An AppAuth (RFC 8252) Gateway For The Spanish SIR2 Federation

José-Manuel Macías
https://keybase.io/macias

GOBIERNO DE ESPAÑA
MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

About AppAuth

Internet Engineering Task Force (IETF) — W. Denniss, Google
Request for Comments: 8252 — J. Bradley, Ping Identity
BCP: 212
Updates: 6749
Category: Best Current Practice — October 2017
ISSN: 2070-1721

RFC 8252

OAuth 2.0 for Native Apps

Abstract

OAuth 2.0 authorization requests from native apps should only be made through external user-agents, primarily the user's browser. This specification details the security and usability reasons why this is the case and how native apps and authorization servers can implement this best practice.

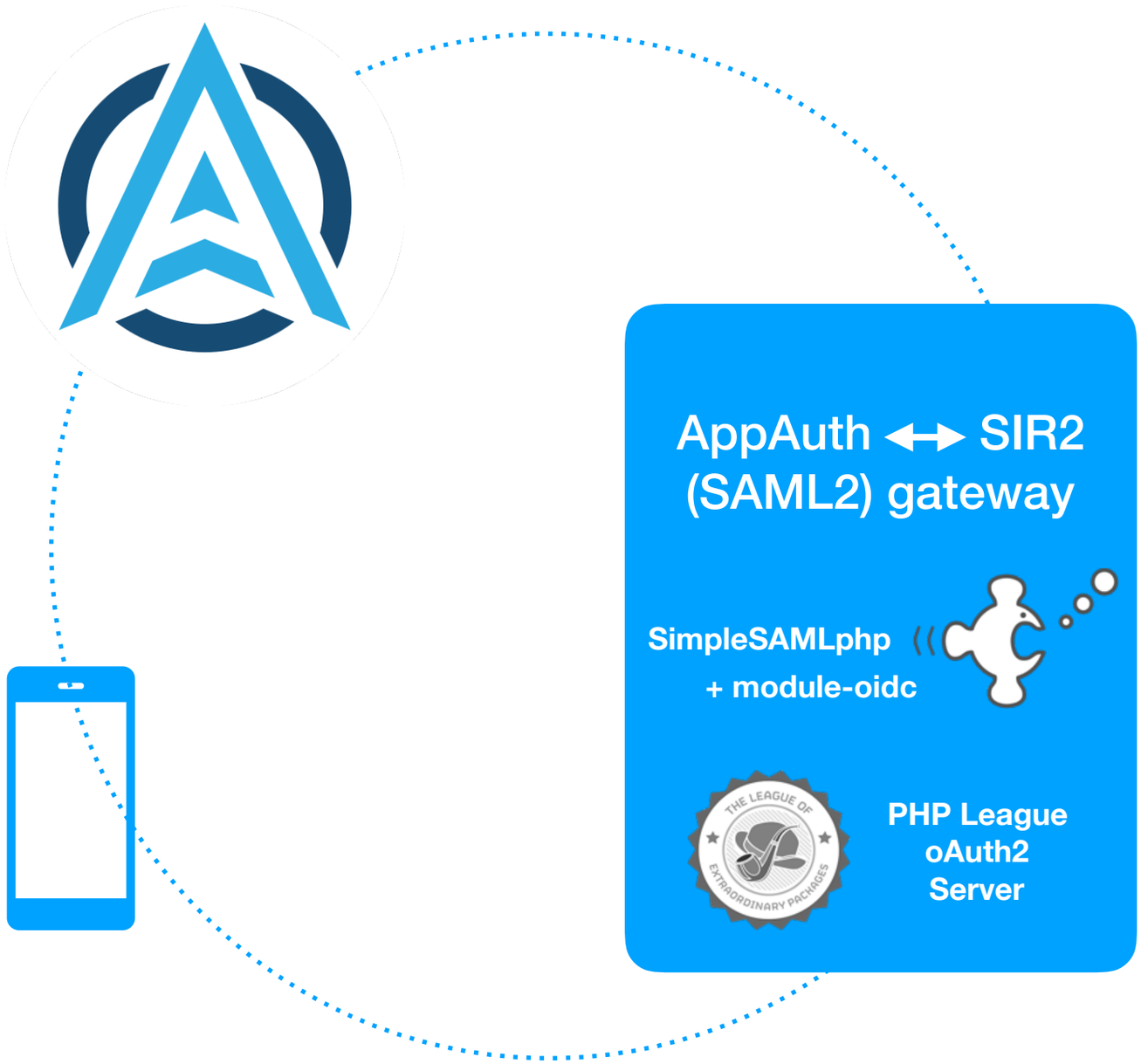
RFC 7636

Proof Key for Code Exchange by OAuth Public Clients

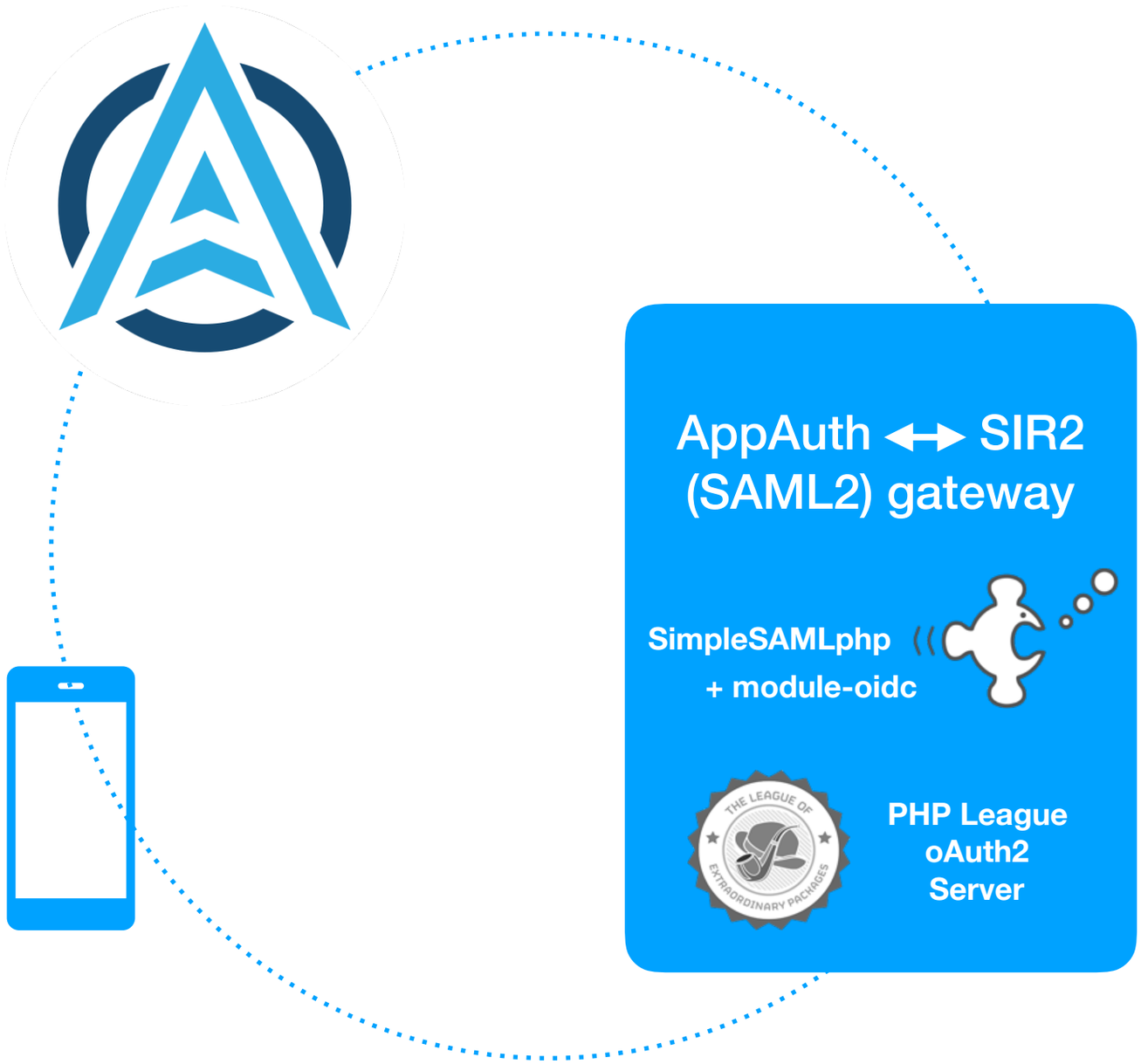
Abstract

OAuth 2.0 public clients utilizing the Authorization Code Grant are susceptible to the authorization code interception attack. This specification describes the attack as well as a technique to mitigate against the threat through the use of Proof Key for Code Exchange (PKCE, pronounced "pixy").

Authentication Flow



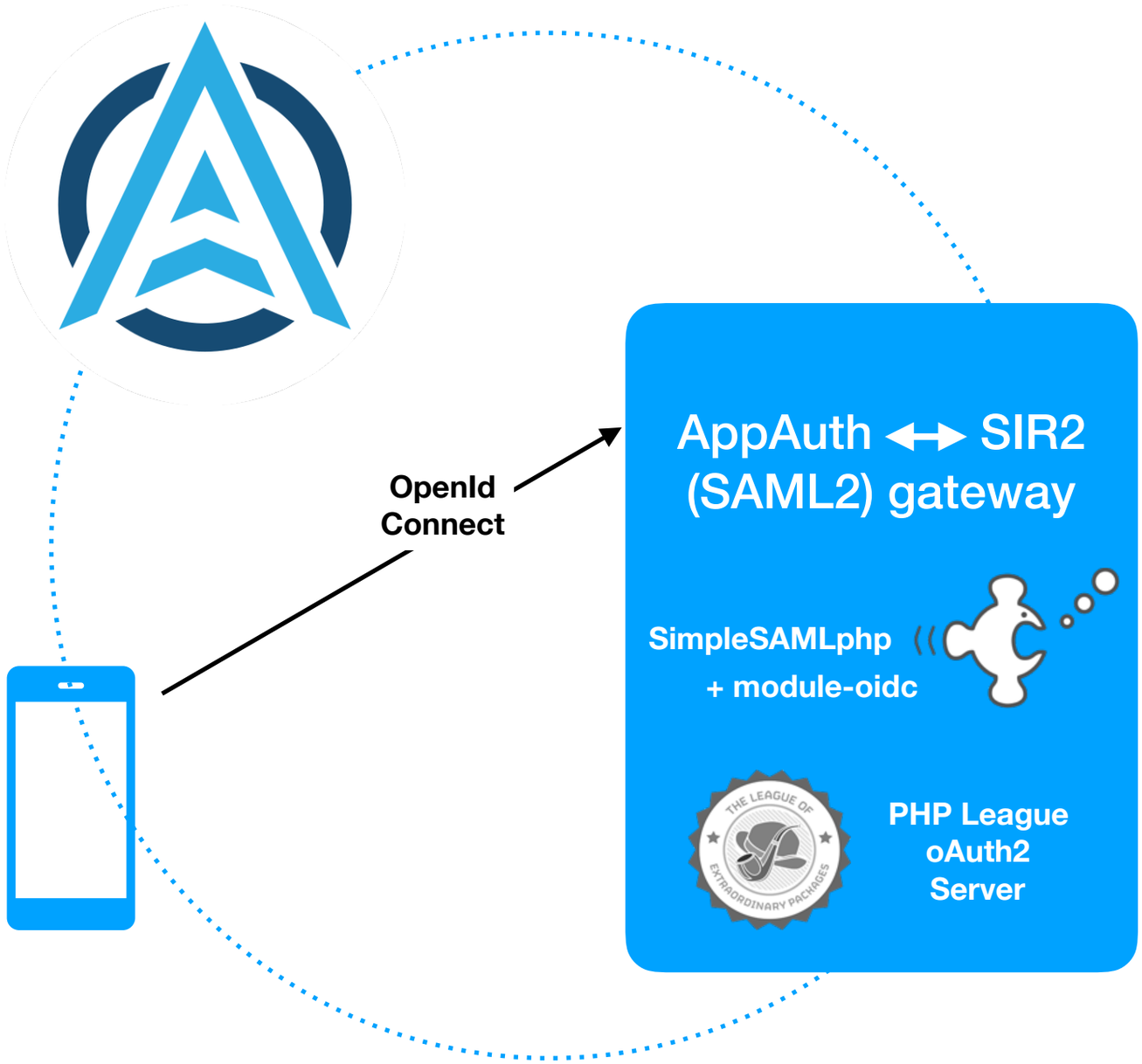
Authentication Flow



discovery_url: `https://appauthgw.sir2…/.well-known/openid-configuration`

redirect_URI: `es.rediris.sir2.appauth-demo://oauth2redirect`

Authentication Flow



SIR2

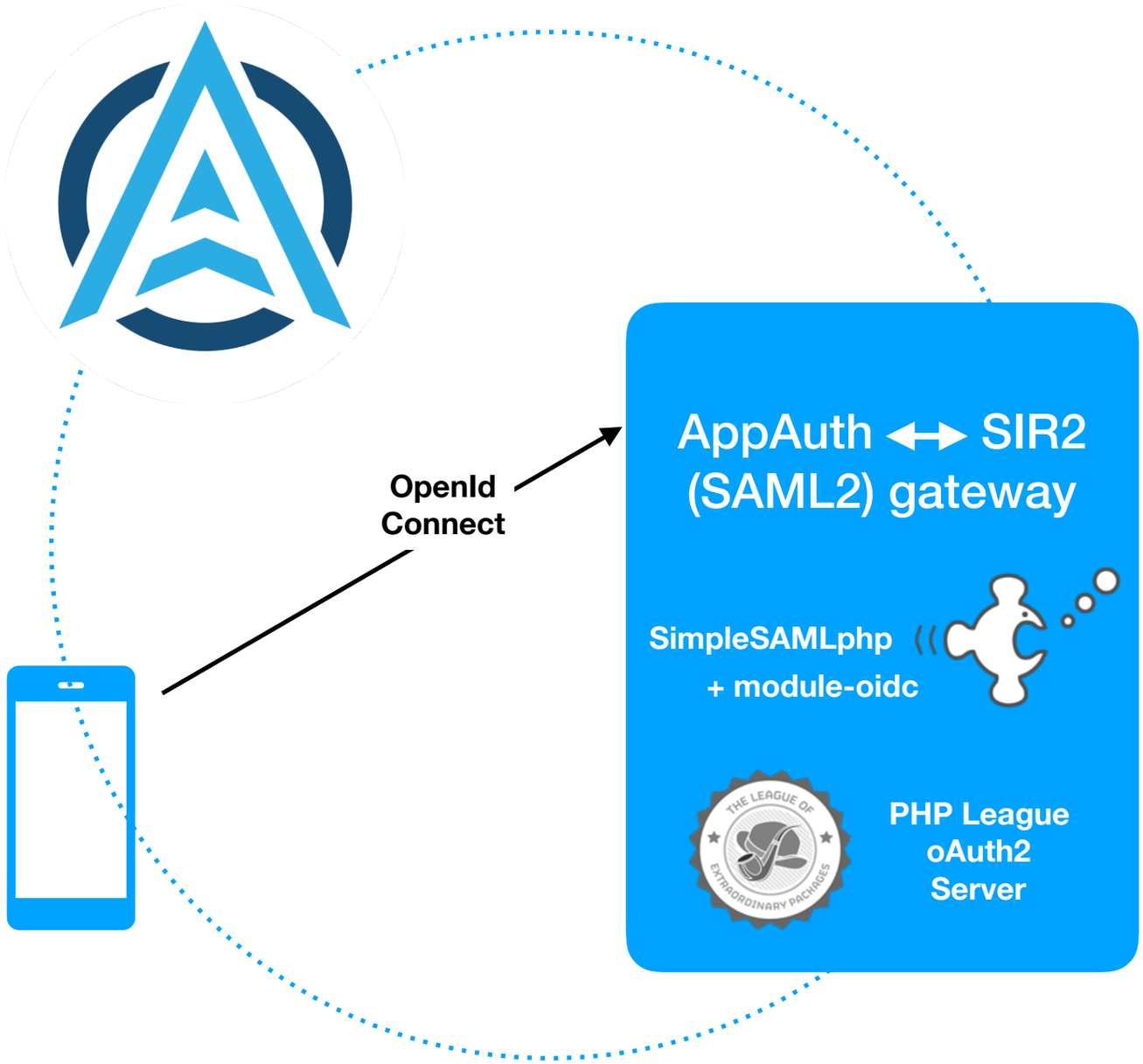
IdPs

discovery_url: https://appauthgw.sir2…/.well-known/openid-configuration

redirect_URI: es.rediris.sir2.appauth-demo://oauth2redirect

GOBIERNO DE ESPAÑA · MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD · MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL · Red IRIS red.es · Infraestructuras Científicas y Técnicas Singulares

Authentication Flow



SIR2

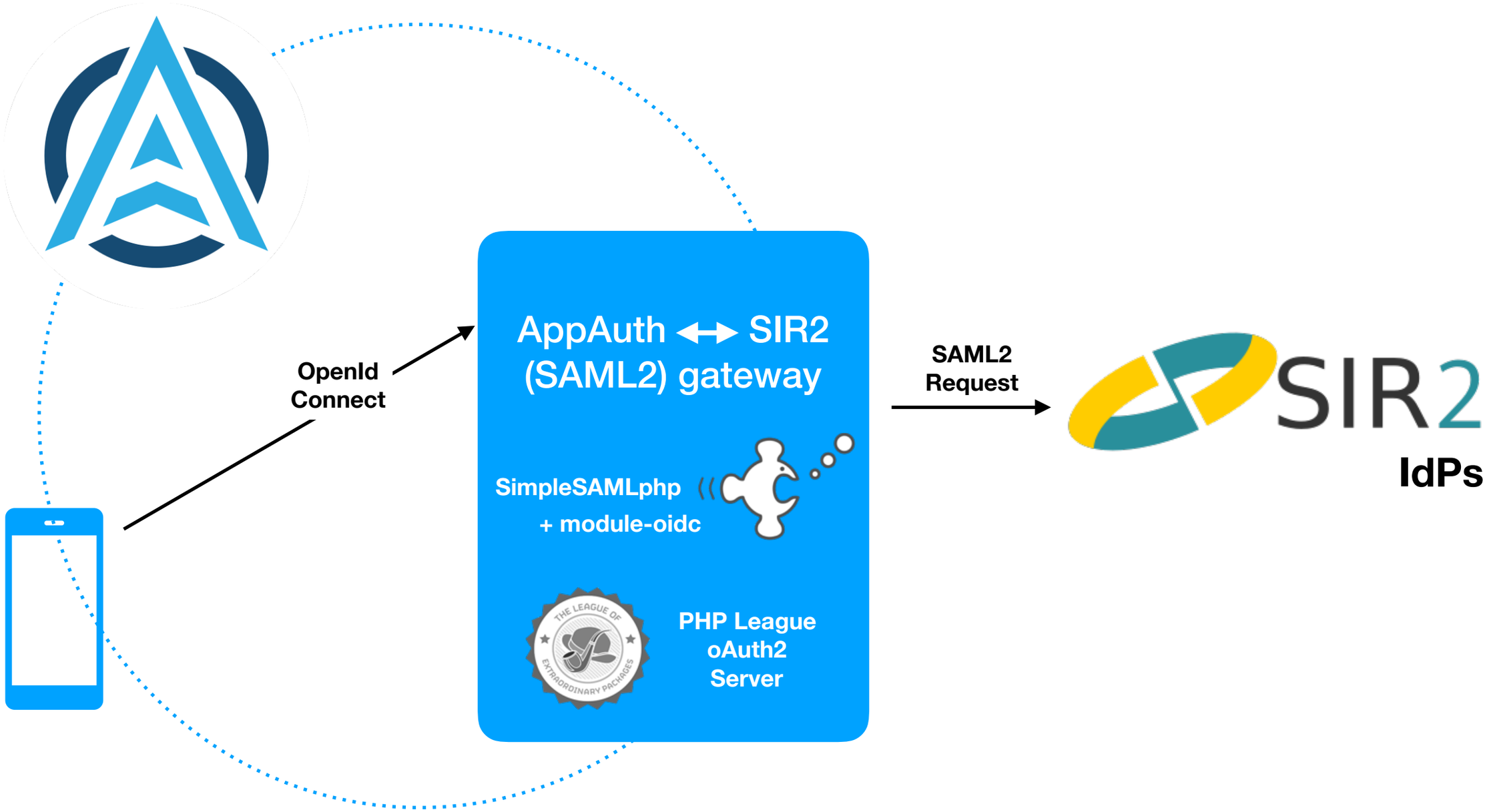
IdPs

GOBIERNO DE ESPAÑA
MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

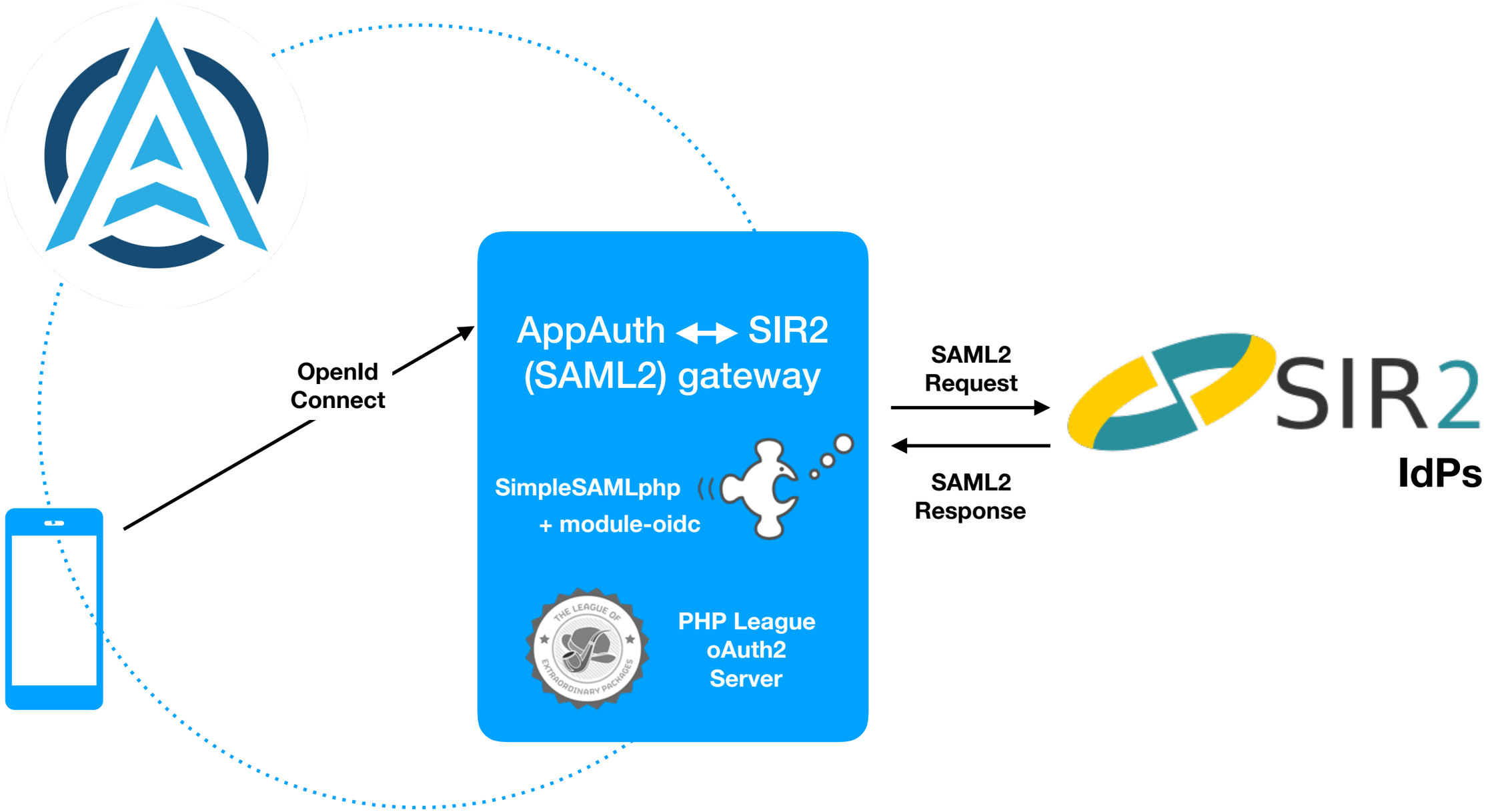
RedIRIS
red.es

Infraestructuras Científicas y Técnicas Singulares

Authentication Flow

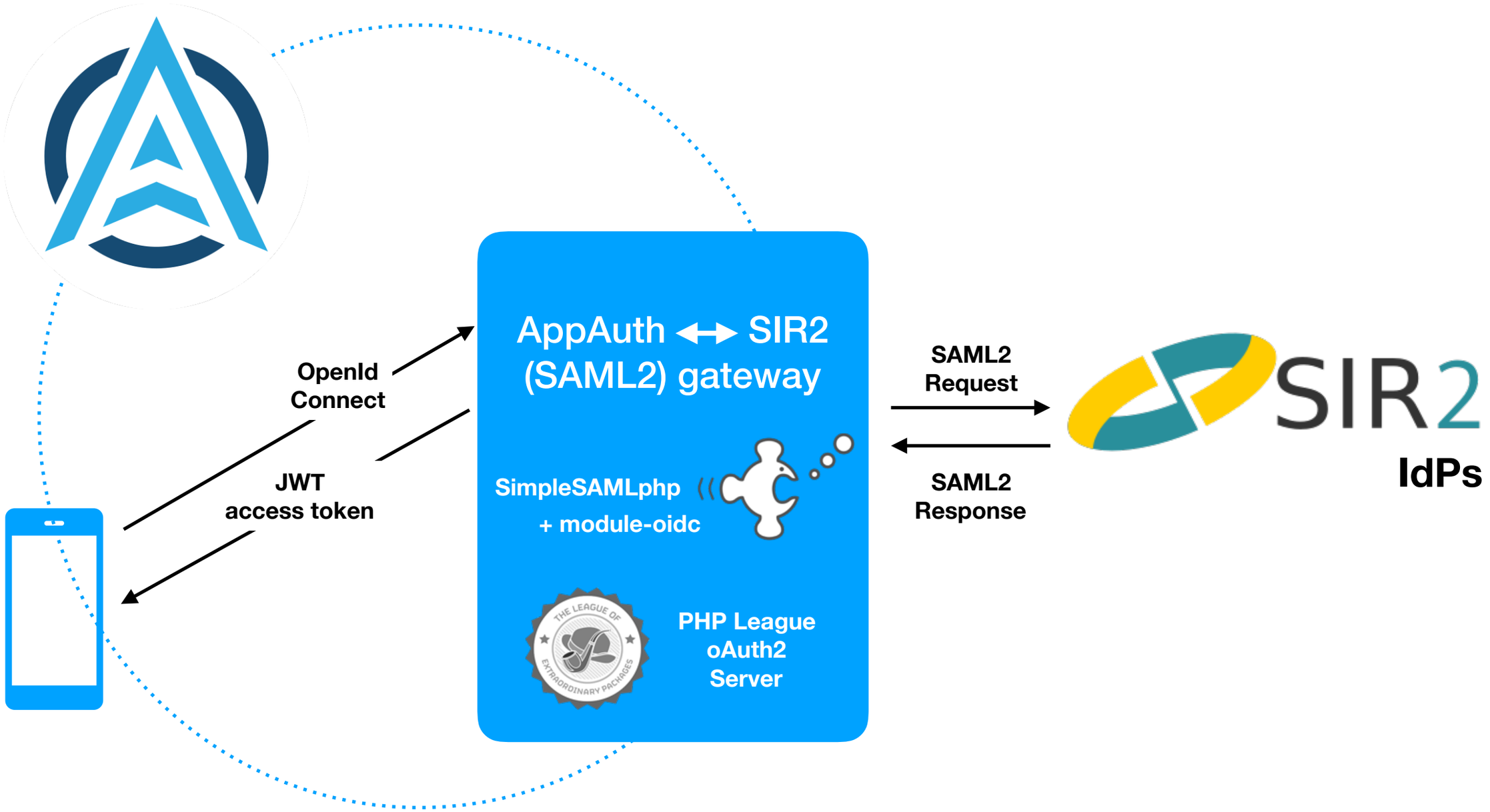


Authentication Flow

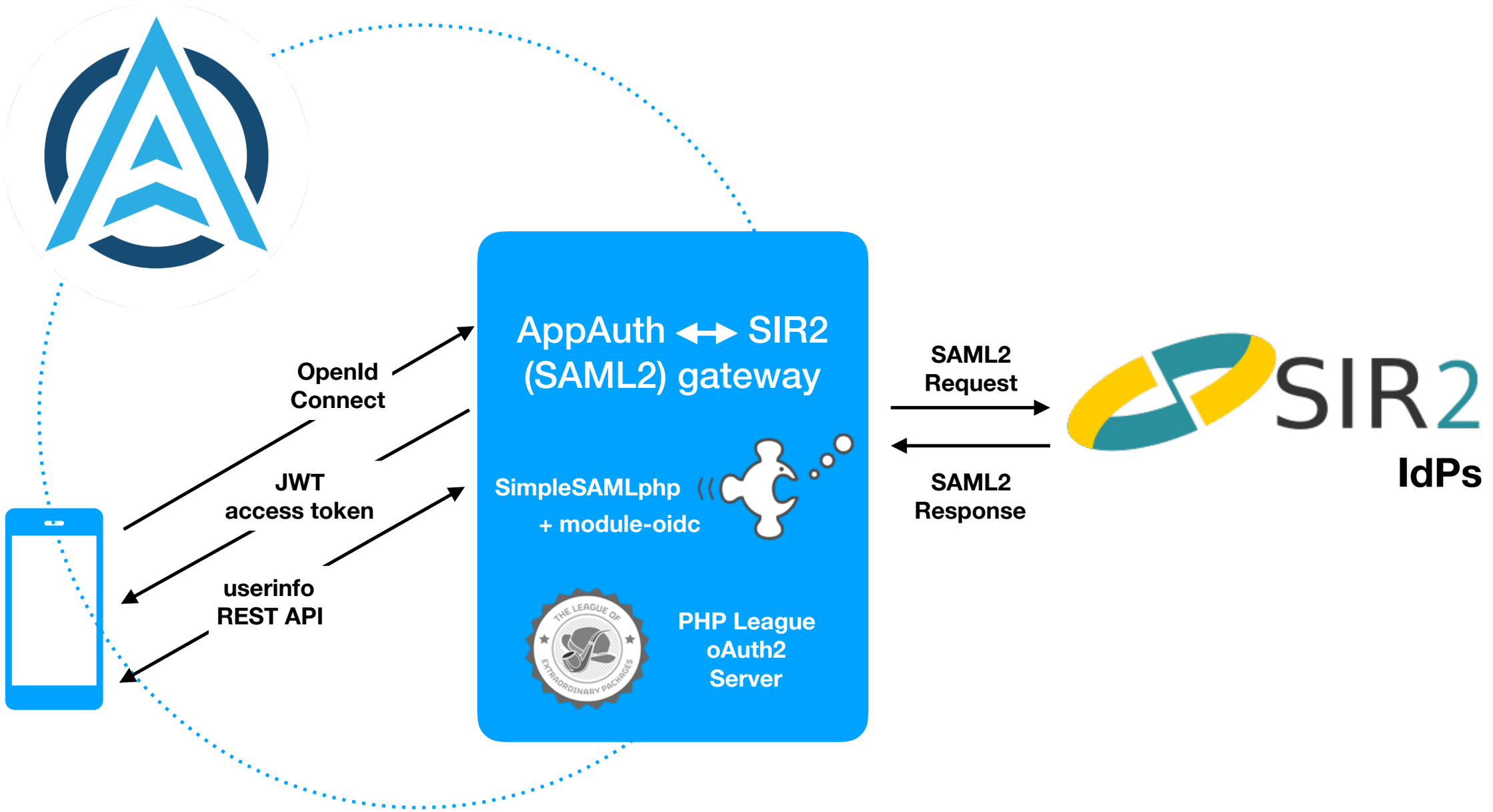


GOBIERNO DE ESPAÑA
MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
red IRIS
red.es
tic Infraestructuras Científicas y Técnicas Singulares

Authentication Flow



Authentication Flow



GOBIERNO DE ESPAÑA
MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
red IRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

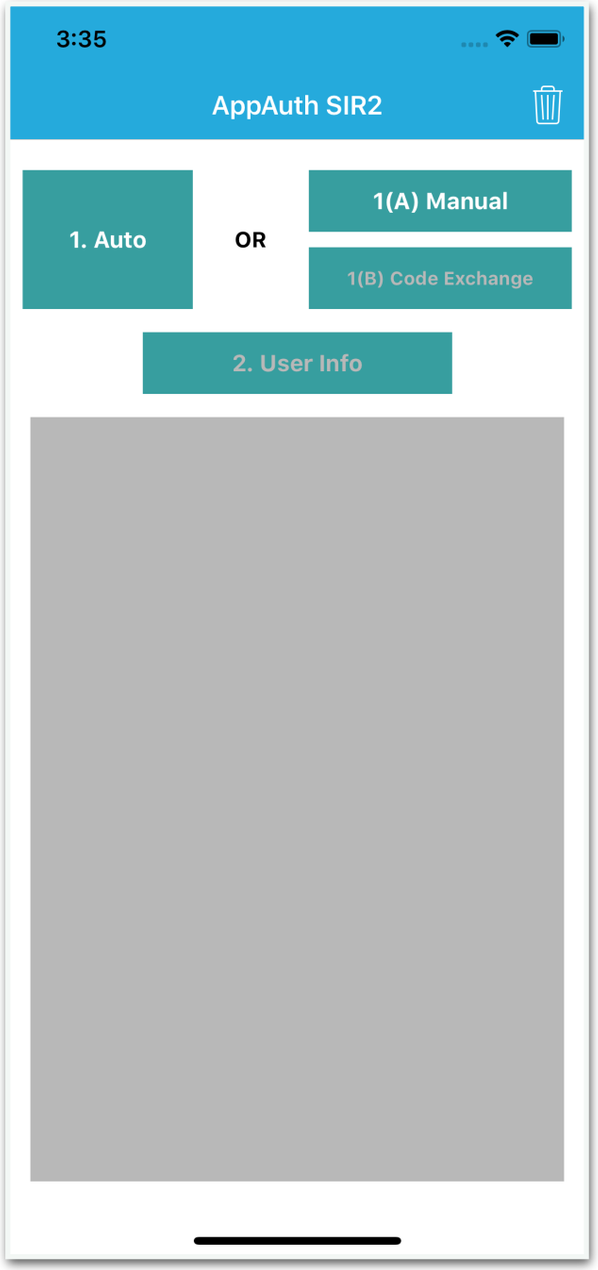
implementation details

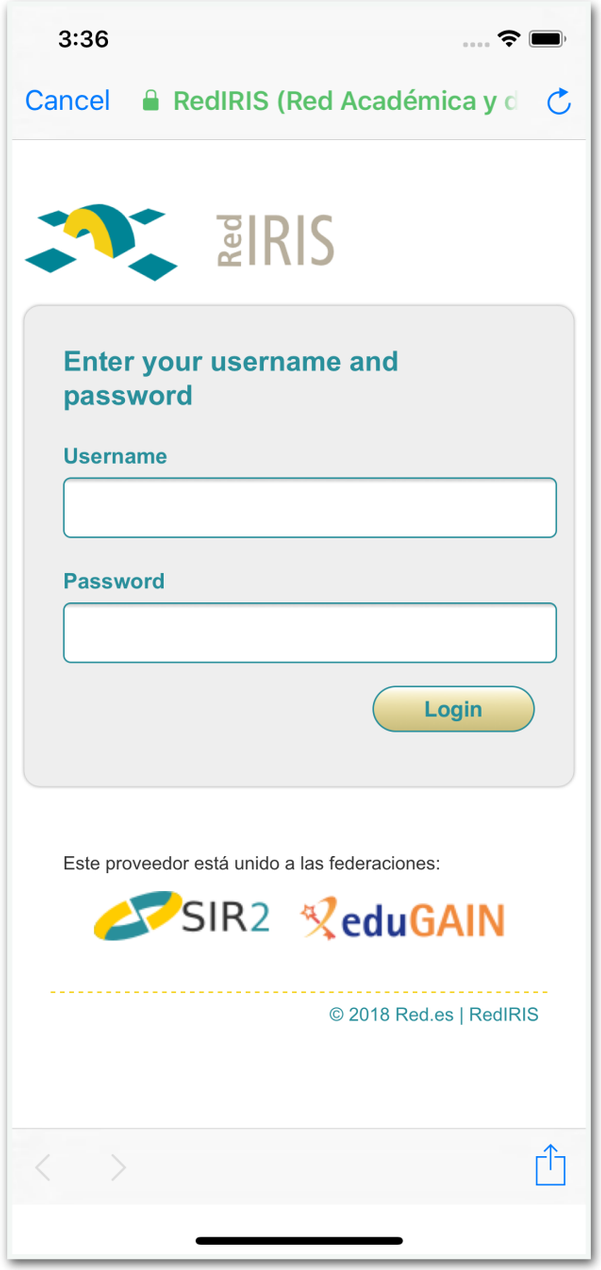
- SimpleSAMLphp with module-oidc by Sergio Gómez
  - https://github.com/rediris-es/simplesamlphp-module-oidc
- The module uses PHP League's oAuth2 Server by Alex Bilbie et al.
- We recommend the appauth.io library for the clients

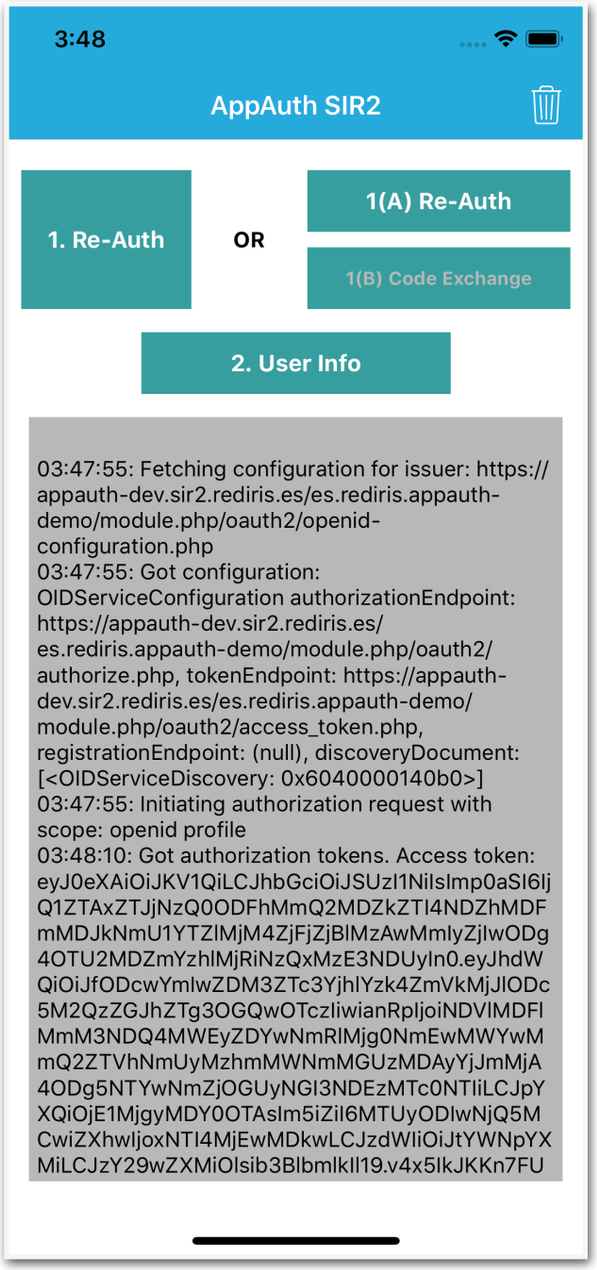
- The SAML world is connected as a 'remote IdP'
- We can use a central (SAML) discovery service, or directly contact a specific identity provider
- The gateway stores basic information, accessible only by the authenticated client

GOBIERNO DE ESPAÑA
MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL
Red IRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

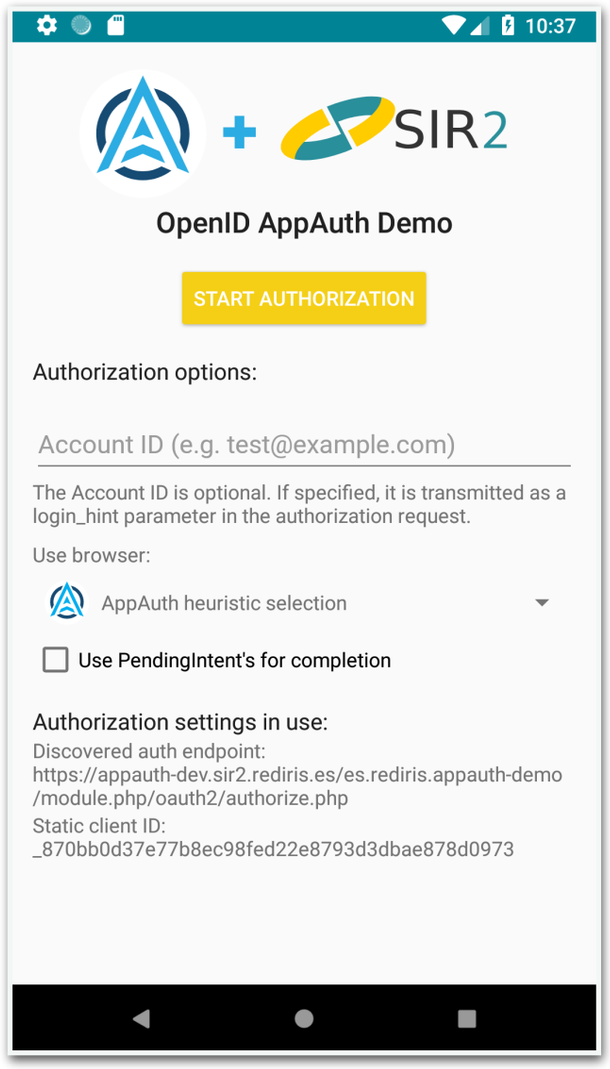
iOS interface

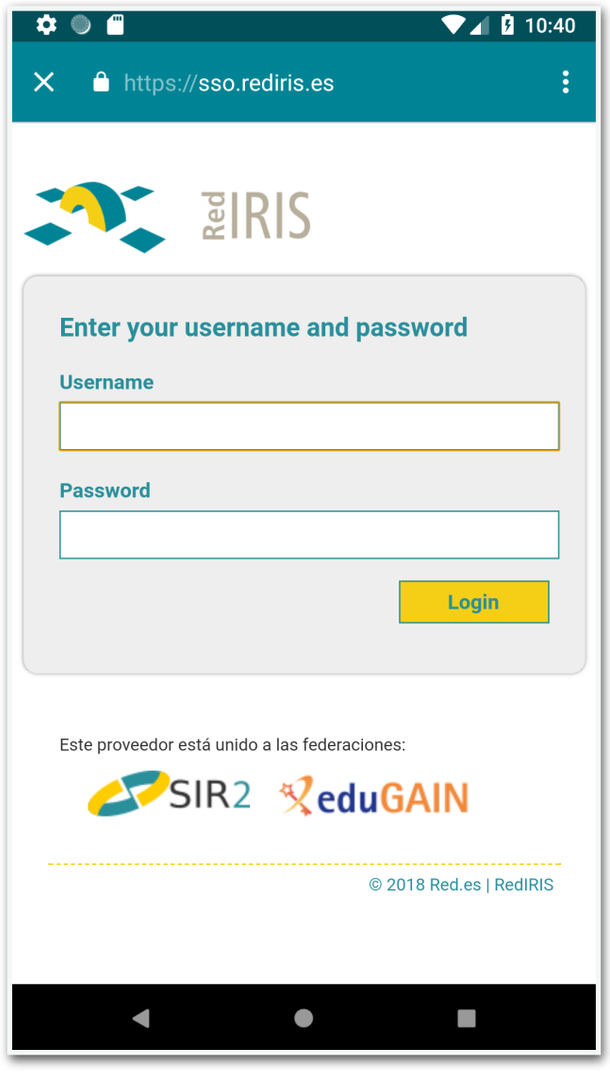


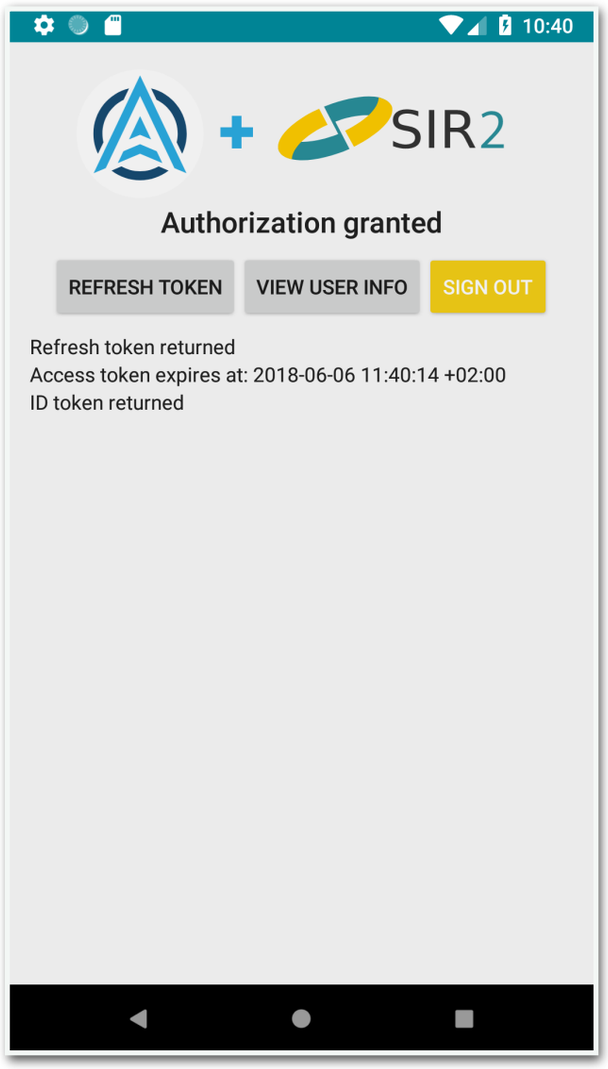




Android interface...







unpublished app available here: https://redir.is/appauthand

GOBIERNO DE ESPAÑA · MINISTERIO ECONOMÍA, INDUSTRIA Y COMPETITIVIDAD · MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL · RedIRIS red.es · tic Infraestructuras Científicas y Técnicas Singulares

Thanks!


GOBIERNO
DE ESPAÑA
MINISTERIO
ECONOMÍA, INDUSTRIA
Y COMPETITIVIDAD
MINISTERIO
DE ENERGÍA, TURISMO
Y AGENDA DIGITAL


Red IRIS
red.es


Infraestructuras
Científicas y Técnicas
Singulares