LANDSENSE

A Citizen Observatory and Innovation Marketplace for Land Use and Land Cover Monitoring

Secure Dimensions

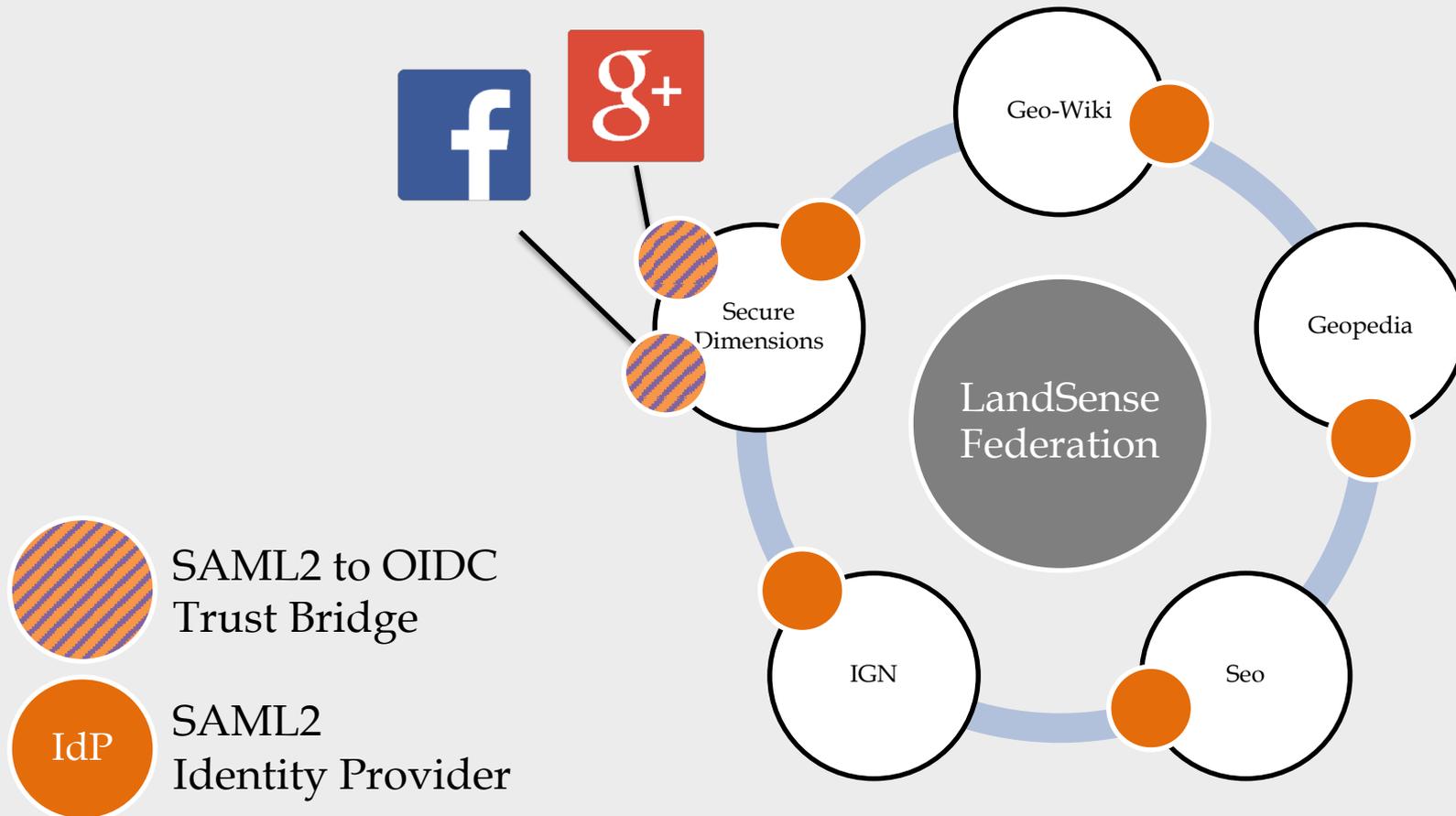This project is funded as an innovation action from the European Union's Horizon 2020 funding program under grant agreement number 689812

LandSense Engagement Platform

CitSci IE

03.12.2018

Andreas Matheus

LandSense (Authentication) Federation

SAML2 to OIDC Trust Bridge

IdP SAML2 Identity Provider

LandSense Federation Technical Aspects

- LandSense (www.landsense.eu) operates a Coordination Centre which publishes the SAML2 Metadata
    - https://cc.landsense.eu/landsense-metadata.xml
- Coordination Centre operates the IdP Discovery Service
    - https://ds.landsense.eu (SWITCH Discovery Service) with support for embedded WAYF
    - IdP gateways to (currently) Google and Facebook
    - Central LandSense Attribute Authority (later)
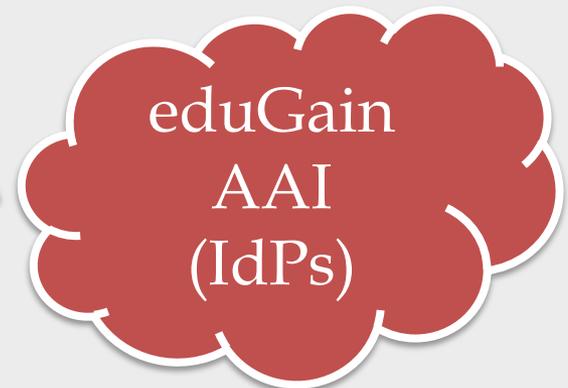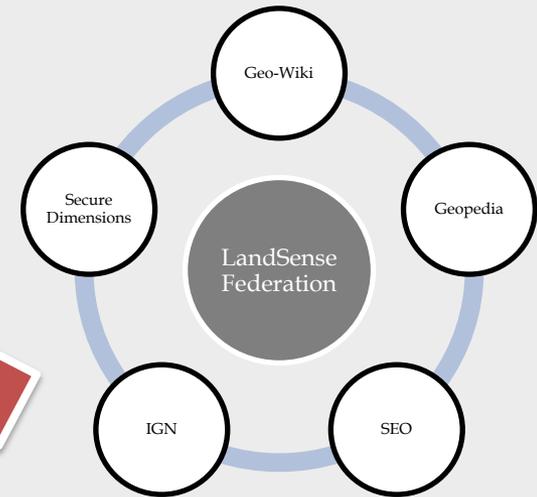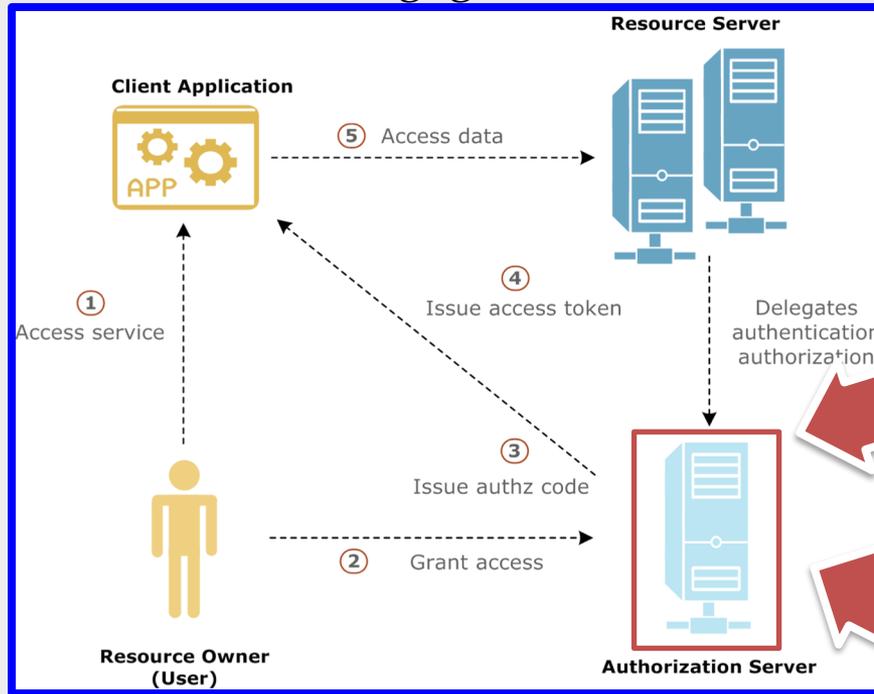- Directly trusted partner IdPs + eduGain IdPs

Linking the Science / Academia

LandSense Engagement Platform Simplified

LandSense Engagement Platform 3rd Party Application

- Standard Web- or Mobile-App development
- Use OAuth2/OIDC SDK and configure for LandSense Authorization Server
  - https://as.landsense.eu/.well-known/openid_configuration
- Register application
  - https://as.landsense.eu
  - Select the Scope(s) that meet your needs
    - Auth => Just information about successful authentication
    - Cryptoname => Unique user identifier that cannot be resolved to personal information
    - Profile => OIDC claims for this scope
    - Email => OIDC claims for this scope
    - Any combination of the above (exclude Auth)
- Operate the Application

LandSense
A Citizen Observatory and Innovation Marketplace
for Land Use and Land Cover Monitoring

LandSense Platform Extension Options

- Extension with an IdP
  - New organization has users
  - Deploy a SAML2 IdP (Shibboleth, SimpleSAMLphp, …) and connect with your user database
  - Register the IdP with the LandSense Coordination Centre or with your national academic federation (e.g. InCommon)

- Extension with an Authorization Server
  - New organization already has an infrastructure based on their Authorization Server with registered applications
  - Enable SAML2 based authentication
  - Register the SP part of the Authorization Server with LandSense or with your national academic federation (.e.g. InCommon)
  - To make the Authorization Server accessible for eduGain users, the SP must be registered with the national Academic Federation

LandSense Engagement Platform Extension with IdP

LandSense Engagement Platform Extension with Authorization Server
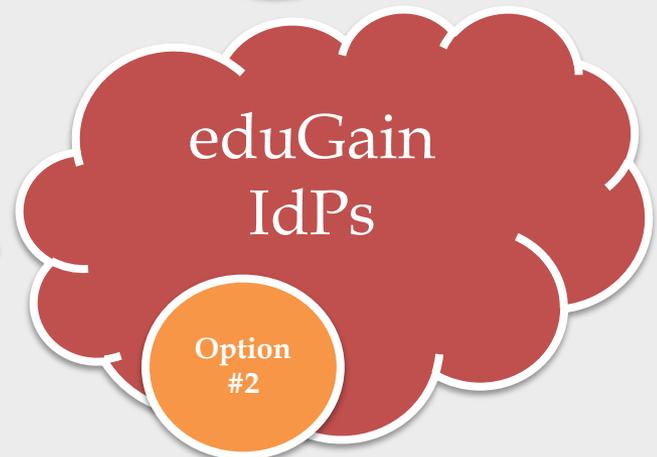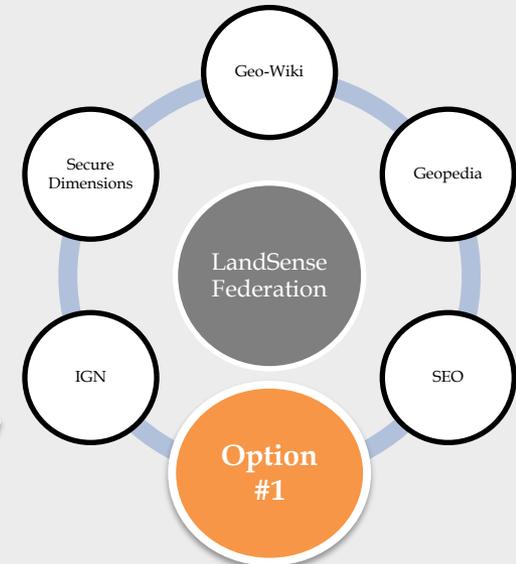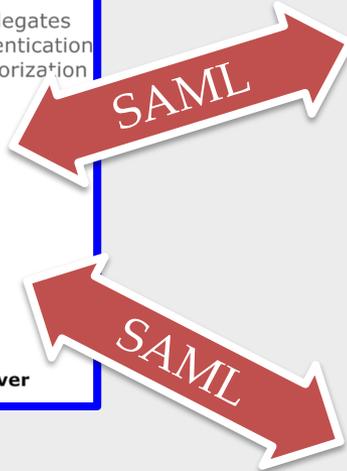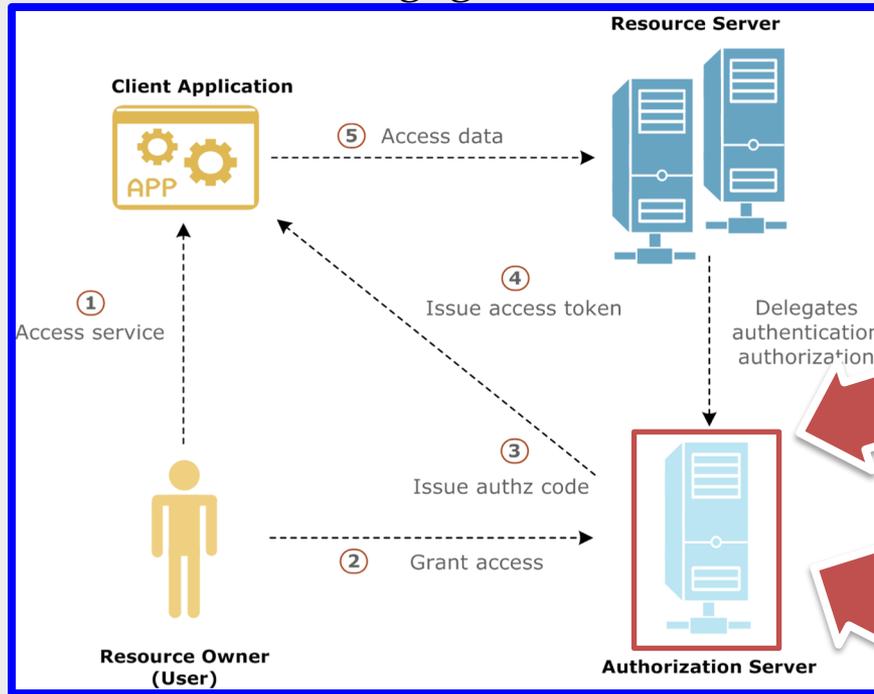
Your Platform

Your Authorization Server's SAML2 SP

SAML (option #1)

LandSense Engagement Platform

SAML (option #2)

SAML

Geo-Wiki

Secure Dimensions

Geopedia

LandSense Federation

IGN

SEO

eduGain AAI (IdPs)

SAML

LandSense
A Citizen Observatory and Innovation Marketplace
for Land Use and Land Cover Monitoring
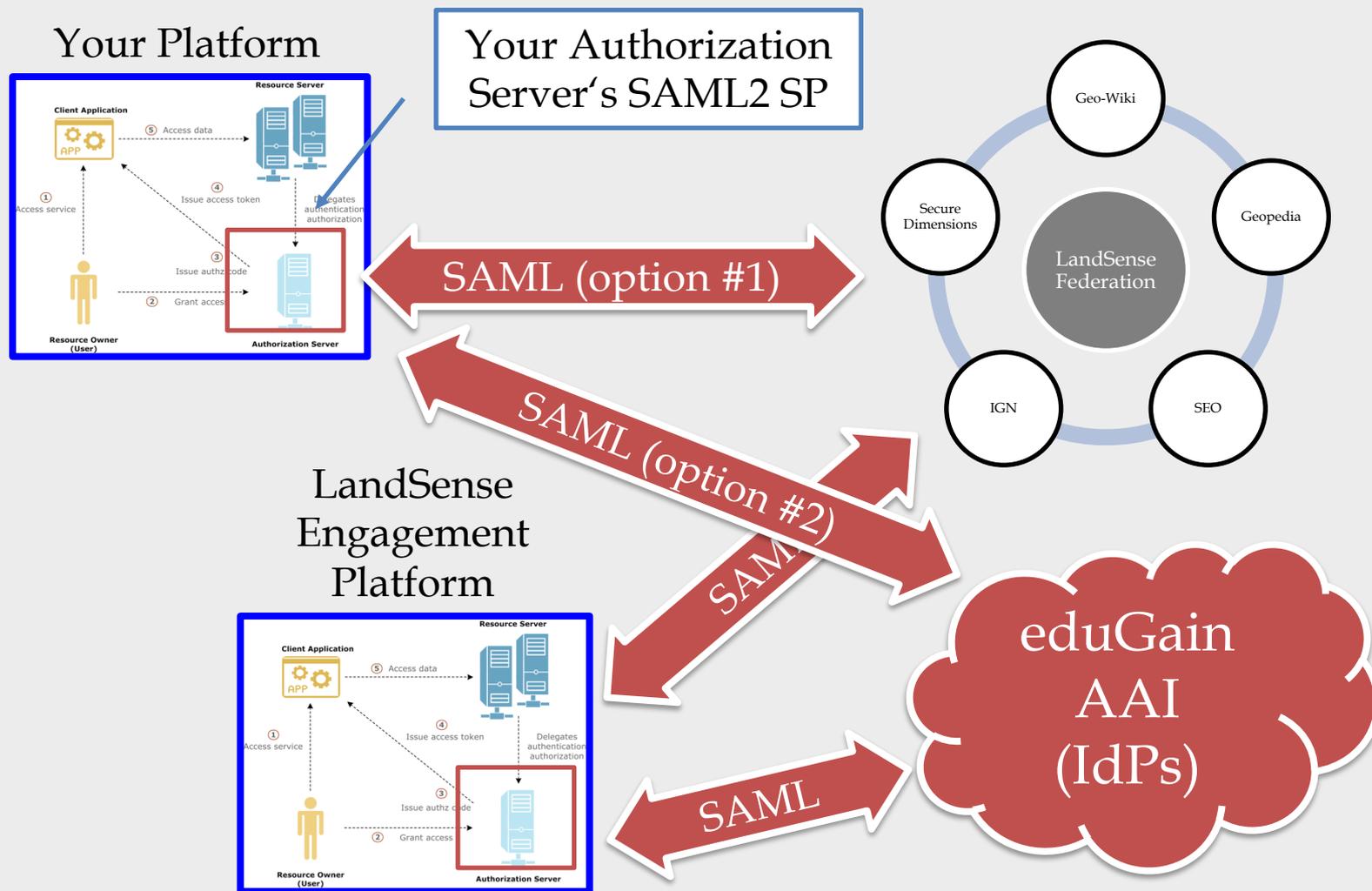
LandSense Engagement Platform Extension with Authorization Server

- The Authorization Server accept SAML2 authentication
  - Map the SAML attributes to OIDC claims
  - Enable these attributes via UserInfo interface
  - Must provide /token and /tokeninfo endpoint
  - Must provide /authorize endpoint
  - Must operate GDPR compliant in terms of personal data collection, processing and storage and /userinfo endpoint
- SAML2 SP part must get registered with the LandSense Coordination Centre
  - => Enables login from LandSense IdPs
- SAML2 SP part can optionally get registered with the national academic federation
  - => Enables login from eduGain IdPs

LandSense
A Citizen Observatory and Innovation Marketplace
for Land Use and Land Cover Monitoring

LandSense Federation and Single-Sign-On

- The Single-Sign-On is important for
  - Enabling GDPR data minimization across services
  - Allow authentication session sharing between different Authorization Servers

- An Application could be registered with multiple Authorization Servers to obtain Access Tokens and access associated Resource Servers. The user won't notice as Single-Sign-On allows automatic session creation and access token release.

  - Registering an Application with multiple Authorization Servers allows the Resource Servers to validate Bearer Access Tokens (no need to use JWT Access Tokens).

  => The application must be able to handle access tokens from multiple Authorization Servers

LandSense
A Citizen Observatory and Innovation Marketplace
for Land Use and Land Cover Monitoring

Single-Sign-On Working Example
First Use of App

Your Platform

2. /authorize

3. login please

6. authn

7. token(s)

1. start app

8. app started

LEP

App registered at **your** platform

4. login

6. authn

5. login challenge

IdP

eduGain

!!! NO Single-Sign-On !!!

LandSense
A Citizen Observatory and Innovation Marketplace
for Land Use and Land Cover Monitoring
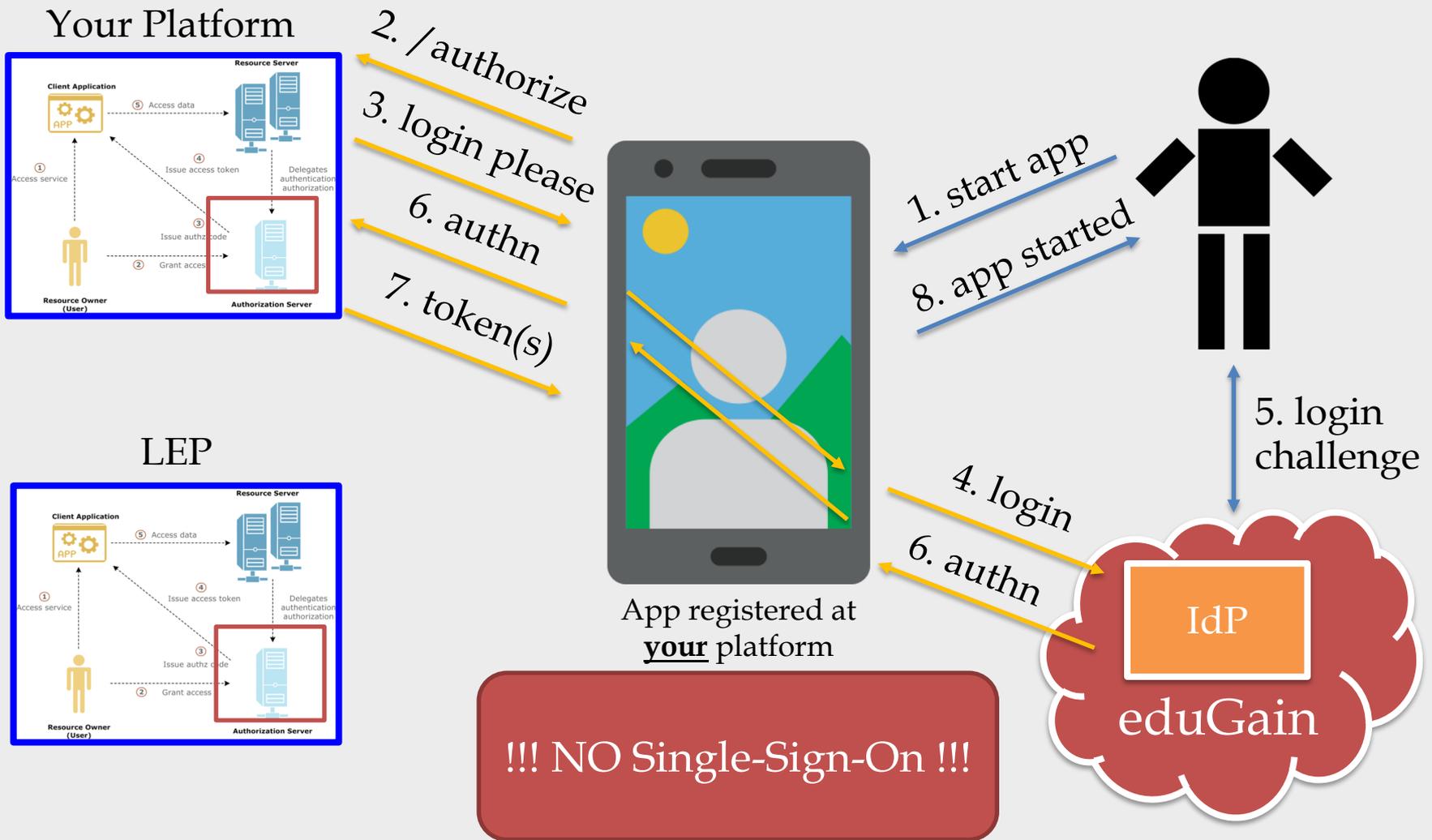
Single-Sign-On Working Example
First Use of App (1/2)
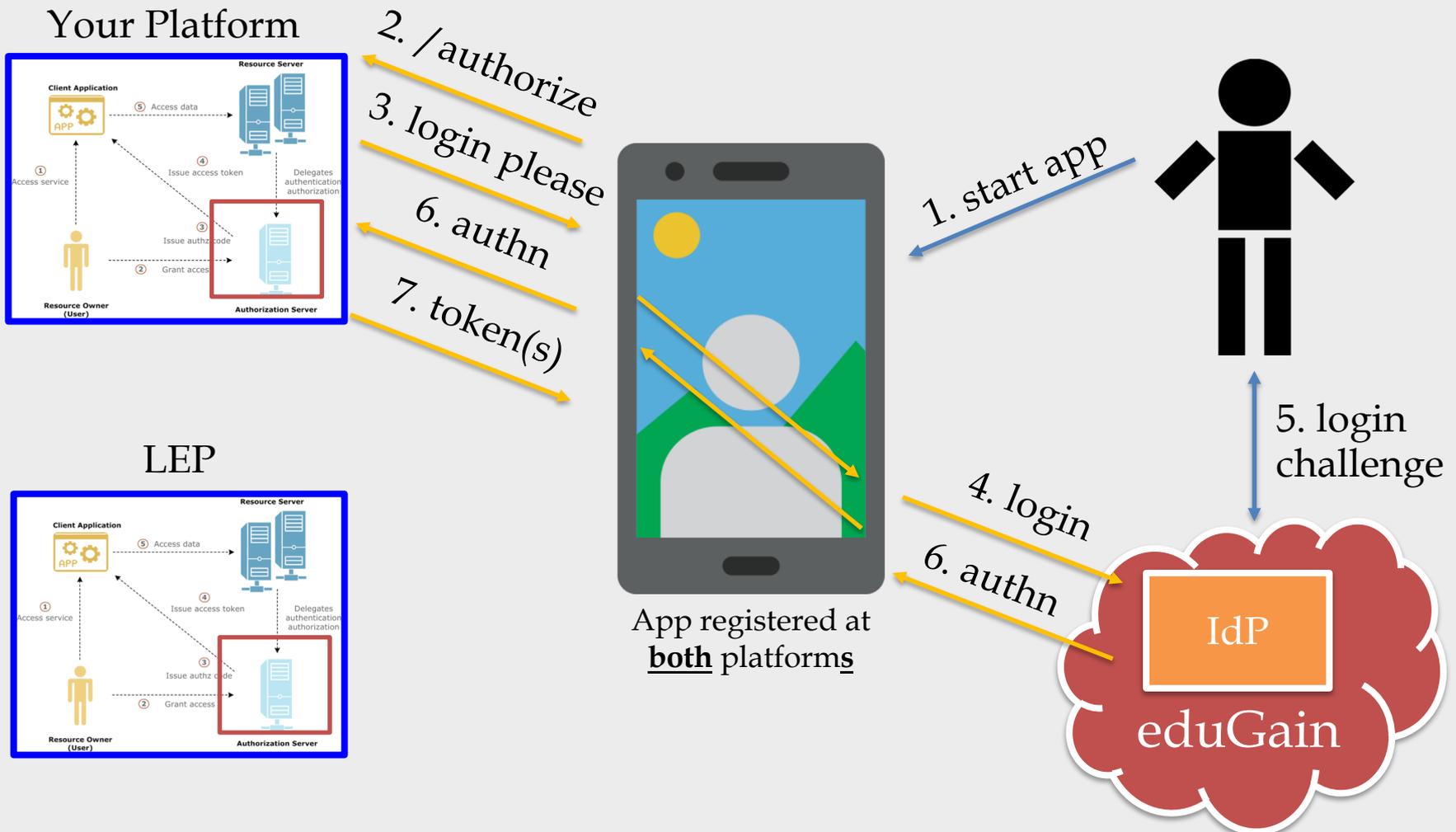
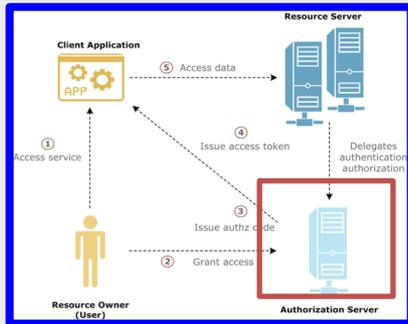# Single-Sign-On Working Example
First Use of App (2/2)

Your Platform
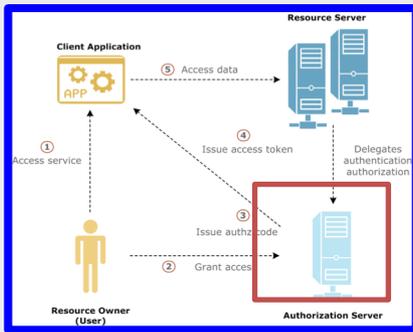
LEP

8. /authorize
9. login please
12. authn
13. token(s)

10. login
11. authn

14. app started

login challenge

IdP

eduGain
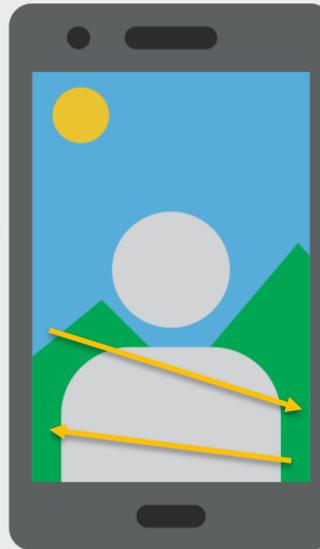
App registered at **both** platform**s**

!!! Single-Sign-On !!!
IdP used existing session for user

LandSense
A Citizen Observatory and Innovation Marketplace
for Land Use and Land Cover Monitoring
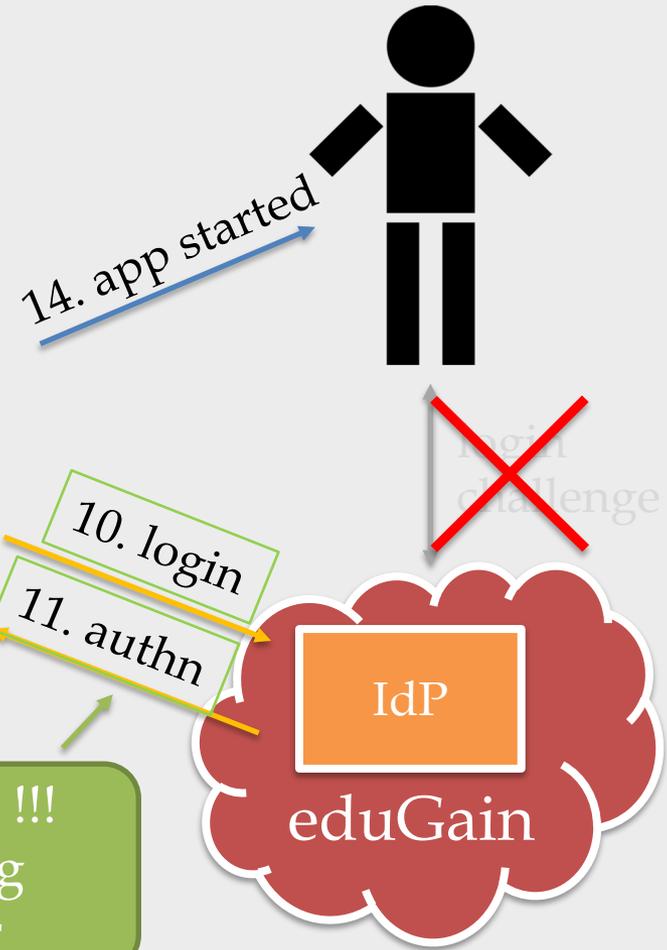
Single-Sign-On Working Example
Use of App (use of Bearer tokens)

Your Platform

validate

2. access token for your platform

1. upload contribution

4. contribution uploaded

LEP

validate

3. access token for LEP

App registered at **both** platform**s**

Application must manage access tokens for either platform

IdP

eduGain

Single-Sign-On Working Example Repeated Use of App

Your Platform

validate

2. access token for your platform

LEP

validate

3. access token for LEP

1. upload contribution

4. contribution uploaded

App registered at **both** platform**s**

Single-Sign-On via Refresh Token(s)

IdP

eduGain

LandSense
A Citizen Observatory and Innovation Marketplace
for Land Use and Land Cover Monitoring

Single-Sign-On Working Example
Use of App (use of JWT tokens)

Your Platform

validate

2. access token from any platform

LEP

validate

3. access token from any platform

1. upload contribution

4. contribution uploaded

App registered at **any** platform

Resource Server can validate token independently

IdP

eduGain

LandSense
A Citizen Observatory and Innovation Marketplace
for Land Use and Land Cover Monitoring

Single-Sign-On Working Example Repeated Use of App (use of JWT tokens)
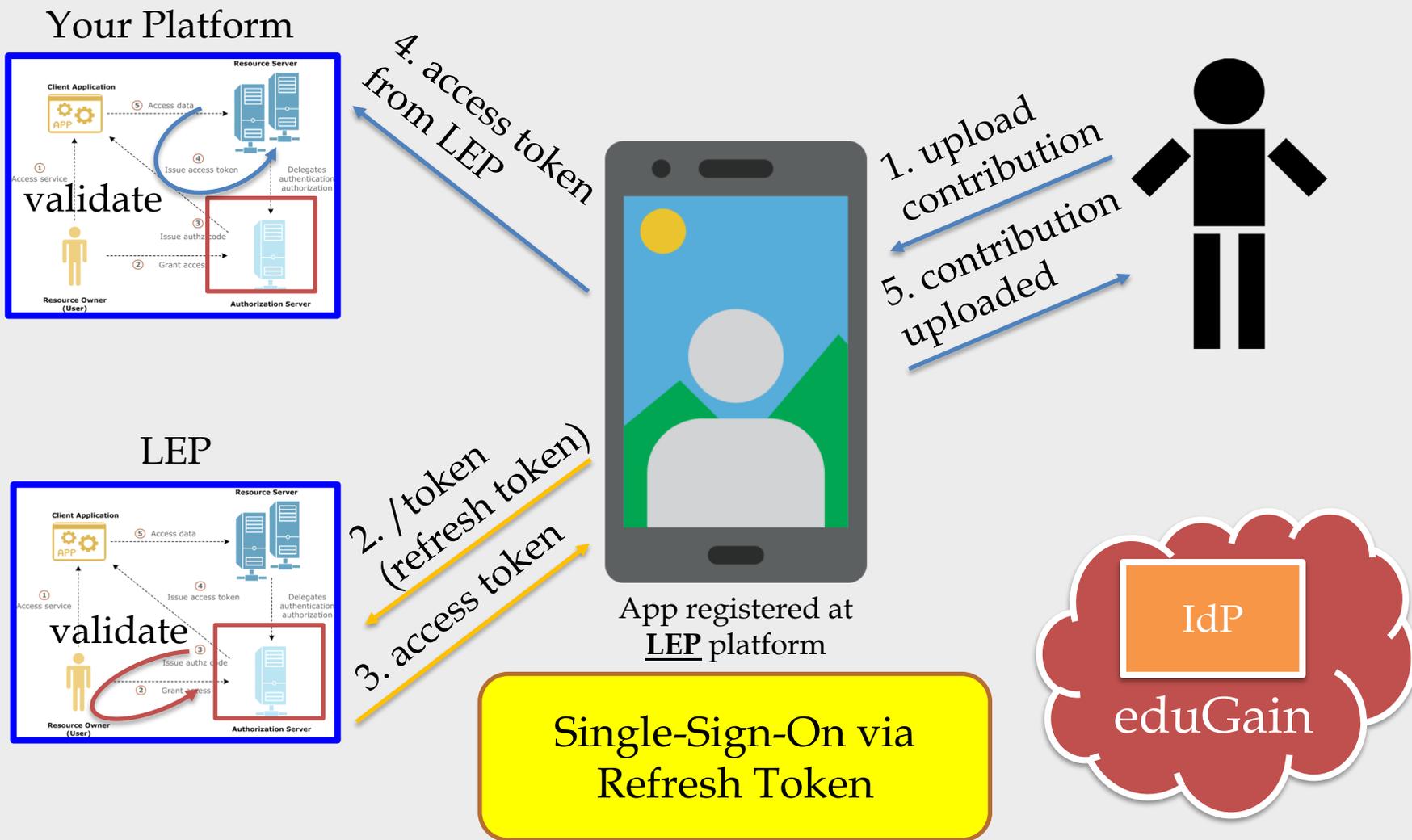
Your Platform

4. access token from LEP

validate

1. upload contribution

5. contribution uploaded

LEP

2. /token (refresh token)

3. access token

validate

App registered at **LEP** platform

Single-Sign-On via Refresh Token

IdP

eduGain

LandSense
A Citizen Observatory and Innovation Marketplace
for Land Use and Land Cover Monitoring

LandSense

A Citizen Observatory and Innovation Marketplace
for Land Use and Land Cover Monitoring

Andreas Matheus
Secure Dimensions GmbH
am@secure-dimensions.de

Connect with us!

info@landsense.eu

 LandSense.eu

 @LandSense

European Commission

Horizon 2020
European Union funding
for Research & Innovation