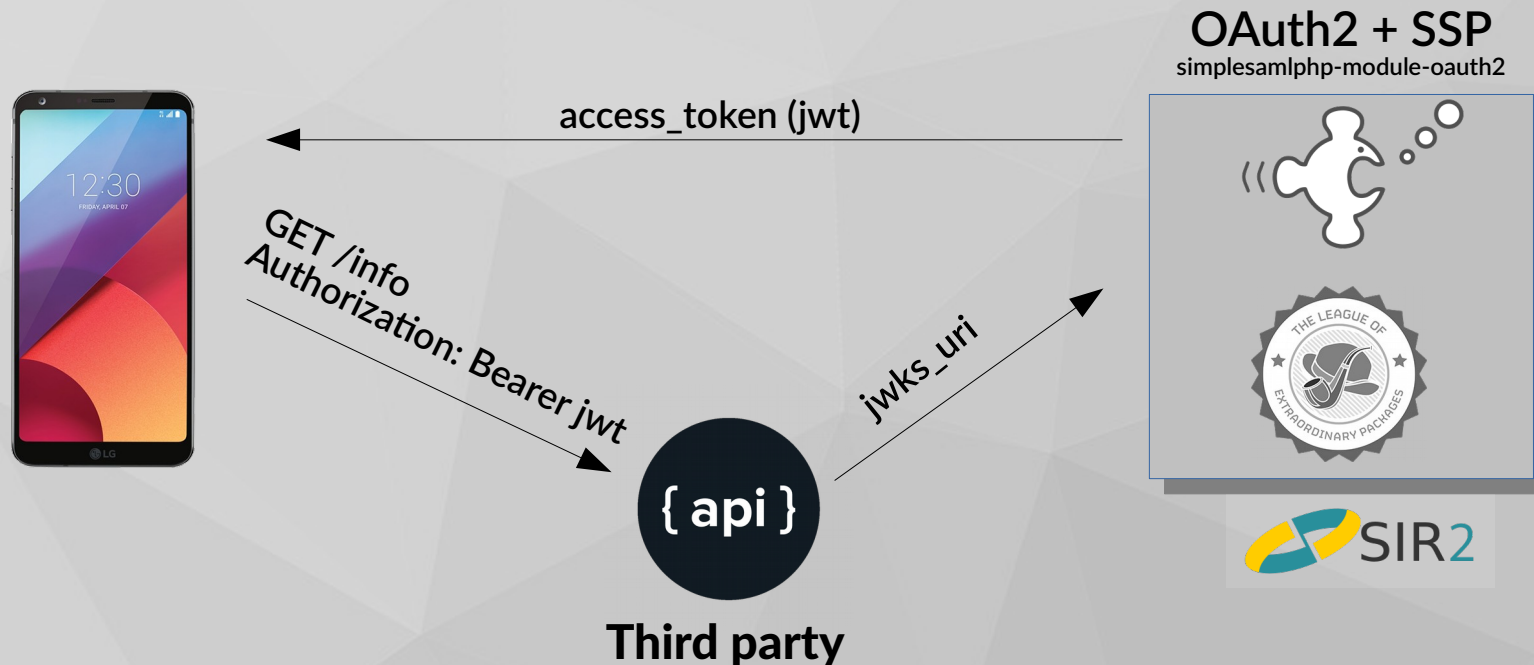
Token JWT

- **Estándar (RFC7519)**
- **Válido para autenticación y para intercambio de información**
- **Firmado por el IDP**



Posibles usos

- Autenticación de usuarios de RedIRIS
- Acceso a APIs de terceros (confianza en la firma del token JWT)



Demo Time



Estado del proyecto

- Terminar de implementar OpenID Connect
- Definir scopes y traducción de atributos
- Pantalla de solicitud de permiso al usuario
- Despliegue de la pasarela en RedIRIS

Módulo de SimpleSAMLphp-OAuth2:

<https://github.com/sgomez/simplesamlphp-module-oauth2>





Autenticación de aplicaciones nativas con AppAuth

SERGIO GÓMEZ BACHILLER
Operador del Servicio de Informática
Universidad de Córdoba

 @sgomez

 sgomez