



RedIRIS

Jornadas Técnicas de RedIRIS - Salamanca
10/05/2018

Autenticación con OpenID Connect a través de SimpleSAMLphp

SERGIO GÓMEZ BACHILLER

**Operador del Servicio de Informática
Universidad de Córdoba**

 @sgomez

 sgomez



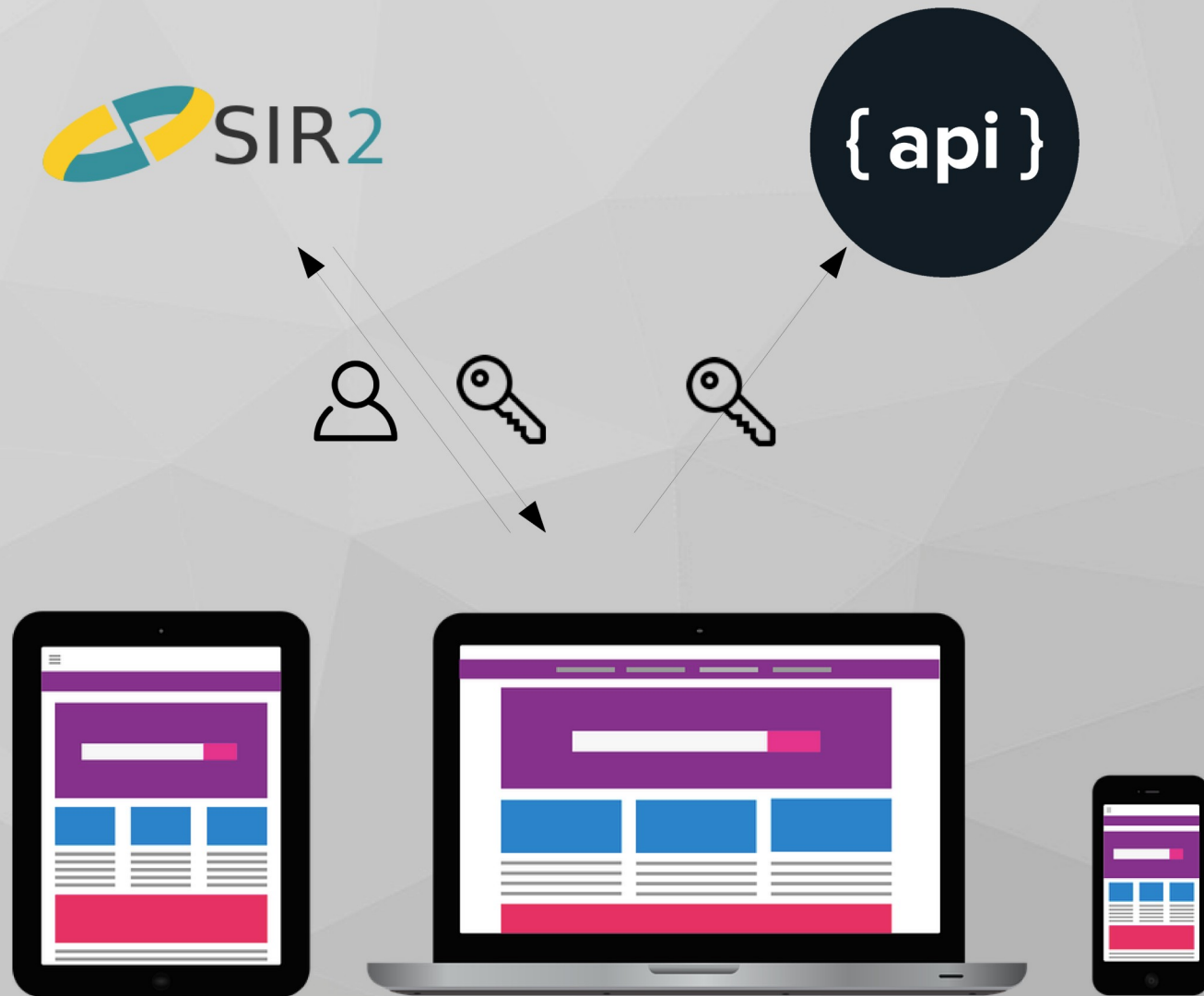
El problema



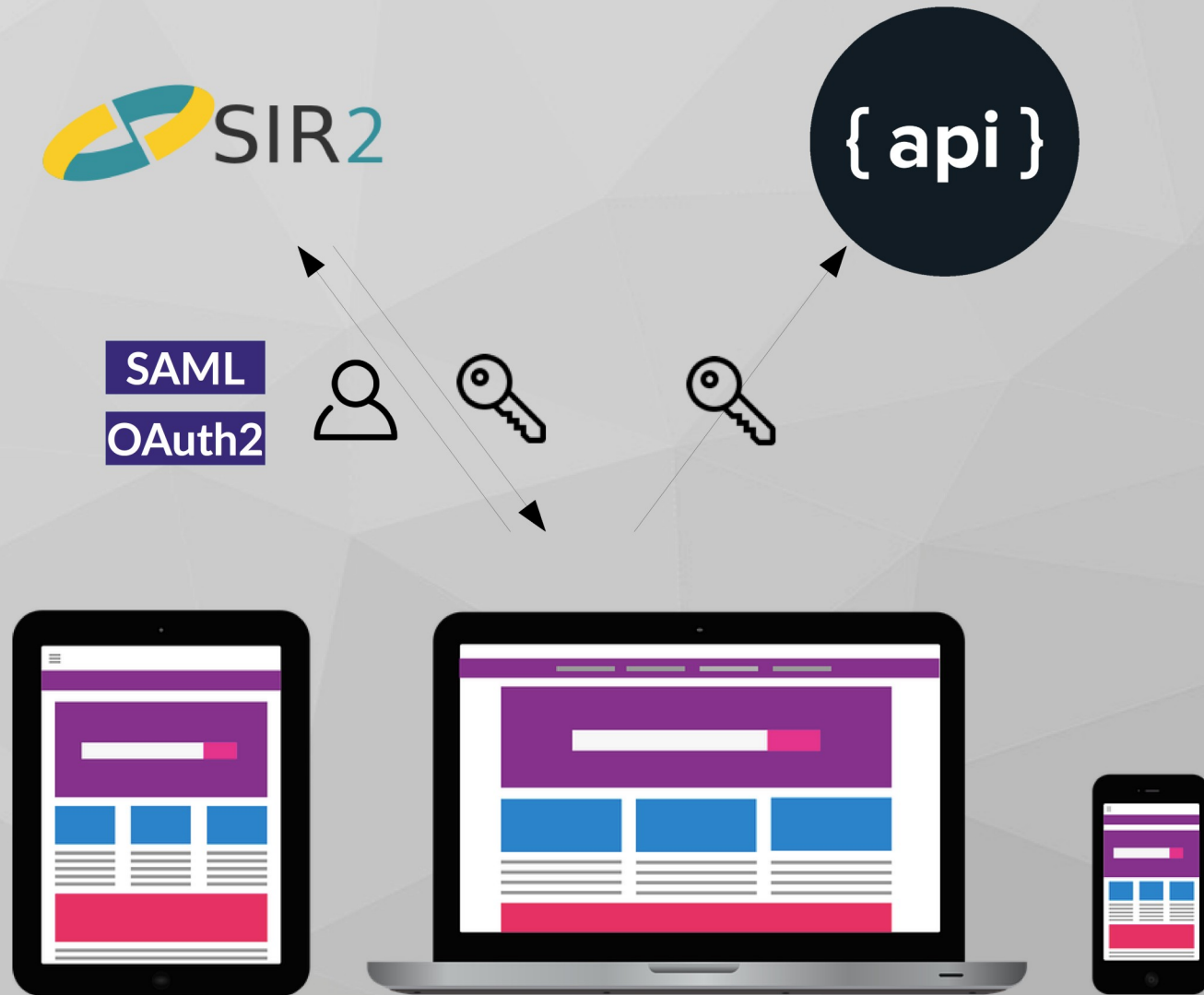
El problema



El problema



El problema



Limitaciones OAuth2

- OAuth2 es un framework de autorización delegada, no de autenticación.
- Falta de definición de (entre otras):
 - Scopes
 - Descubrimiento de puntos de acceso



Limitaciones OAuth2

Scopes (id usuario, email)



<https://www.googleapis.com/auth/userinfo.email>
<https://www.googleapis.com/auth/userinfo.profile>



id, email, first_name, last_name, ...



user (read:user, user:email)

Limitaciones OAuth2

Authorization endpoint



<https://accounts.google.com/o/oauth2/auth>



<https://www.facebook.com/v3.0/dialog/oauth>



<https://github.com/login/oauth/authorize>



Limitaciones OAuth2

Token endpoint



<https://accounts.google.com/o/oauth2/token>



https://graph.facebook.com/v3.0/oauth/access_token



https://github.com/login/oauth/access_token



¿Qué es OpenID Connect?

- Capa encima de OAuth2
- Proporciona:
 - Autenticación (id_token)
 - Scopes (openid, profile, email, address, phone)
 - Autodescubrimiento de end-points
 - ...



Configuración OpenID Connect

Scopes y claims en OIDC:

Scope	Claims
openid	
profile	name, family_name, given_name, middle_name, nickname, preferred_username, profile, picture, website, gender, birthdate, zoneinfo, locale, updated_at.
email	email, email_verified
address	address
phone	phone_number, phone_number_verified



Configuración OpenID Connect

Esquema de discovery_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 OpenID Connect

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"
    }
  ]
}
```



Módulo simpleSAMLphp OIDC

Características

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



Esquema de funcionamiento



Esquema de funcionamiento



Esquema de funcionamiento



```
EyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IjEyMzQ1NiIsInp1diI6IjE2MzQ1NiJ9.TJVA95OrM7E2cBab30RMHrHDcEfxj  
oYZgeFONFh7HgQ
```

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

Esquema de funcionamiento



```
EyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiaXNpdCI6ImFkbG9uIiwiaWF0IjoiMTUxOTI3MDQzLjE1In0.YZgeFONFh7HgQ
```

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



Esquema de funcionamiento



```
EyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiaWF0IjoiYXNjaWkiLCJ1aWQiOiJ1aWQiLCJ0eXBlIjoiYXV0bnVzZXIuTjVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7HgQ
```

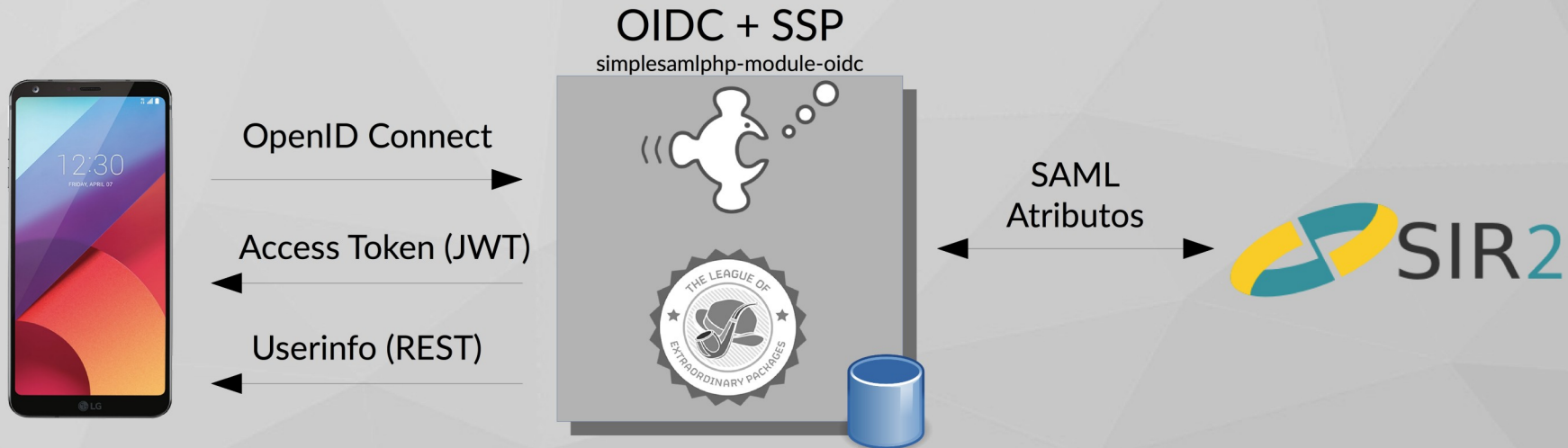
FIRMA



Esquema de funcionamiento



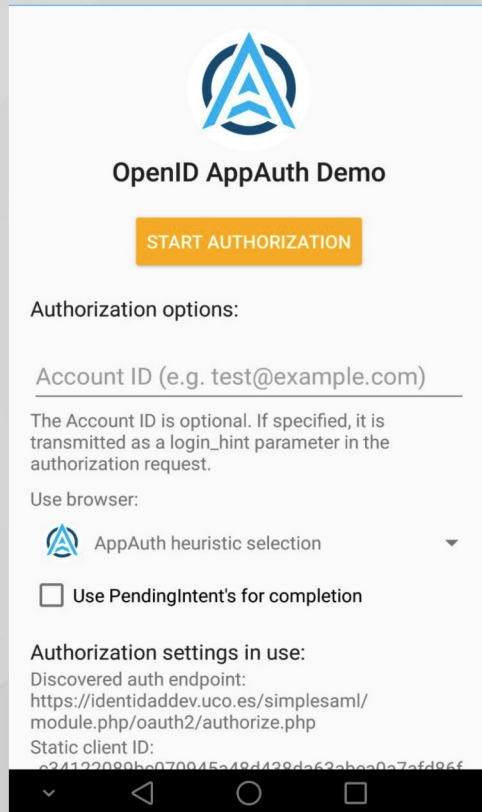
Esquema de funcionamiento



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

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:

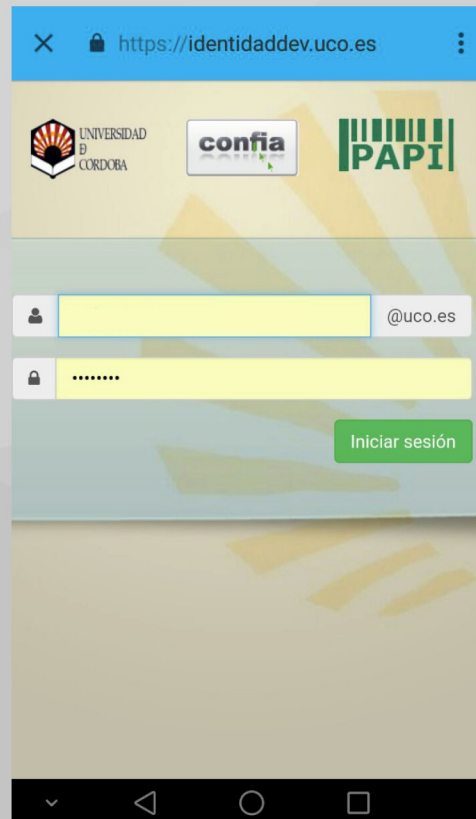
AppAuth heuristic selection

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:
e34122080be070045e48d428df62abce0a7afd86f



https://identidaddev.uco.es

UNIVERSIDAD DE CORDOBA

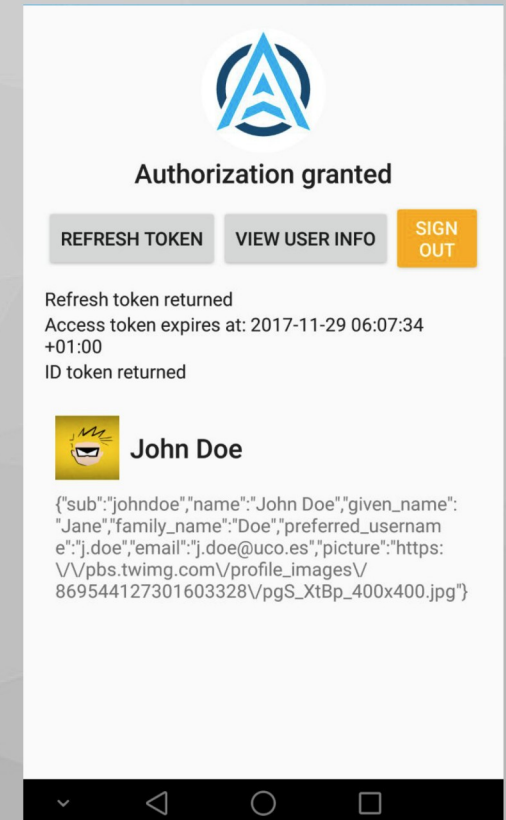
confia

PAPI

@uco.es

.....


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": "John", "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)

OpenID Connect sin PKCE



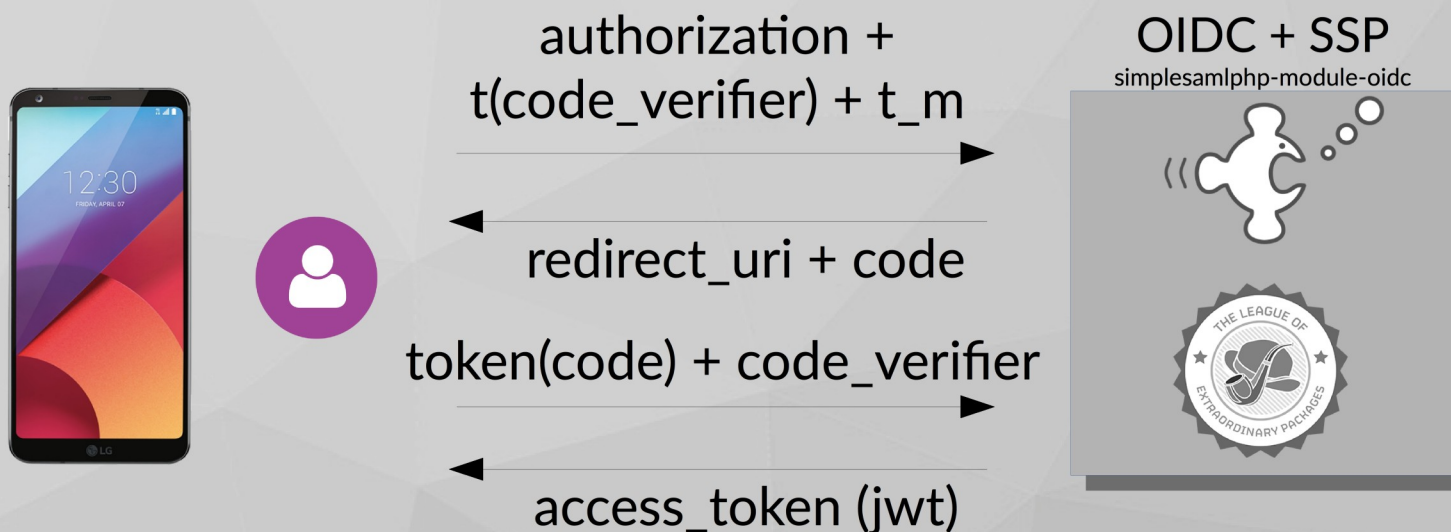
Seguridad (PKCE)

OpenID Connect sin PKCE



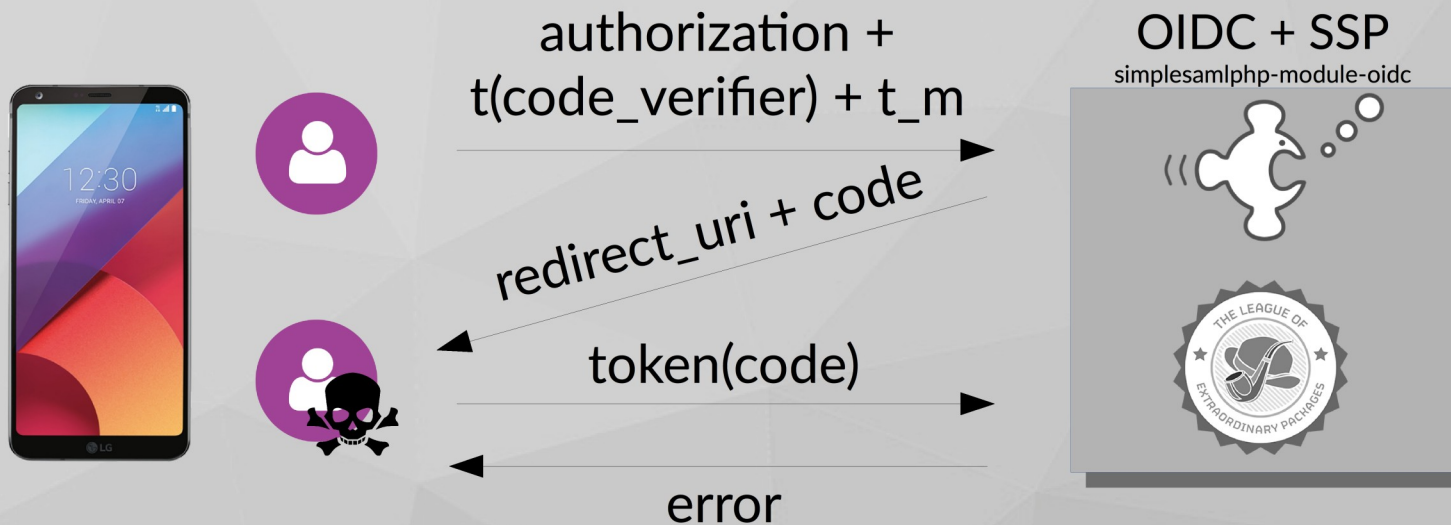
Seguridad (PKCE)

OpenID Connect con PKCE



Seguridad (PKCE)

OpenID Connect con PKCE



Demo Time



Retos

- Traducir atributos SAML ↔ OIDC
- Proporcionar el SDK basado en AppAuth
- Terminar de implementar funcionalidades no esenciales

Módulo de SimpleSAMLphp OpenID Connect:

<https://github.com/rediris-es/simplesamlphp-module-oidc>





Autenticación con OpenID Connect a través de SimpleSAMLphp

SERGIO GÓMEZ BACHILLER
Operador del Servicio de Informática
Universidad de Córdoba



@sgomez



sgomez

