# LANDSENSE

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

Secure Dimensions

# The LandSense Engagement Platform

# Realization of GDPR Compliance and Lessons Learned with Login from eduGAIN

## AAI-Forum - 70. DFN-Betriebstagung
## Berlin

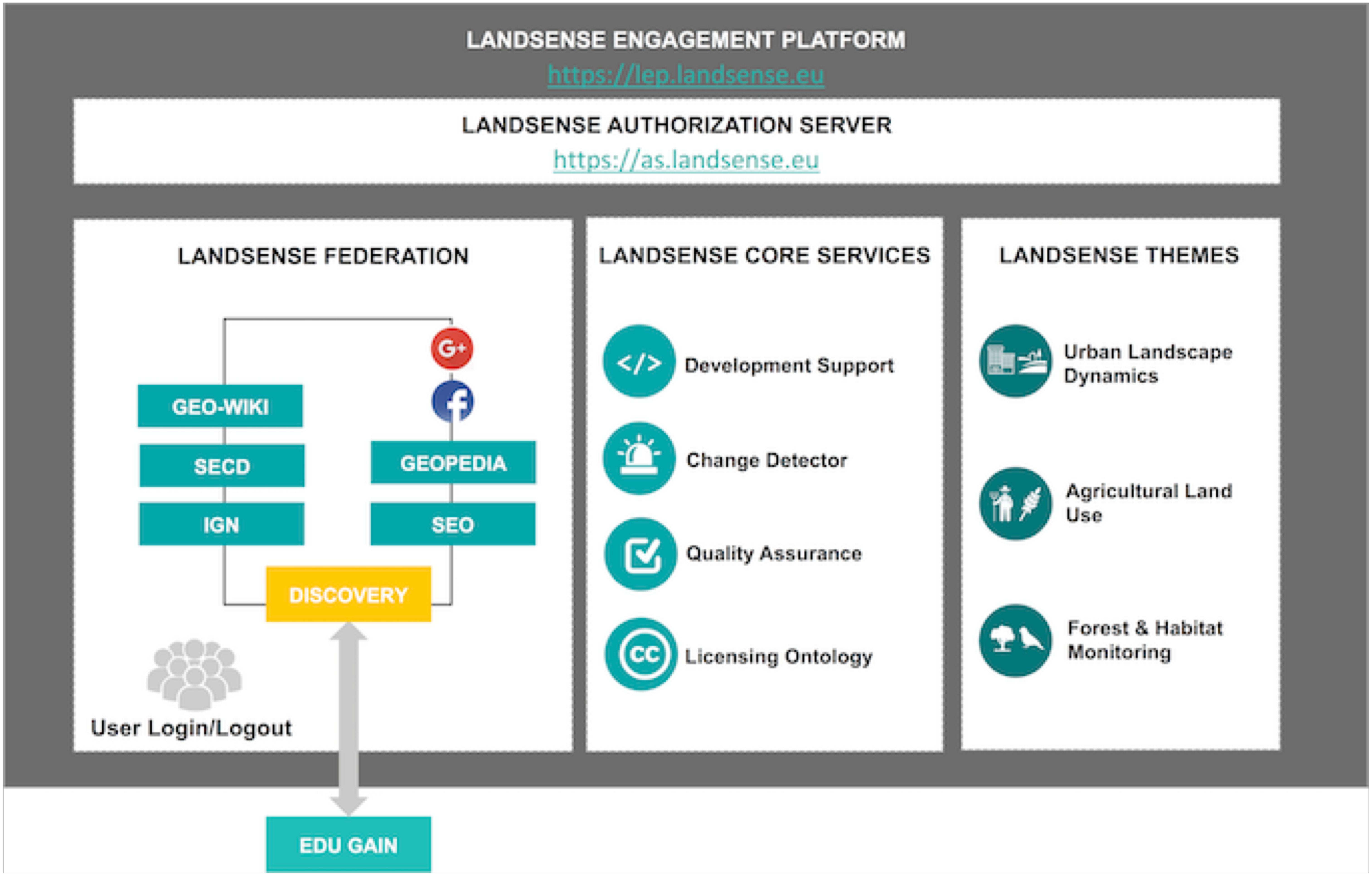
19. März 2019

Andreas Matheus

# About LandSense

- One of 4 European Flagship Citizen Observatories
- Citizen Science Engagement Platform
- Public Participation / Incubator
- Campaigns on Land Use / Land Cover and Change in Austria, France, Germany, Serbia and Spain
- Participate as citizen or scientist
- Engage as application developer
- Use our apps, services, APIs and data sets
- Provide services, APIs or other tools

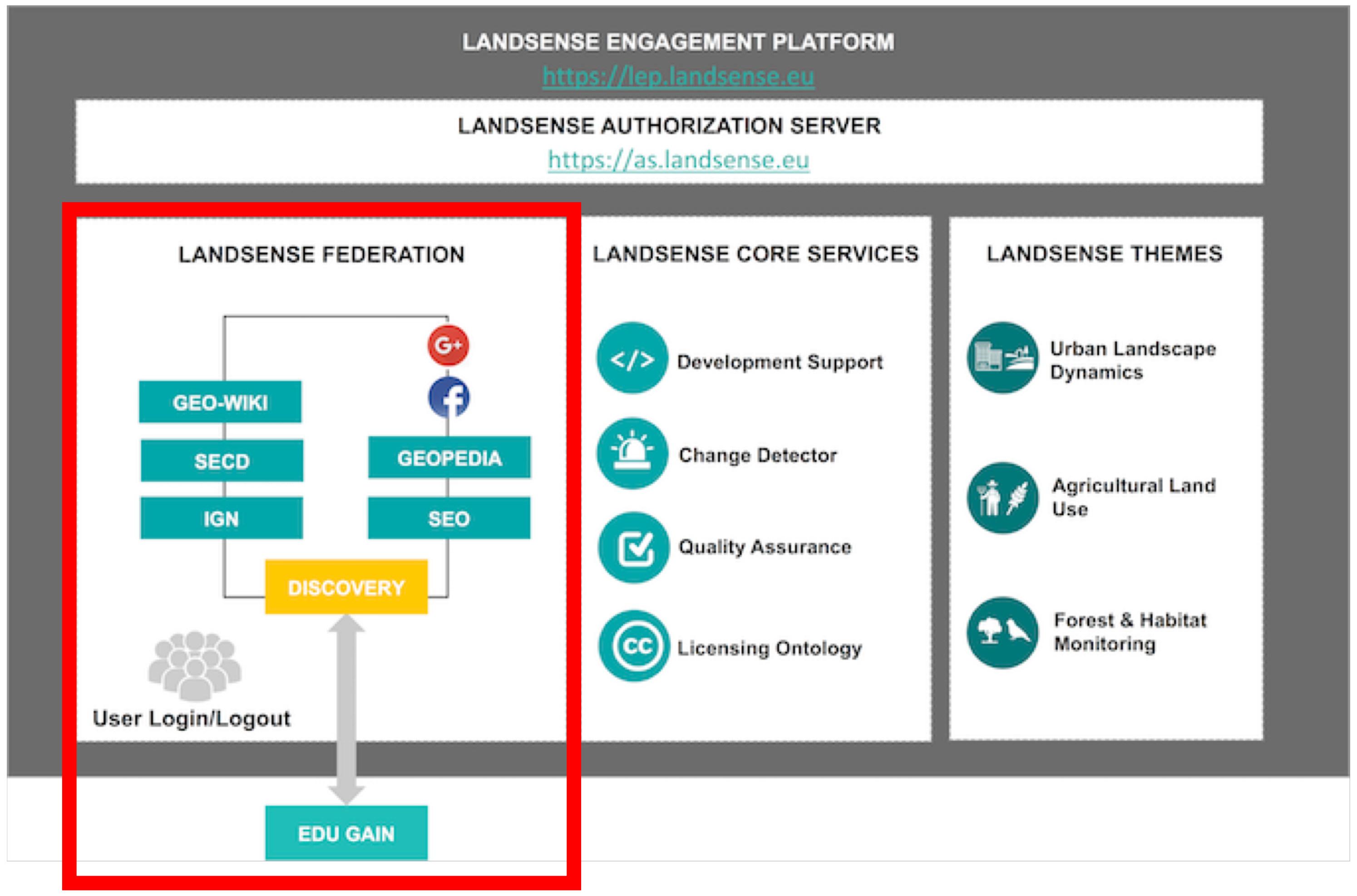
# LandSense Engagement Platform



# LandSense Engagement Platform

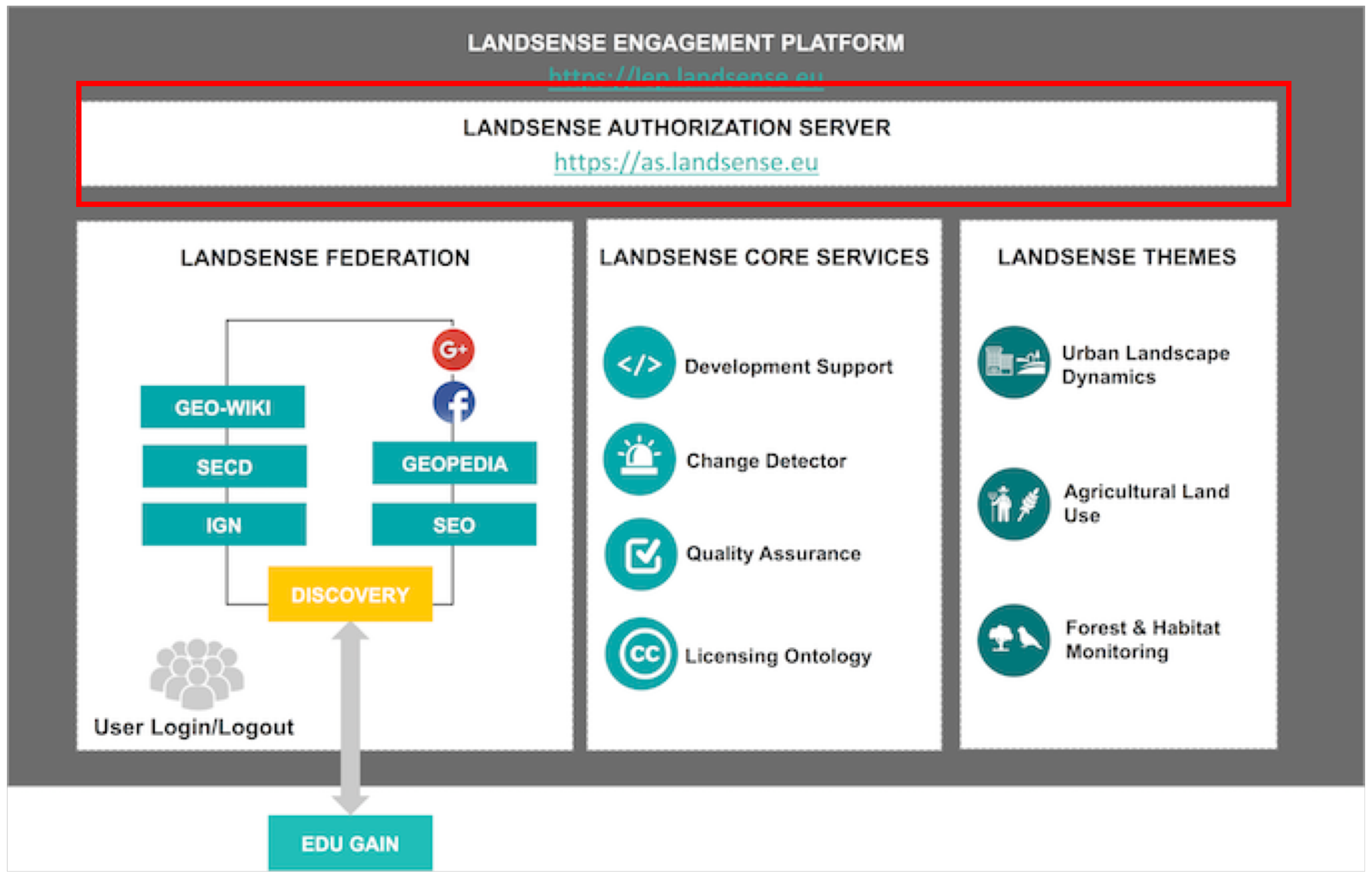
## Authentication Federation

- Circle of Trust managed by the LandSense coordination center
- Login options with LandSense partners, Google, Facebook and Academic Federations via eduGAIN



## Authorization Server

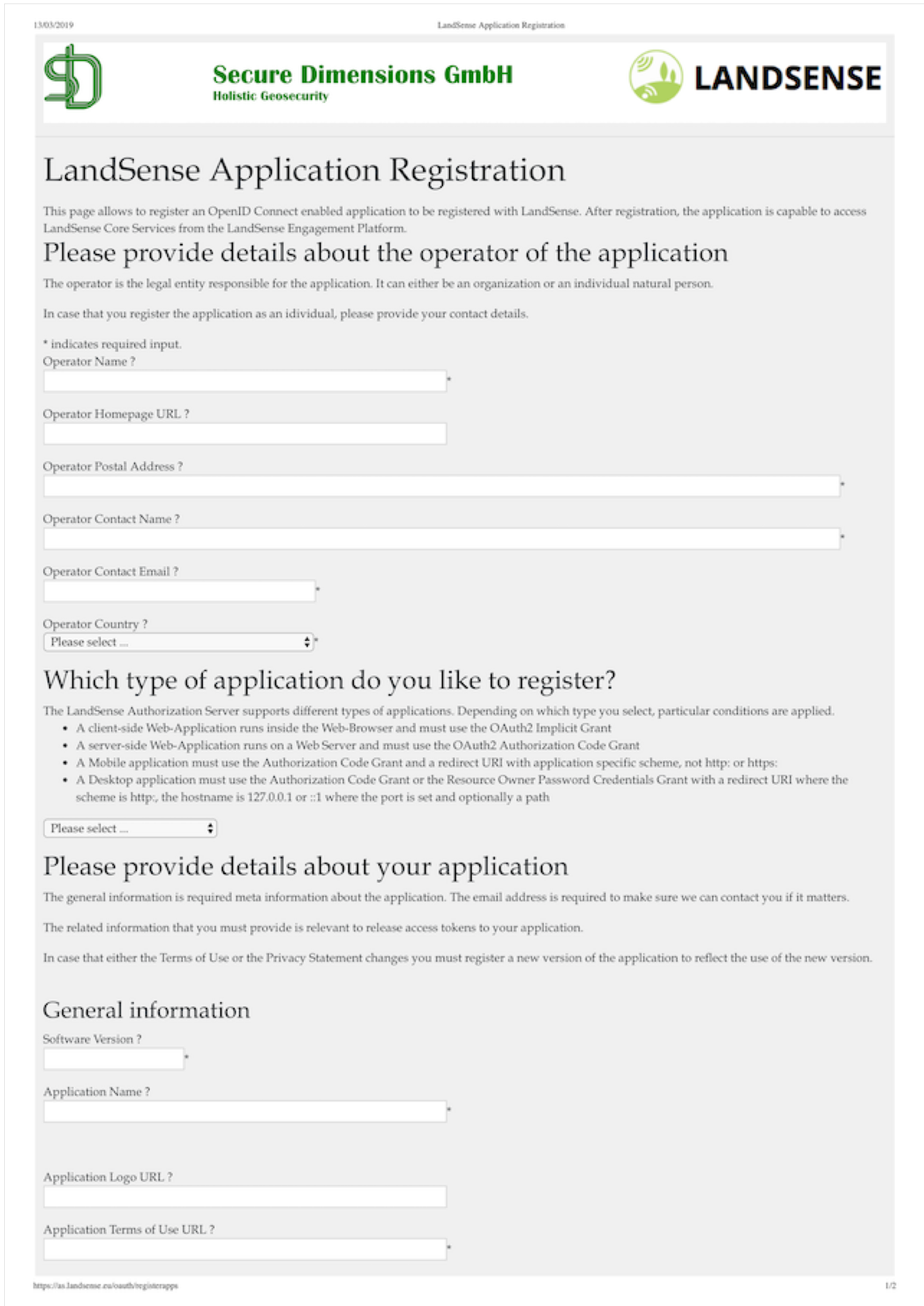
- OpenID Connect compliant with SAML based Login from LandSense Federation (and eduGAIN)
- Broker of Personal Information from login IdP to registered App



# LandSense and GDPR (1/2)

- **GDPR mandates the rules for processing Personal Data in Europe becoming affective May 25, 2018**
- **LandSense Authorization Server – as Broker of personal data – is GDPR compliant. Complicated Privacy Statement**
- **When registering an App with the Authorization Server, operator must provide details (including Privacy Policy URL)**
  - **Must choose the amount of personal data wanted**
- **Personal Data levels support GDPR Data Minimization**
  - **Auth(enticated): No personal data**
  - **Cryptoname: No personal data just a one-way hash of user unique identifier (requires IdP to release it)**
  - **Profile: Personal Data as defined by OIDC scope *profile***
  - **Email: Personal Data as defined by OIDC scope *email***

# LandSense Application Registration



13/03/2019 LandSense Application Registration

Secure Dimensions GmbH
Holistic Geosecurity

LANDSENSE

## LandSense Application Registration

This page allows to register an OpenID Connect enabled application to be registered with LandSense. After registration, the application is capable to access LandSense Core Services from the LandSense Engagement Platform.

## Please provide details about the operator of the application

The operator is the legal entity responsible for the application. It can either be an organization or an individual natural person.

In case that you register the application as an idividual, please provide your contact details.

* indicates required input.

Operator Name ? *

Operator Homepage URL ?

Operator Postal Address ? *

Operator Contact Name ? *

Operator Contact Email ? *

Operator Country ? Please select ... *

## Which type of application do you like to register?

The LandSense Authorization Server supports different types of applications. Depending on which type you select, particular conditions are applied.

- A client-side Web-Application runs inside the Web-Browser and must use the OAuth2 Implicit Grant
- A server-side Web-Application runs on a Web Server and must use the OAuth2 Authorization Code Grant
- A Mobile application must use the Authorization Code Grant and a redirect URI with application specific scheme, not http: or https:
- A Desktop application must use the Authorization Code Grant or the Resource Owner Password Credentials Grant with a redirect URI where the scheme is http:, the hostname is 127.0.0.1 or ::1 where the port is set and optionally a path

Please select ...

## Please provide details about your application

The general information is required meta information about the application. The email address is required to make sure we can contact you if it matters.

The related information that you must provide is relevant to release access tokens to your application.

In case that either the Terms of Use or the Privacy Statement changes you must register a new version of the application to reflect the use of the new version.

### General information

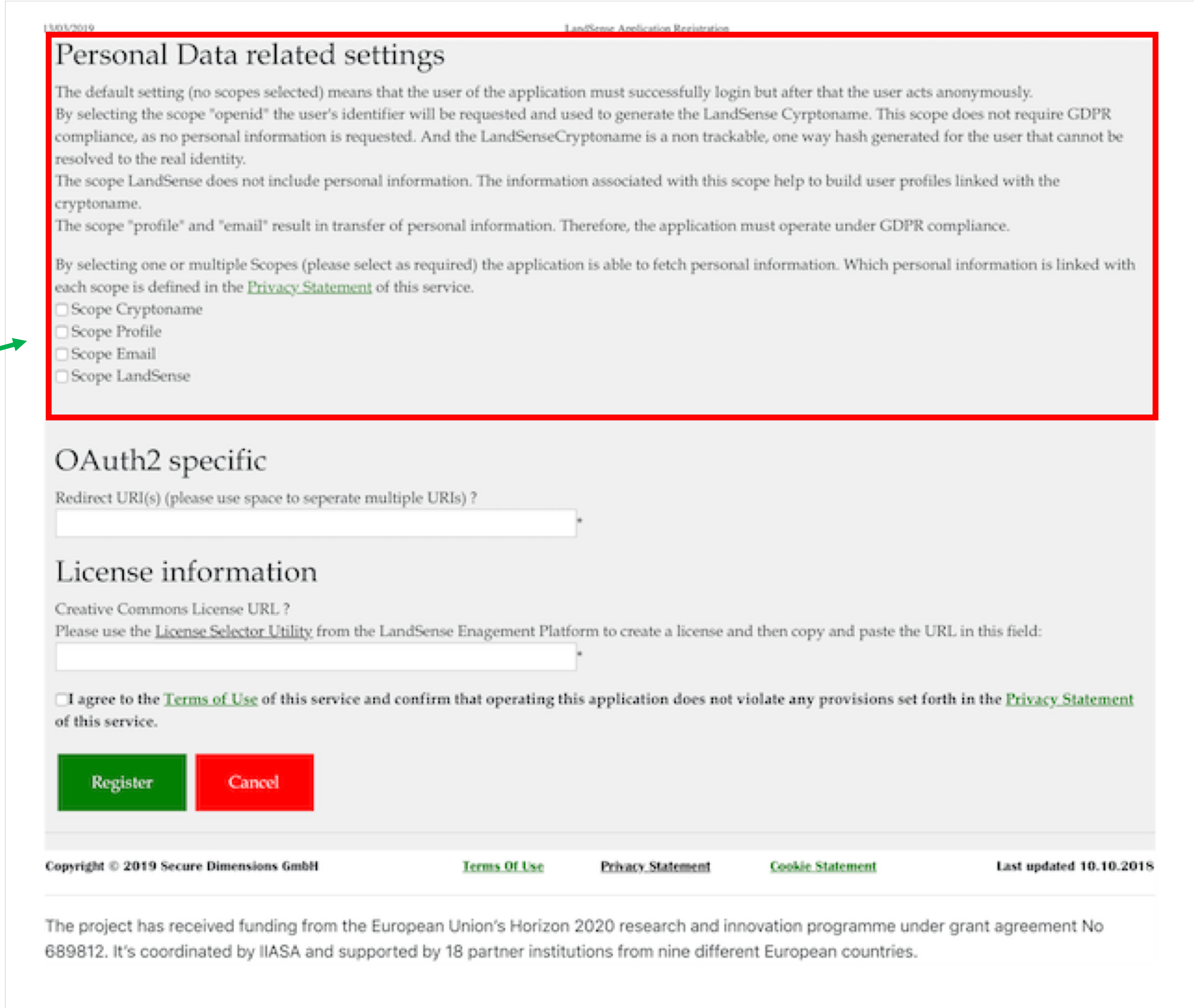
Software Version ? *

Application Name ? *

Application Logo URL ?

Application Terms of Use URL ? *

https://as.landsense.eu/oauth/registerapps 1/2



13/03/2019 LandSense Application Registration

### Personal Data related settings

The default setting (no scopes selected) means that the user of the application must successfully login but after that the user acts anonymously.
By selecting the scope "openid" the user's identifier will be requested and used to generate the LandSense Cyrptoname. This scope does not require GDPR compliance, as no personal information is requested. And the LandSenseCryptoname is a non trackable, one way hash generated for the user that cannot be resolved to the real identity.
The scope LandSense does not include personal information. The information associated with this scope help to build user profiles linked with the cryptoname.
The scope "profile" and "email" result in transfer of personal information. Therefore, the application must operate under GDPR compliance.

By selecting one or multiple Scopes (please select as required) the application is able to fetch personal information. Which personal information is linked with each scope is defined in the Privacy Statement of this service.

☐ Scope Cryptoname
☐ Scope Profile
☐ Scope Email
☐ Scope LandSense

### OAuth2 specific

Redirect URI(s) (please use space to seperate multiple URIs) ? *

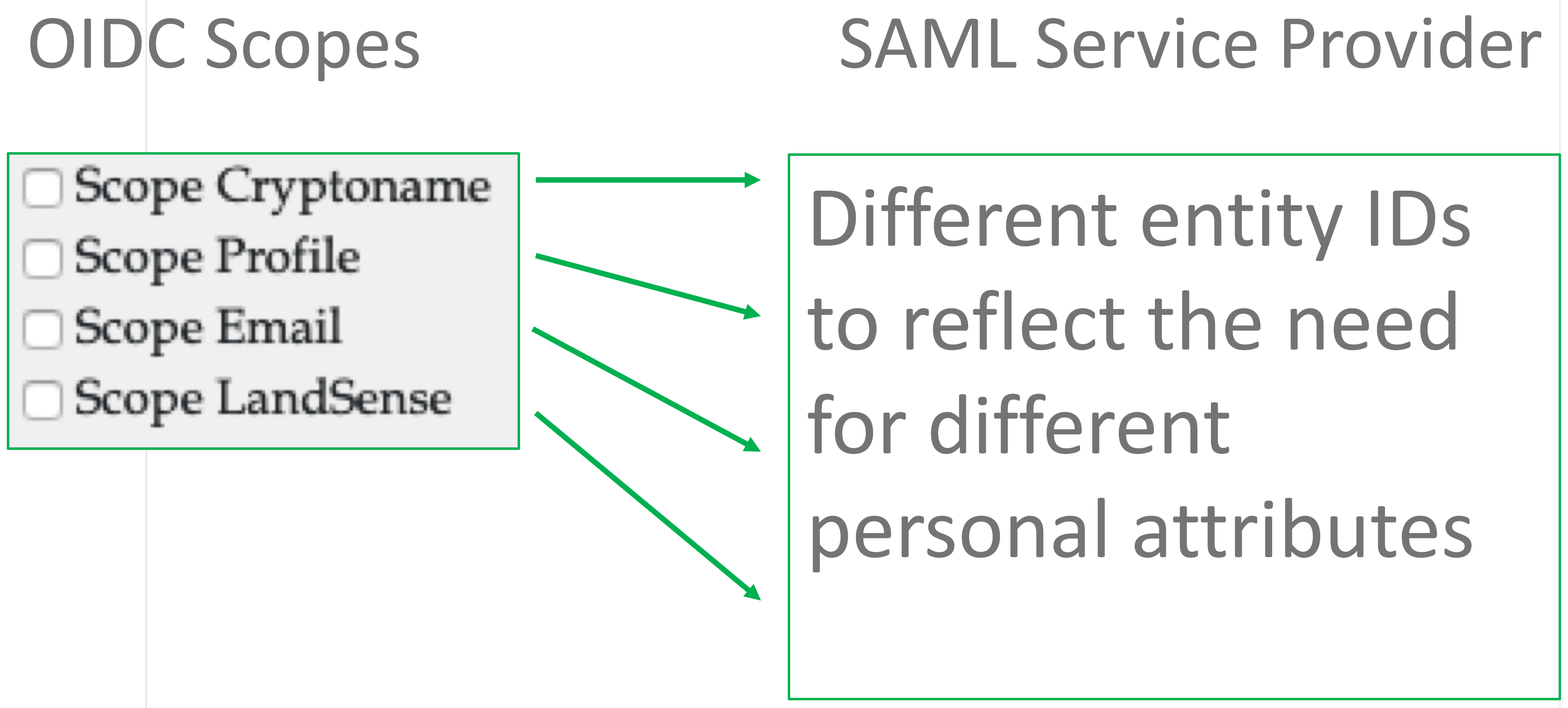
### License information

Creative Commons License URL ?
Please use the License Selector Utility from the LandSense Enagement Platform to create a license and then copy and paste the URL in this field: *

☐ **I agree to the Terms of Use of this service and confirm that operating this application does not violate any provisions set forth in the Privacy Statement of this service.**

**Copyright © 2019 Secure Dimensions GmbH** Terms Of Use Privacy Statement Cookie Statement **Last updated 10.10.2018**

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 689812. It's coordinated by IIASA and supported by 18 partner institutions from nine different European countries.



OIDC Scopes

SAML Service Provider

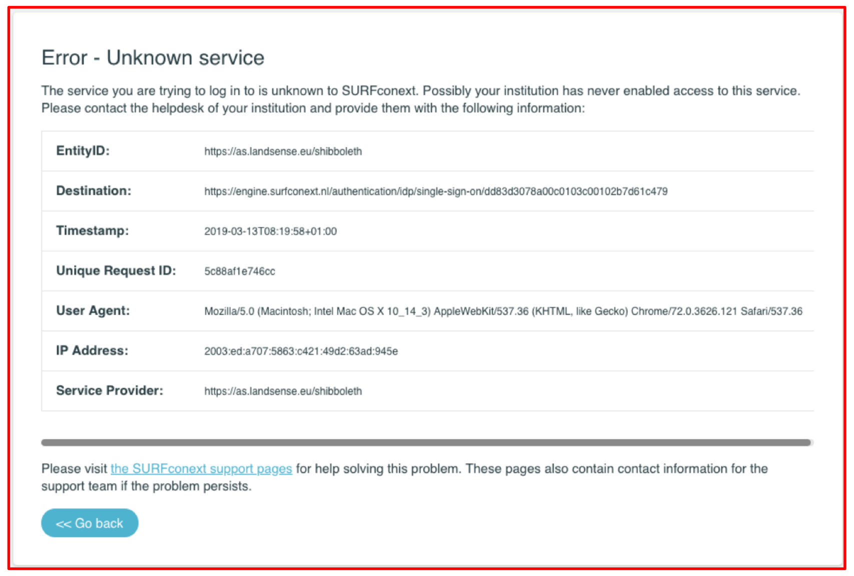
☐ Scope Cryptoname
☐ Scope Profile
☐ Scope Email
☐ Scope LandSense

Different entity IDs to reflect the need for different personal attributes

https://as.landsense.eu/oauth/registerapps 2/2

# LandSense and eduGAIN

- LandSense AS different entityIDs and the SAML Metadata
  - “auth”: no requirements (transient identifier is fine)
  - “crypto”: unique identifier => generated cryptoname
  - “profile”: unique identifier + name, firstname, etc.
  - “email” : unique identifier + email
- Practical results
  - Whether AS receives a unique identifier depends on IdP
  - No eduGAIN IdP seem to release personal data ☹
- IdP from Surfnet produce exception
  They are part of eduGAIN aren‘t they?



Error - Unknown service

The service you are trying to log in to is unknown to SURFconext. Possibly your institution has never enabled access to this service. Please contact the helpdesk of your institution and provide them with the following information:

| | |
|---|---|
| **EntityID:** | https://as.landsense.eu/shibboleth |
| **Destination:** | https://engine.surfconext.nl/authentication/idp/single-sign-on/dd83d3078a00c0103c00102b7d61c479 |
| **Timestamp:** | 2019-03-13T08:19:58+01:00 |
| **Unique Request ID:** | 5c88af1e746cc |
| **User Agent:** | Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36 |
| **IP Address:** | 2003:ed:a707:5863:c421:49d2:63ad:945e |
| **Service Provider:** | https://as.landsense.eu/shibboleth |

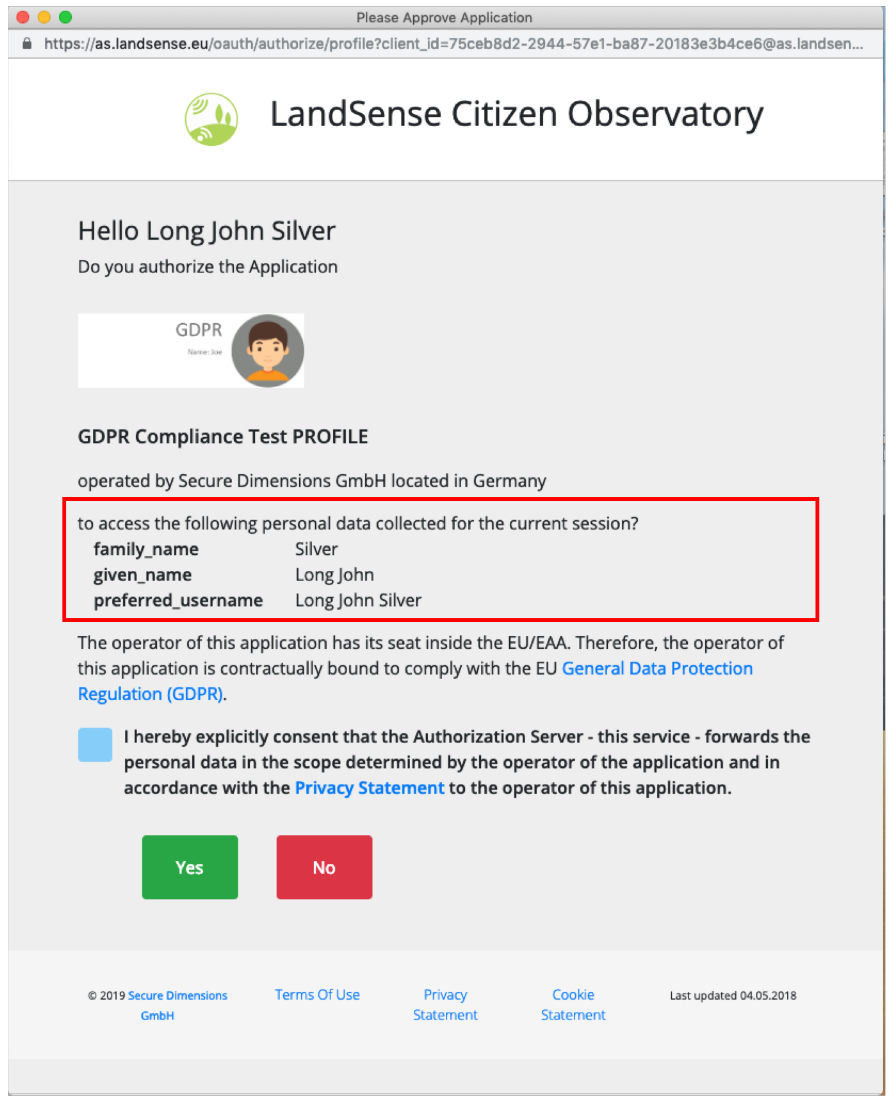
Please visit the SURFconext support pages for help solving this problem. These pages also contain contact information for the support team if the problem persists.

- LandSense operates a “Test” App
  to evaluate the aspects of the GDPR and the compliance
  https://apps.landsense.secure-dimensions.de

# LandSense and GDPR (2/2)

## User is under control

- Before an App can use personal data, the user must agree!
- The AS prevents any App to get more personal data than approved



Please Approve Application

https://as.landsense.eu/oauth/authorize/profile?client_id=75ceb8d2-2944-57e1-ba87-20183e3b4ce6@as.landsen...

LandSense Citizen Observatory

Hello Long John Silver

Do you authorize the Application

**GDPR Compliance Test PROFILE**

operated by Secure Dimensions GmbH located in Germany

to access the following personal data collected for the current session?

| | |
|---|---|
| **family_name** | Silver |
| **given_name** | Long John |
| **preferred_username** | Long John Silver |

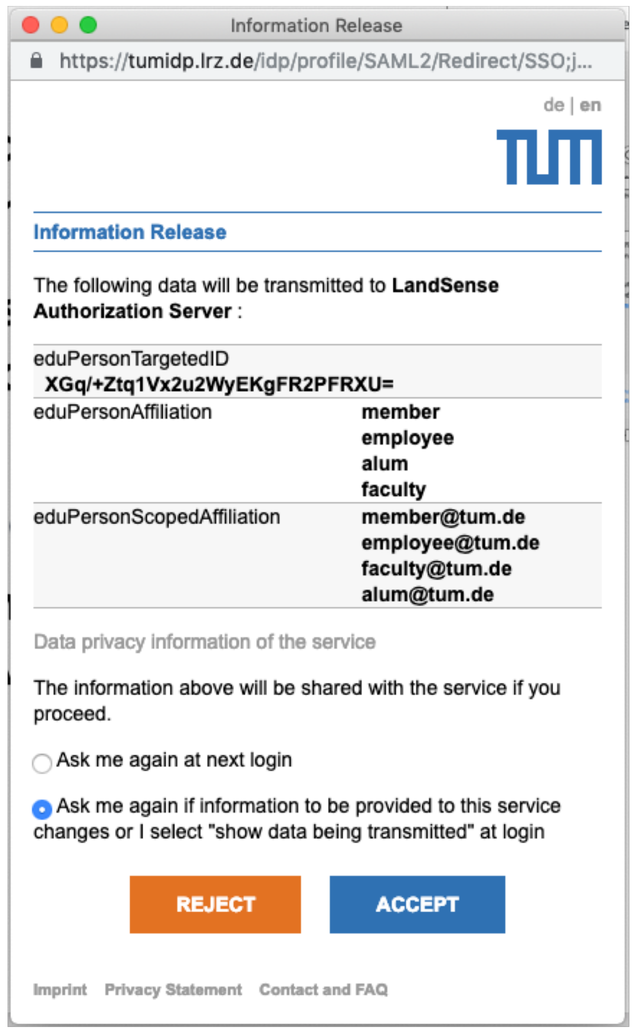
The operator of this application has its seat inside the EU/EAA. Therefore, the operator of this application is contractually bound to comply with the EU General Data Protection Regulation (GDPR).

□ **I hereby explicitly consent that the Authorization Server - this service - forwards the personal data in the scope determined by the operator of the application and in accordance with the Privacy Statement to the operator of this application.**

© 2019 Secure Dimensions GmbH Terms Of Use Privacy Statement Cookie Statement Last updated 04.05.2018

## Personal Data from eduGAIN

- AS uses different SAML SP entities depending on App level
- IdP asks user to approve release of *non* personal data – why?
- Why can this approval request not contain personal attributes?



Information Release

https://tumidp.lrz.de/idp/profile/SAML2/Redirect/SSO;j...

**Information Release**

The following data will be transmitted to **LandSense Authorization Server** :

| | |
|---|---|
| eduPersonTargetedID<br>**XGq/+Ztq1Vx2u2WyEKgFR2PFRXU=** | |
| eduPersonAffiliation | **member**<br>**employee**<br>**alum**<br>**faculty** |
| eduPersonScopedAffiliation | **member@tum.de**<br>**employee@tum.de**<br>**faculty@tum.de**<br>**alum@tum.de** |

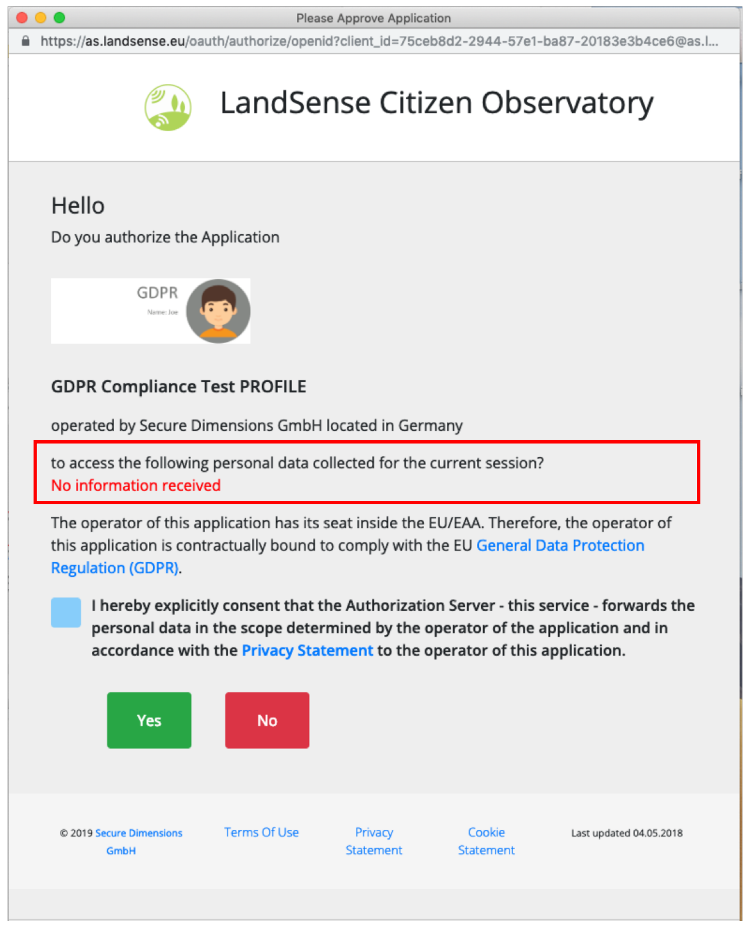
Data privacy information of the service

The information above will be shared with the service if you proceed.

○ Ask me again at next login

● Ask me again if information to be provided to this service changes or I select "show data being transmitted" at login

Imprint Privacy Statement Contact and FAQ



Please Approve Application

https://as.landsense.eu/oauth/authorize/openid?client_id=75ceb8d2-2944-57e1-ba87-20183e3b4ce6@as.l...

LandSense Citizen Observatory

Hello

Do you authorize the Application

**GDPR Compliance Test PROFILE**

operated by Secure Dimensions GmbH located in Germany

to access the following personal data collected for the current session?

No information received

The operator of this application has its seat inside the EU/EAA. Therefore, the operator of this application is contractually bound to comply with the EU General Data Protection Regulation (GDPR).

□ **I hereby explicitly consent that the Authorization Server - this service - forwards the personal data in the scope determined by the operator of the application and in accordance with the Privacy Statement to the operator of this application.**

© 2019 Secure Dimensions GmbH Terms Of Use Privacy Statement Cookie Statement Last updated 04.05.2018

# Conclusions and Issues

- eduGAIN Federation provides great opportunity to connect Citizen Science and Science!
- LandSense proofs that GDPR compliant brokering of personal data from the SAML into the OpenID Connect world is possible – which is very important to operate modern Mobile- and Web-Apps!
- BUT … eduGAIN Federation lacks of guarantee to be useful!
  - Release of a unique user attribute is *always* required
  - Release of personal attributes – based on user consent – is required without writing letters to all 2857 entities
- LandSense and Citizen Science is only one example where the eduGAIN community could collaborate to strengthen the quality of research. The LandSense approach could be a model for anothers!

# LandSense

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

Dr. 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