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

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

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.

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

AppAuth ↔ SIR2 (SAML2) gateway

SimpleSAMLphp + module-oidc

PHP League OAuth2 Server

SIR2

IdPs
discovery_url: https://appauthgw.sir2.../.well-known/openid-configuration
redirect_URI: es.rediris.sir2.appauth-demo://oauth2redirect
**Authentication Flow**

- **IdPs**
- **AppAuth**
- **SIR2**
- **OpenId Connect**

**SimpleSAMLphp + module-oidc**

**PHP League OAuth2 Server**

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

**redirect_URI**: es.rediris.sir2.appauth-demo://oauth2redirect
Authentication Flow

AppAuth <-> SIR2 (SAML2) gateway

OpenId Connect

SimpleSAMLphp + module-oidc

PHP League OAuth2 Server

IdPs
Authentication Flow

- SAML2 Request
- OpenID Connect
- SimpleSAMLphp + module-oidc
- PHP League OAuth2 Server

AppAuth ↔ SIR2 (SAML2) gateway

IdPs

SIR2

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA, INDUSTRY
Y COMPETITIVIDAD
MINISTERIO DE ENERGÍA, TURISMO
Y AGENDA DIGITAL
red.es
Authentication Flow

IdPs

SAML2

Request

AppAuth ↔ SIR2 (SAML2) gateway

OpenId Connect

SimpleSAMLphp + module-oidc

PHP League oAuth2 Server

SAML2 Request

SAML2 Response

SIR2

IdPs
Authentication Flow

- **AppAuth ↔ SIR2 (SAML2) gateway**
  - SimpleSAMLphp + module-oidc
  - PHP League OAuth2 Server

- **SAML2 Request**
- **SAML2 Response**

- **IdPs**: SIR2

- **Tokens**: JWT access token, OpenId Connect

- **Access Flow**:
  - **Device**
  - **AppAuth**
  - **(SAML2) gateway**
  - **SIR2**
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
Android interface...

unpublished app available here: https://redir.is/appauthand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