LandSense

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

Deliverable 3.9

LandSense Citizen Observatory user guidelines and training material

This project has received funding from the European Union's
Horizon 2020 research and innovation programme
under grant agreement No.689812

Project acronym:	**LandSense**
Project title:	**A Citizen Observatory and Innovation Marketplace for Land Use and Land Cover Monitoring**
Project number:	**689812**
Instrument:	**Horizon 2020**
Call identifier:	**SC5-17-2015**
Topic	**Demonstrating the concept of citizen observatories**
Type of action	**Innovation action**

Start date of project:	**01-09-2016**
Duration:	**52 months**

Deliverable number	**D3.9**
Deliverable title	**LandSense Citizen Observatory user guidelines and training material**
Deliverable due date	**31-10-2020**
Lead beneficiary	**Sinergise**
Work package	**WP3: build: LandSense infrastructure, tools and services**
Deliverable type	**Report**
Submission date: **Revision:**	**5-2-2021** **Version 1.0**

Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Title:
LandSense Citizen Observatory user guidelines and training material
Author/Organization:
Matej Batič/Sinergise
Contributor/Organization:
Andreas Matheus/Secure Dimensions

Short Description:
This deliverable outlines the publicly available components of the LandSense platform and provides users with guidelines and instructional how-tos. A subsection is dedicated to dealing with GDPR issues, and – together with the online demonstration application – gives contributors a clear insight into what (personal) data is shared with an application (and between them) based on different scopes. Overall, the deliverable serves as a compendium of LandSense applications, tools and services, and answers questions where to find them and how to use them.
Keywords:
quality assurance, quality control, services, API, documentation, demonstration, infrastructure

History:				
Version	Author(s)	Status	Comment	Date
0.1	Matej Batič	Draft	First draft	1/2/2021
0.3	Matej Batič	Draft	Updated version with section 5	3/2/2021
1.0	Matej Batič	Submitted version	Finalization of deliverable	5/2/2021

Review:			
Version	Reviewer	Comment	Date
0.1	Inian Moorthy	Review content, figures and tables	2/2/2021
0.3	Inian Moorthy	Review content, approved for submission	4/2/2021

Table of Contents

List of Figures

List of Tables

List of Acronyms

API	Application Programming Interface
AS	Authorization Server
BFAST	Breaks For Additive Season and Trend
EO	Earth Observation
GIS	Geographic Information System
GDPR	General Data Protection Regulation
LEP	LandSense Engagement Platform
LULC	Land Use / Land Cover
NDVI	normalized density vegetation index
QA	Quality Assurance
REST	REpresentational State Transfer
URL	Uniform Resource Locator

Executive summary

LandSense has implemented various tools, applications and services to promote the implementation of citizen science/crowdsourcing campaigns, assessing the quality of citizen observations and other associated tasks in the domain of land use and land cover monitoring. Some of the tools were provided by consortium partners, and will be continued afterwards independently of LandSense, some will be sustained by other European (or other) projects, and a few have been open sourced for broad accessibility.

The deliverable summarizes these tools and applications and provides users with guidelines and training material on how to use them. All of the tools are accessible through LandSense Engagement Platform (LEP, https://landsense.eu), mostly through "Campaigns" and "Innovate" sections.

A large part of the deliverable is dedicated to the LandSense Authorization service, which glues the federation of these tools and services together and provides a General Data Protection Regulation (GDPR) compliant framework for citizen science data collection. The online demonstration application, available on the LEP, gives contributors a clear insight into what (personal) data is shared with an application (and between them) based on different scopes. The pillar services change detection and quality assurance (QA) and control services, are presented together with instructions on how to use them or install and run your own (in case of QA service). Finally, a quick overview of the (LandSense) applications and partners' tools that will continue after the end of the project is indicated to make this deliverable a compendium of LandSense applications, tools and services.

1 Introduction

The document guides the reader throughout the LandSense federation from the perspective of how it can be used and exploited. The LandSense Engagement Platform (LEP) outlined in Figure 1 brings together solutions that contribute to the transfer, assessment, valuation, uptake and exploitation of citizens' contributions, Land Use/Land Cover (LULC) data and related results of the LandSense project and is accessible on https://landsense.eu. Some of the services come with their own demonstration (web) application, available on LEP, as well as published documentation, mostly suitable for developers. This deliverable either adds the missing pieces, or reports on where the user and developer guidelines, tutorials and how-tos are available. The deliverable should thus be viewed as a compendium of various training/development guidelines (and a directory of where to find them).

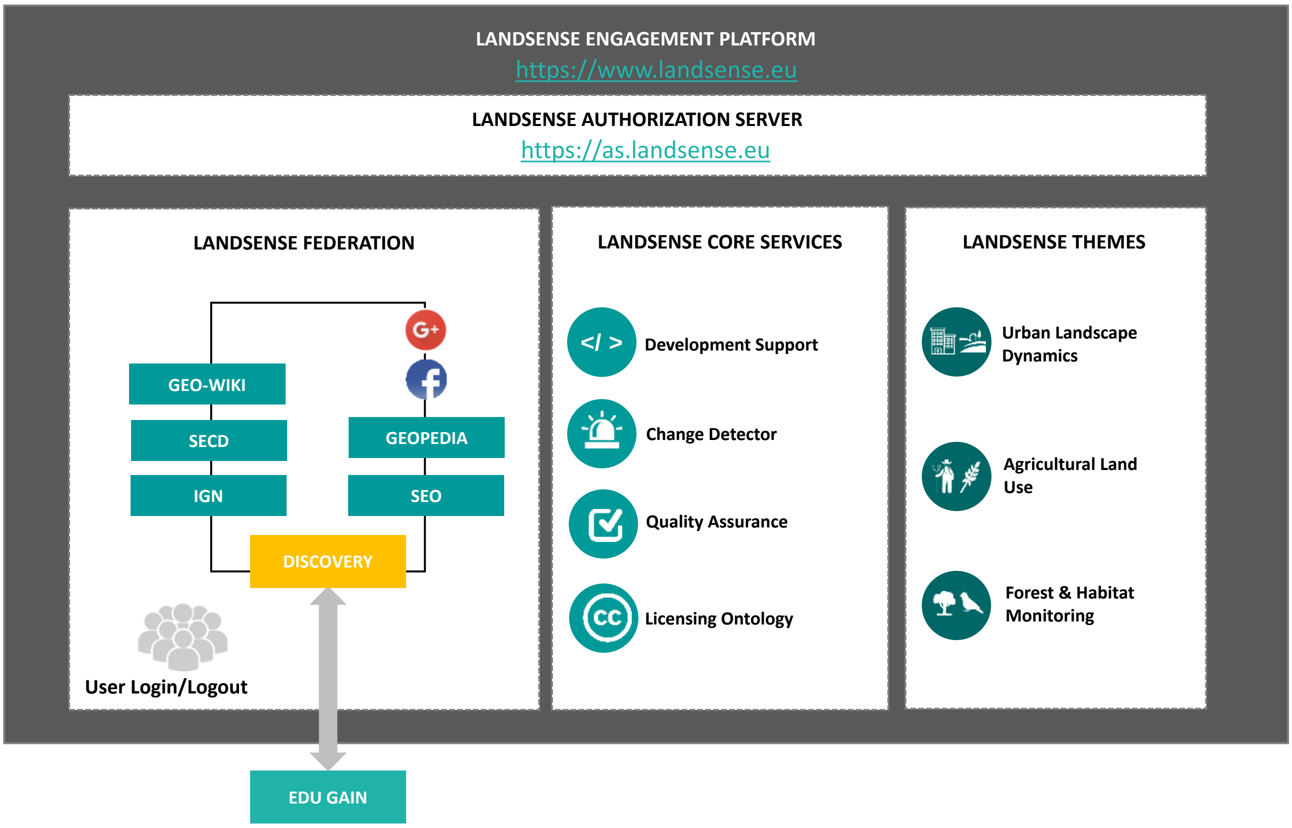


Figure 1: Building blocks of the LandSense Engagement Platform

The LEP is constructed by bringing together and extending various key pieces of technology like: Geo-Wiki, LACO-Wiki, Geopedia, a number of mobile applications and novel services. It provides the technical and legal basis to demonstrate the LandSense objectives to tackle different environmental monitoring issues:

- The **Urban Landscape Dynamics** theme focuses on engaging citizens via mobile applications to discover land change in urban and peri-urban areas. Pilot cases were implemented in Amsterdam, Toulouse, Vienna and Heidelberg to engage citizens in monitoring their local environment.
- The **Agriculture Land Use** theme focuses on leveraging the power of Earth Observation (EO) systems and advanced crowdsourcing techniques to deliver value added services to European farmers and public authorities in the agricultural sector. Demonstration cases are run in Serbia.
- The **Forest & Habitat Monitoring** theme triggers volunteer networks for in-situ data collection to help monitor protected areas within BirdLife International Important Bird and Biodiversity Areas and Key Biodiversity Areas through networks in Spain and Indonesia.

The LandSense Authorization Server (AS) is the underlying part of the LEP that acts as a broker of user authentication and personal information between the Identity Providers of the LandSense Federation and the operators of registered applications and services. The description of AS, guidelines for usage, and GDPR compliance considerations are described in Section 2. The LandSense Incremental Login demonstrator application described therein is particularly useful for general public to understand and familiarize with how LandSense handled (personal) data sharing.

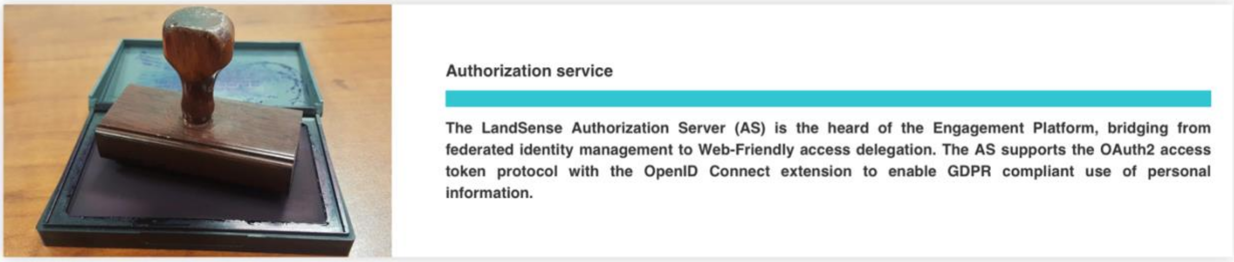
Furthermore, the LandSense team developed several tools and services within the federation. The services include EO data-based Change Detection (CD) and Quality Assurance (QA) and Control of citizen-collected datasets. Section 3 gives a short overview of the **Change Detection (CD)** Services, split into three different services focusing on three different topics. The guidelines to the CD services and demonstration applications are also given in Section 3. Note that some of the services were used within LandSense for a particular use-case and are now offered by a specific LandSense partner. In such cases this deliverable provides information on the particular service and how to get in contact with service providers.

The **Quality Assurance (QA)** Services are described in Section 4. The section provides guidelines how to set up the (open-sourced) QA Service on one's own infrastructure, describes the tests available through service and shows the demonstrator applications for some of the tests, available on LEP. Finally, the section provides information on which QA tests were used on publicly available datasets, collected throughout LandSense.

In Section 5 we provide reader with links to different applications created during LandSense project for the purposes of data collection within various campaigns and use-cases, and tools and services that partners provided and were used within LandSense.

2 LandSense Engagement Platform

LandSense Engagement Platform (LEP) is a directory of EO-based solutions that contribute to the transfer, assessment, valuation, uptake and exploitation of LULC data and related results. It is an important part of the LandSense Citizen Observatory and allows citizens to view, analyze and share data collected from different campaigns. This is achieved by bringing together and extending various key pieces of technology including Geo-Wiki, LACO-Wiki, Geopedia, Sentinel Hub and the EODC, joined together in the LandSense Federation. In addition, the LEP exposes various services that are useful to developers and innovators dealing with citizen science and LULC. The platform is accessible to anyone, but some features are only available to logged-in users. To facilitate the uptake of the platform, login is possible using several social media accounts, LandSense partners' accounts and academic institutions participating in eduGAIN. This section reports on the underlying basis of the federation: the LandSense Authorization Server, https://as.landsense.eu.



Authorization service

The LandSense Authorization Server (AS) is the heard of the Engagement Platform, bridging from federated identity management to Web-Friendly access delegation. The AS supports the OAuth2 access token protocol with the OpenID Connect extension to enable GDPR compliant use of personal information.

Figure 2: Authorization Service detail on LEP (https://landsense.eu/Project/LEP)

2.1 LandSense Authorization Server

The LandSense Authorization Server (AS) is one of the key services of the LEP which allows users to login from a variety of supported login providers. Upon a successful login, the AS receives a set of information, released by the login provider. This can vary from no personal information up to the privacy policy applicable to the acting application. Each application that wants to leverage the authentication provided by the AS must have been registered previously. With the registration, the application developer (or the operator) selects one of the available privacy policies. In case personal data is required by the application, a privacy statement must be bundled with the registration. The privacy statement explains the GDPR compliance of the application and in particular outlines the need and purpose for the personal information.

When the application is used, the amount of personal information becoming available to the application is controlled (limited) by the applicable privacy policy. In case the application was registered with a privacy policy that enables the flow of personal information, the personal information will only be forwarded by the AS once the user has given consent. When asked for consent, the user can review the privacy statement with registering the application. The user can visit the "me" pages of the AS to withdraw the consent (untrust the application) at any time.

Using the AS is a two-step approach:

1. an application developer (or operator) must register the application or service
2. the registered application / service can be used by individual users to authenticate.

2.2 Review of GDPR compliance and related functional requirements

Any application or service that consumes, processes and stores personal information operated within the EEA must be compliant to the GDPR issued by the European Parliament. The functional requirements can be derived from the GDPR publication. From the legal text of the GDPR, functional requirements can be derived that must be implemented in the AS. The following is list of principles and functional requirements to implement:

- **Transparency**: The entire processing of personal information must be transparent to the user. The user has further the right to either be informed about the processing or must be given an easy way to review which personal information was collected, stored and processed. For the case of the AS, the user must also be able to see which personal information was made available to a registered application. These functions are implemented under the "me" pages.
- **Opt-in consent**: When a registered application is started by a user for the first time, and that application requests personal information from the AS, the user is required to give consent; otherwise, the AS does not release personal information to the application. Once the consent was given, the user can go to "me" pages of the AS to revoke the trust to that application. After the revoke, the application does not receive personal information any longer until the user gives consent again.
- **User is always under control**: The user can stop the release of personal information any time by undertaking a logout from the application. Depending on the architecture of the application, the AS "me" pages may show a simple "logout" (for Web-Applications) and a "logout from device" for Mobile-Applications.
- **Right to be forgotten**: The AS has two categories of users: Developers or operators that register applications and people that use the registered applications. A developer must provide personal information when registering an application. This personal information will get deleted once the registered application is deleted. For users of registered applications, they can delete their personal data that is active for the current session via a logout. The historical log of processed personal information will be deleted automatically after 90 days.
- **Minimization**: A developer of operator of an application must choose one of the supported policies. Depending on the selected policy, the AS will not provide any personal information to the applications, provide a unique identifier that cannot be used to resolve personal information, or provide personal information according to the OpenID Connect scopes 'profile' and 'email'. Note: The scopes 'address' and 'phone number' are currently not implemented.

- **Secure storage**: All personal information available for a session and the historical processing log are stored encrypted in a database. The encryption of the session data is based on a secret system key whereas the processing history is encrypted with individual cipher keys per user.

In addition to the direct GDPR related requirements, the AS does not track users. No analytics are included, and no other tracking functionality is implemented.

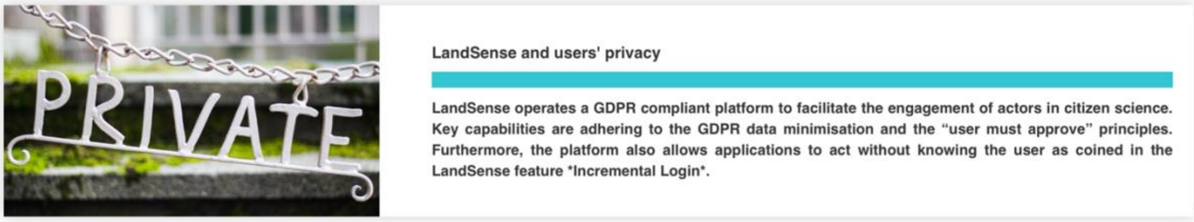
2.2.1 Verifying the GDPR Minimization Requirement

For any truly GDPR compliant implementation, it is important to request, store and process only the minimum set of personal information as it is required to fulfill its functionality. The minimization requirement is implemented in the AS via different Personal Information (PI) release policies, described in Table 1.

Table 1: Personal information release policies

Personal Information release policies		
Icon	**Privacy policy name**	**Description**
Authenticated (✓)	Anonymous policy	The AS executes the OAuth2 flow which does not include personal information. It is therefore not possible for an application to receive personal information; neither via an "id_token" nor via the "UserInfo" endpoint.
Cryptoname 56c4d986-b1d4-11e8-96f8-529269fb1459	ID policy	The AS executes the OpenID Connect flow but only return the user's identifier to the application. This identifier is named "sub" in the OpenID Connect community standard.
GDPR Name: Joe Email: joe@123.xyz	PI policy	The AS executes the OpenID Connect flow and does return that personal information to the application which matches the PI scope. The supported PI scopes and which personal information is returned in forms of claims is specified in the OpenID Connect community standard. Currently implemented in the AS are the scopes 'profile' and 'email'.

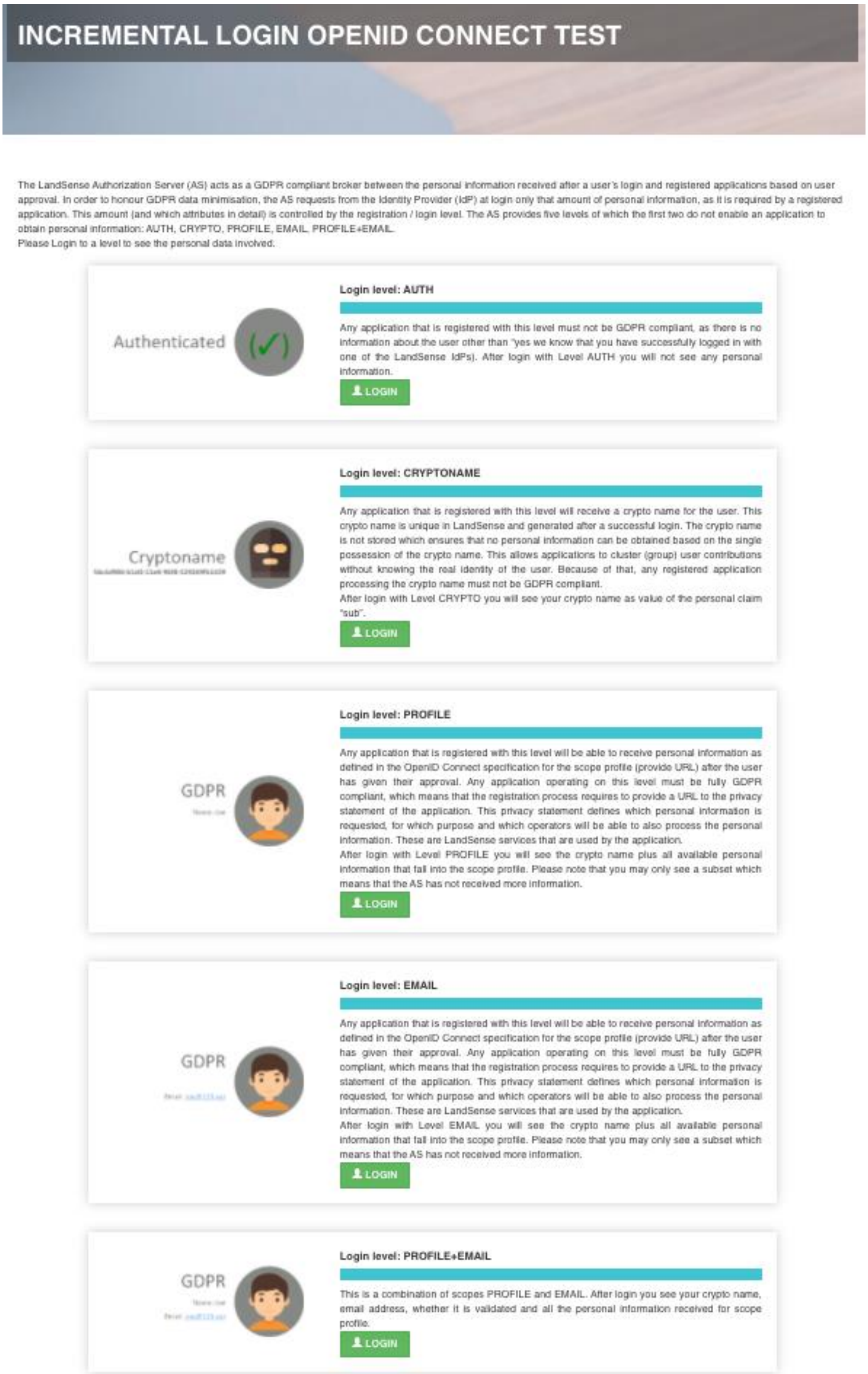
The LandSense Incremental Login Test verifies these fundamental requirements and gives users concrete insight into data that is shared through different PI policies. From a technical perspective, the Incremental Login Test consists of different applications that are registered with different privacy policies. Each application Login Level is based on another application. This can be verified under the AS "Operators" page.



LandSense and users' privacy

LandSense operates a GDPR compliant platform to facilitate the engagement of actors in citizen science. Key capabilities are adhering to the GDPR data minimisation and the "user must approve" principles. Furthermore, the platform also allows applications to act without knowing the user as coined in the LandSense feature "Incremental Login".

Figure 3: Incremental Login demo detail on LEP (https://landsense.eu/Project/IncrementalLogin)



INCREMENTAL LOGIN OPENID CONNECT TEST

The LandSense Authorization Server (AS) acts as a GDPR compliant broker between the personal information received after a user's login and registered applications based on user approval. In order to honour GDPR data minimisation, the AS requests from the Identity Provider (IdP) at login only that amount of personal information, as it is required by a registered application. This amount (and which attributes in detail) is controlled by the registration / login level. The AS provides five levels of which the first two do not enable an application to obtain personal information: AUTH, CRYPTO, PROFILE, EMAIL, PROFILE+EMAIL.
Please Login to a level to see the personal data involved.

Login level: AUTH

Any application that is registered with this level must not be GDPR compliant, as there is no information about the user other than "yes we know that you have successfully logged in with one of the LandSense IdPs). After login with Level AUTH you will not see any personal information.

Login level: CRYPTONAME

Any application that is registered with this level will receive a crypto name for the user. This crypto name is unique in LandSense and generated after a successful login. The crypto name is not stored which ensures that no personal information can be obtained based on the single possession of the crypto name. This allows applications to cluster (group) user contributions without knowing the real identity of the user. Because of that, any registered application processing the crypto name must not be GDPR compliant.
After login with Level CRYPTO you will see your crypto name as value of the personal claim "sub".

Login level: PROFILE

Any application that is registered with this level will be able to receive personal information as defined in the OpenID Connect specification for the scope profile (provide URL) after the user has given their approval. Any application operating on this level must be fully GDPR compliant, which means that the registration process requires to provide a URL to the privacy statement of the application. This privacy statement defines which personal information is requested, for which purpose and which operators will be able to also process the personal information. These are LandSense services that are used by the application.
After login with Level PROFILE you will see the crypto name plus all available personal information that fall into the scope profile. Please note that you may only see a subset which means that the AS has not received more information.

Login level: EMAIL

Any application that is registered with this level will be able to receive personal information as defined in the OpenID Connect specification for the scope profile (provide URL) after the user has given their approval. Any application operating on this level must be fully GDPR compliant, which means that the registration process requires to provide a URL to the privacy statement of the application. This privacy statement defines which personal information is requested, for which purpose and which operators will be able to also process the personal information. These are LandSense services that are used by the application.
After login with Level EMAIL you will see the crypto name plus all available personal information that fall into the scope profile. Please note that you may only see a subset which means that the AS has not received more information.

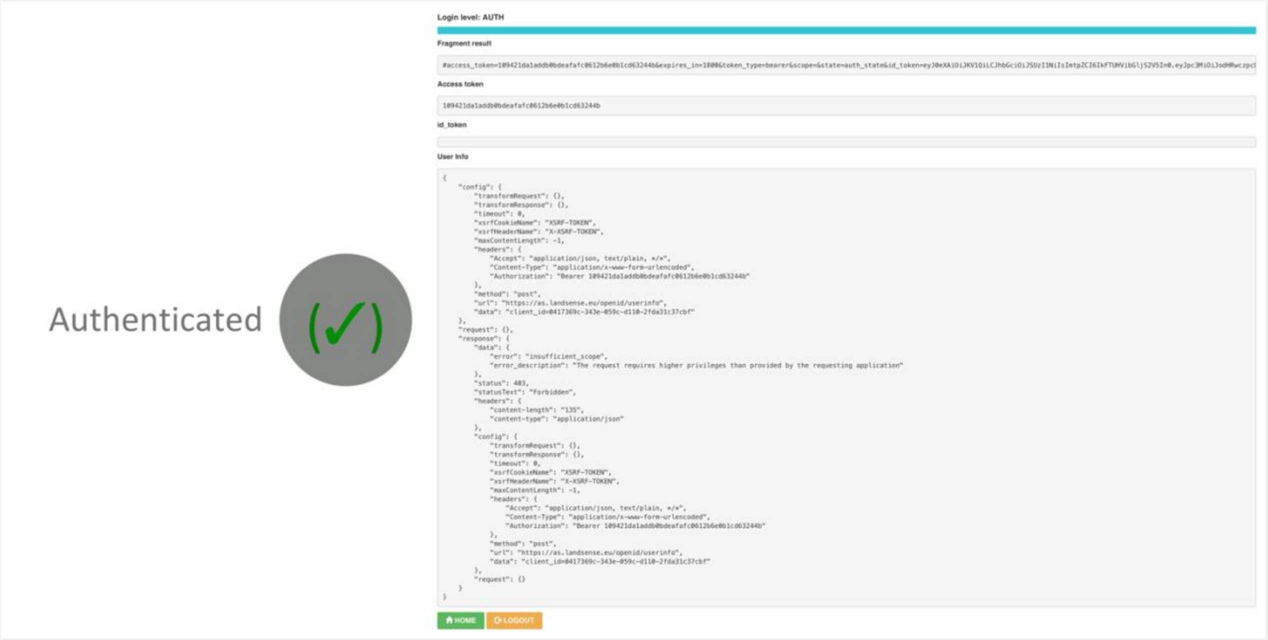
Login level: PROFILE+EMAIL

This is a combination of scopes PROFILE and EMAIL. After login you see your crypto name, email address, whether it is validated and all the personal information received for scope profile.

Figure 4: LandSense Incremental Login Demo

When following an application via the LOGIN button, the application will request a login and then display the result concerning access token and personal information.

As illustrated in Figure 5, the application does not receive personal information; neither via an id_token nor via the UserInfo endpoint. Instead, a HTTP status code 403 (FORBIDDEN) is returned to the applications when trying to fetch personal information via the UserInfo endpoint.



Authenticated

Login level: AUTH

Fragment result

```
#access_token=109421da1addb0bdeafafc0612b6e0b1cd63244b&expires_in=1800&token_type=bearer&scope=&state=auth_state&id_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IkFTUHVibGljS2V5In0.eyJpc3MiOiJodHRwczpc
```

Access token

```
109421da1addb0bdeafafc0612b6e0b1cd63244b
```

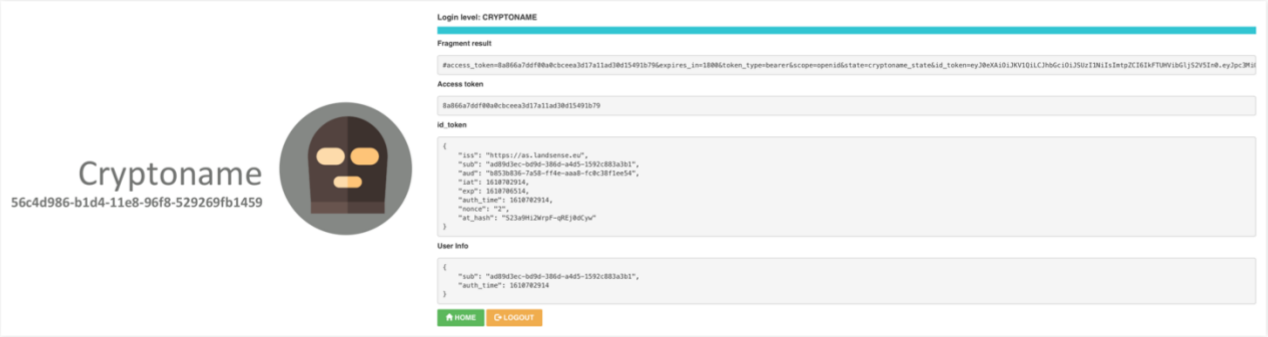
id_token

User Info

```
{
    "config": {
        "transformRequest": {},
        "transformResponse": {},
        "timeout": 0,
        "xsrfCookieName": "XSRF-TOKEN",
        "xsrfHeaderName": "X-XSRF-TOKEN",
        "maxContentLength": -1,
        "headers": {
            "Accept": "application/json, text/plain, */*",
            "Content-Type": "application/x-www-form-urlencoded",
            "Authorization": "Bearer 109421da1addb0bdeafafc0612b6e0b1cd63244b"
        },
        "method": "post",
        "url": "https://as.landsense.eu/openid/userinfo",
        "data": "client_id=0417369c-343e-059c-d110-2fda31c37cbf"
    },
    "request": {},
    "response": {
        "data": {
            "error": "insufficient_scope",
            "error_description": "The request requires higher privileges than provided by the requesting application"
        },
        "status": 403,
        "statusText": "Forbidden",
        "headers": {
            "content-length": "135",
            "content-type": "application/json"
        },
        "config": {
            "transformRequest": {},
            "transformResponse": {},
            "timeout": 0,
            "xsrfCookieName": "XSRF-TOKEN",
            "xsrfHeaderName": "X-XSRF-TOKEN",
            "maxContentLength": -1,
            "headers": {
                "Accept": "application/json, text/plain, */*",
                "Content-Type": "application/x-www-form-urlencoded",
                "Authorization": "Bearer 109421da1addb0bdeafafc0612b6e0b1cd63244b"
            },
            "method": "post",
            "url": "https://as.landsense.eu/openid/userinfo",
            "data": "client_id=0417369c-343e-059c-d110-2fda31c37cbf"
        },
        "request": {}
    }
}
```

Figure 5: Application registered with AUTH Policy

Figure 6 illustrates that the application only receives the user's unique identifier but not personal information. As the user's identifier is a crypto ID (name) that is not stored at the AS, it cannot be used to resolve personal information. The UserInfo endpoint releases a "sub", which is unique to this user, but cannot be resolved back to them.



Cryptoname
56c4d986-b1d4-11e8-96f8-529269fb1459

Login level: CRYPTONAME

Fragment result

```
#access_token=8a866a7ddf00a0cbceea3d17a11ad30d15491b79&expires_in=1800&token_type=bearer&scope=openid&state=cryptoname_state&id_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IkFTUHVibGljS2V5In0.eyJpc3Mi
```

Access token

```
8a866a7ddf00a0cbceea3d17a11ad30d15491b79
```

id_token

```
{
    "iss": "https://as.landsense.eu",
    "sub": "ad89d3ec-bd9d-386d-a4d5-1592c883a3b1",
    "aud": "b853b836-7a58-ff4e-aaa8-fc0c38f1ee54",
    "iat": 1610702914,
    "exp": 1610706514,
    "auth_time": 1610702914,
    "nonce": "2",
    "at_hash": "S23a9Hi2WrpF-qREj0dCyw"
}
```

User Info

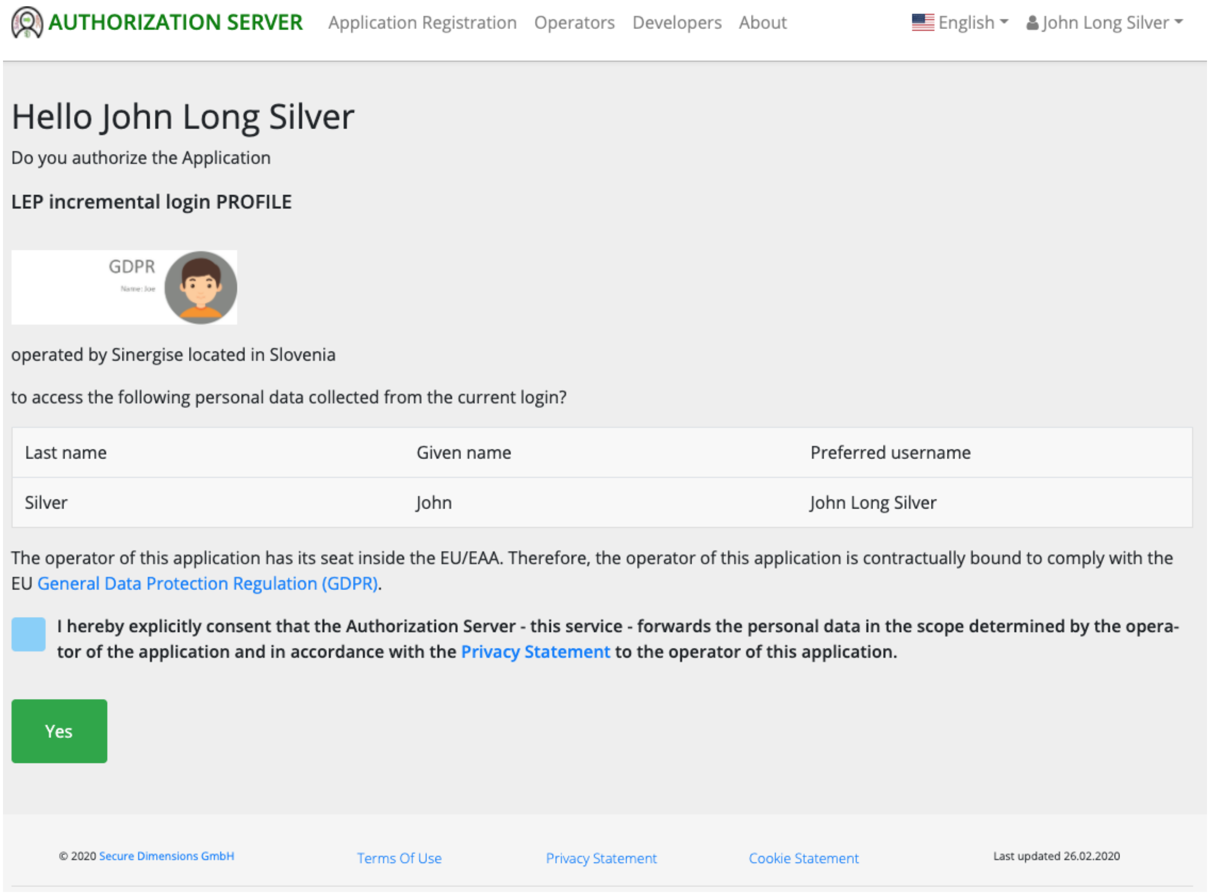
```
{
    "sub": "ad89d3ec-bd9d-386d-a4d5-1592c883a3b1",
    "auth_time": 1610702914
}
```

Figure 6: Application registered with ID Policy

Figures below illustrate that each application receives personal information as they are registered via the PI Policy. To demonstrate the data minimization principle, each application only receives

i. PI Policy – Scope 'profile' (Figure 7 and Figure 8) information
ii. PI Policy – Scope 'email' (Figure 9 and Figure 10) information
iii. PI Policy – Scope 'email+profile' (Figure 11 and Figure 12) information.

For each of the applications registered with the PI Profile, the user must (at first use) approve that the personal information is provided to the applications.



Hello John Long Silver

Do you authorize the Application

LEP incremental login PROFILE

operated by Sinergise located in Slovenia

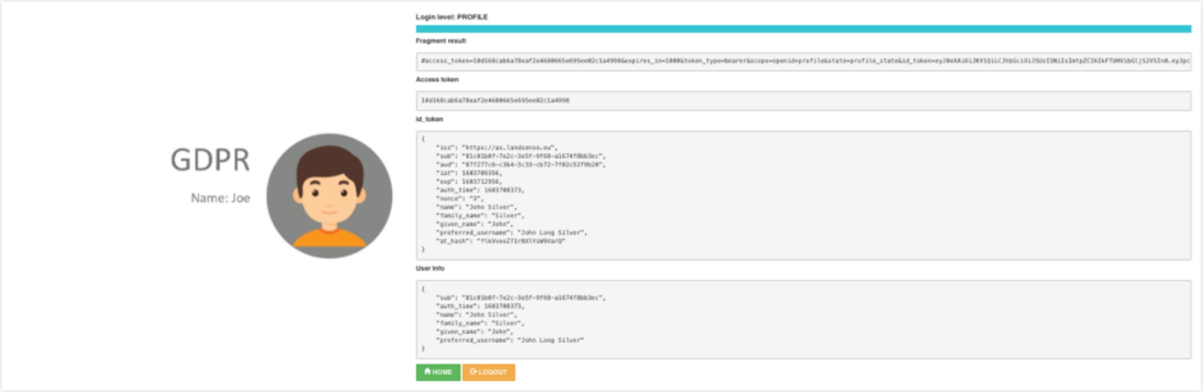
to access the following personal data collected from the current login?

Last name	Given name	Preferred username
Silver	John	John Long 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.

Figure 7: AS asking user to approve release of listed personal information to the application



Login level: PROFILE

Fragment result

```
#access_token=10d168cab6a78eaf2e4680665e695ee02c1a4998&expires_in=1800&token_type=bearer&scope=openid+profile&state=profile_state&id_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6IkFTUHV1bGljS2V5In0.eyJpc
```

Access token

```
10d168cab6a78eaf2e4680665e695ee02c1a4998
```

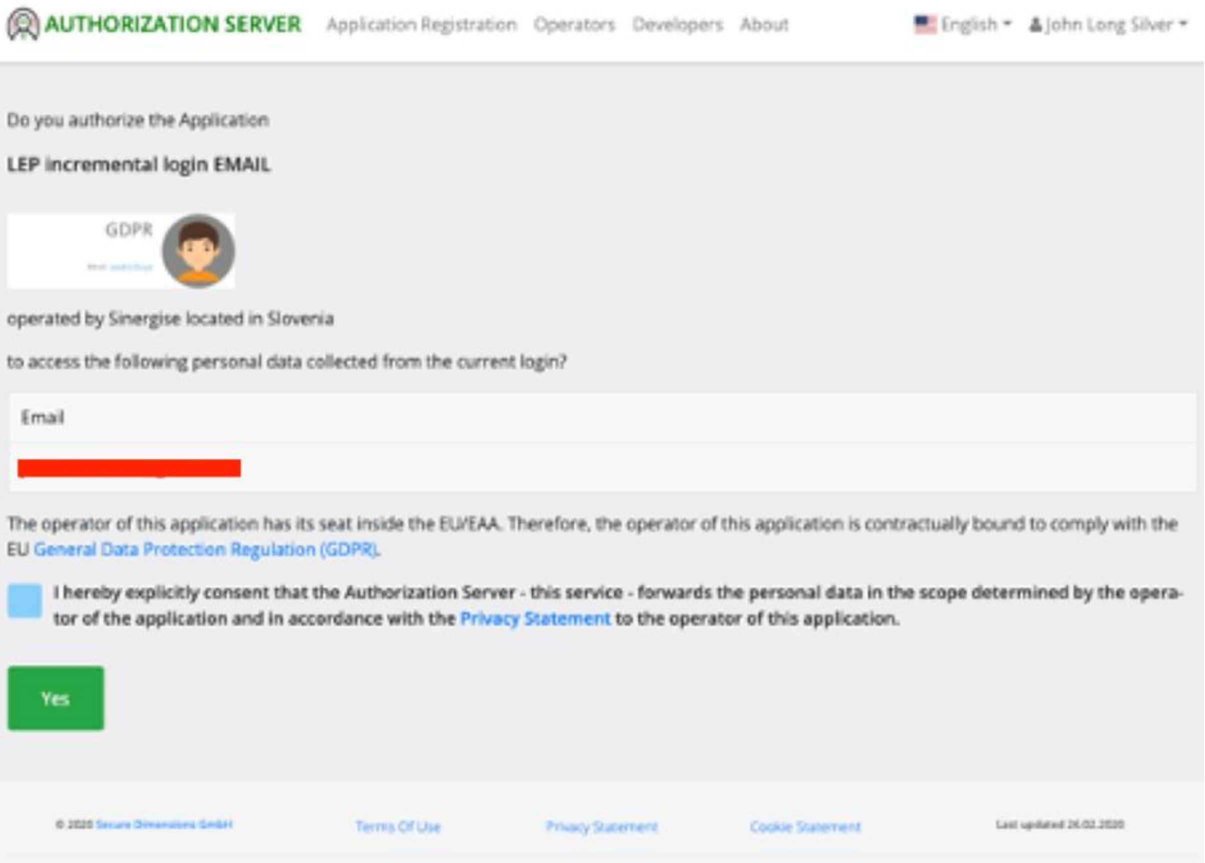
id_token

```
{
    "iss": "https://as.landsense.eu",
    "sub": "81c01b0f-7e2c-3e5f-9f68-a1674f8bb3ec",
    "aud": "87f277c6-c3b4-3c33-cb72-7f02c52f9b20",
    "iat": 1603709356,
    "exp": 1603712956,
    "auth_time": 1603708373,
    "nonce": "3",
    "name": "John Silver",
    "family_name": "Silver",
    "given_name": "John",
    "preferred_username": "John Long Silver",
    "at_hash": "fikVveeZ71rBXlYsW9VarQ"
}
```

User Info

```
{
    "sub": "81c01b0f-7e2c-3e5f-9f68-a1674f8bb3ec",
    "auth_time": 1603708373,
    "name": "John Silver",
    "family_name": "Silver",
    "given_name": "John",
    "preferred_username": "John Long Silver"
}
```

Figure 8: Application has received exactly the authorized information



Do you authorize the Application

LEP incremental login EMAIL

operated by Sinergise located in Slovenia

to access the following personal data collected from the current login?

Email

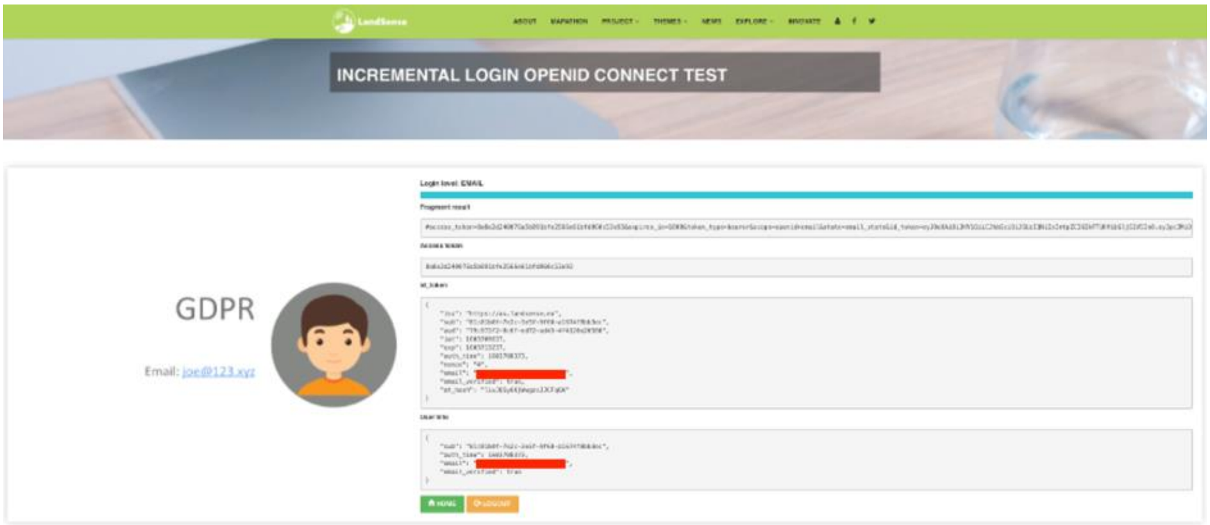
[redacted]

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.**

© 2020 Secure Dimensions GmbH Terms Of Use Privacy Statement Cookie Statement Last updated 26.02.2020

Figure 9: AS asking user to approve release of listed personal information to the application



INCREMENTAL LOGIN OPENID CONNECT TEST

GDPR

Email: joe@123.xyz

Login level: EMAIL

Fragment result

```
#access_token=[illegible]&expires_in=[illegible]&token_type=bearer&scope=openid+email&state=email_state&id_token=[illegible]
```

Access token

```
[illegible]
```

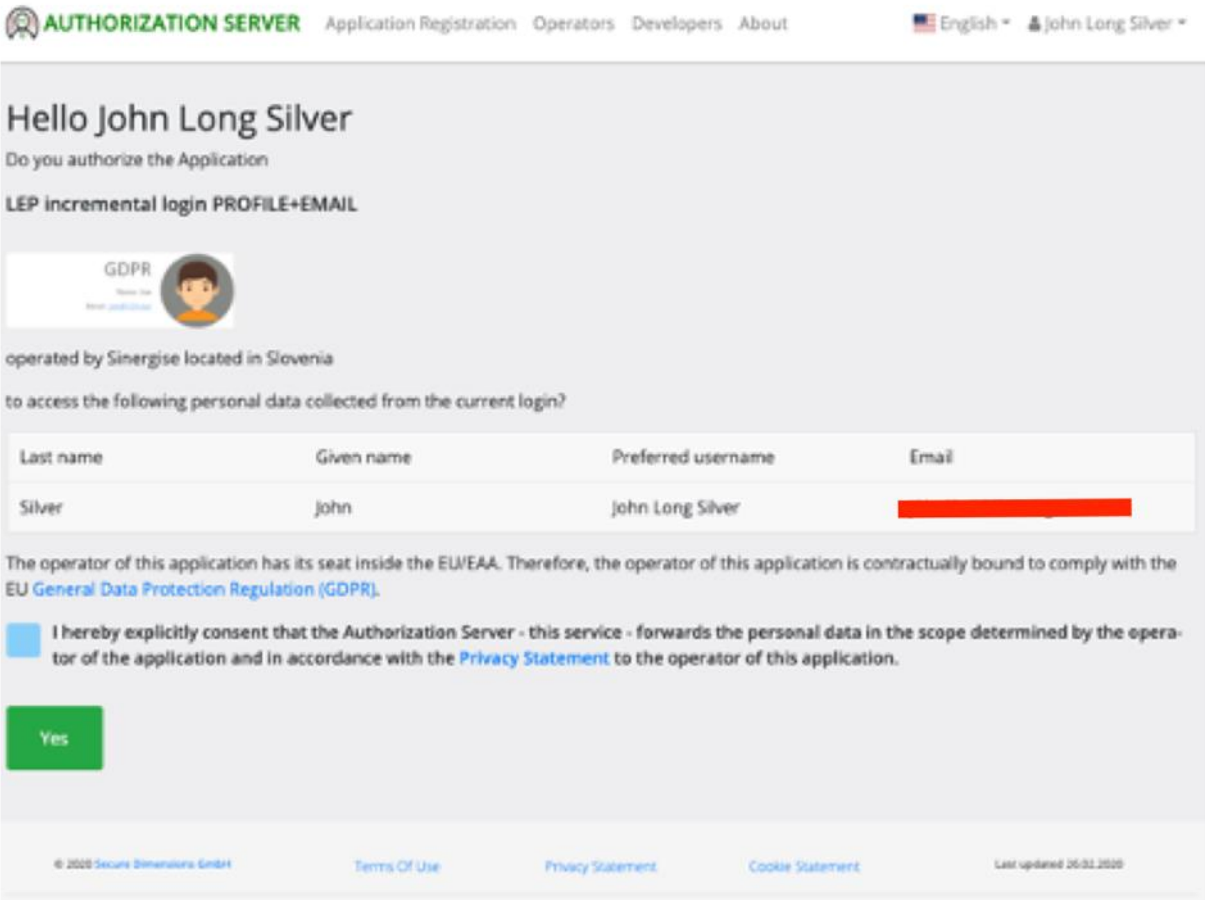
id_token

```
{
    "iss": "https://as.landsense.eu",
    "sub": [illegible],
    "aud": [illegible],
    "iat": [illegible],
    "exp": [illegible],
    "auth_time": [illegible],
    "nonce": [illegible],
    "email": "[redacted]",
    "email_verified": true,
    "at_hash": [illegible]
}
```

User Info

```
{
    "sub": [illegible],
    "auth_time": [illegible],
    "email": "[redacted]",
    "email_verified": true
}
```

Figure 10: Application has received exactly the authorized information



Hello John Long Silver

Do you authorize the Application

LEP incremental login PROFILE+EMAIL

operated by Sinergise located in Slovenia

to access the following personal data collected from the current login?

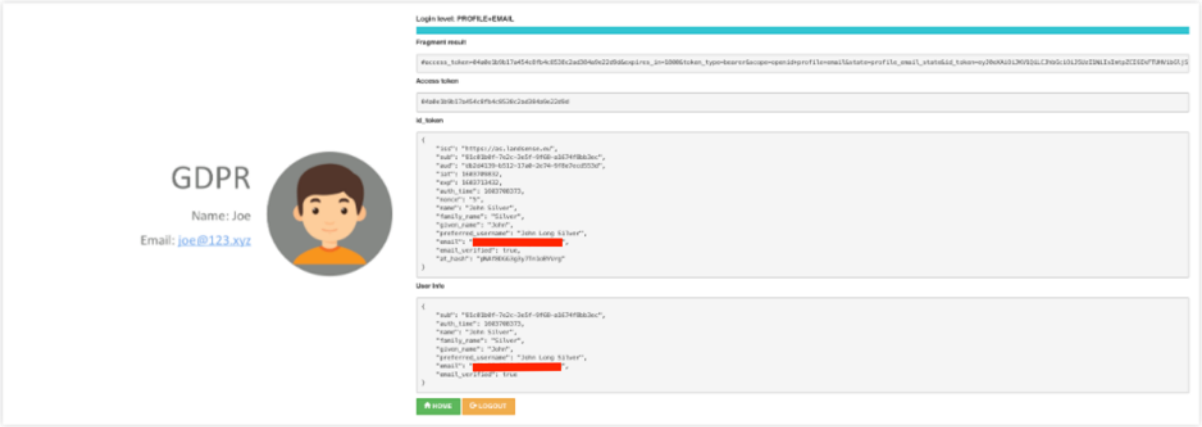
Last name	Given name	Preferred username	Email
Silver	John	John Long Silver	[redacted]

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.**

© 2020 Secure Dimensions GmbH   Terms Of Use   Privacy Statement   Cookie Statement   Last updated 26.02.2020

Figure 11: AS asking user to approve release of listed personal information to the application



Login level: PROFILE+EMAIL

Fragment result

```
#access_token=04a0e3b9b17a454c0fb4c0536c2ad304a0e22d9d&expires_in=18000&token_type=bearer&scope=openid+profile+email&state=profile_email_state&id_token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Ik[illegible]
```

Access token

```
04a0e3b9b17a454c0fb4c0536c2ad304a0e22d9d
```

id_token

```
{
    "iss": "https://as.landsense.eu/",
    "sub": "61c03b0f-7e2c-3e5f-9f60-a1674f8bb3ec",
    "aud": "db2d4139-b512-17a0-2c74-9f8e7ecd553d",
    "iat": 1683709832,
    "exp": 1683713432,
    "auth_time": 1683708373,
    "nonce": "5",
    "name": "John Silver",
    "family_name": "Silver",
    "given_name": "John",
    "preferred_username": "John Long Silver",
    "email": "[redacted]",
    "email_verified": true,
    "at_hash": "[illegible]"
}
```

User Info

```
{
    "sub": "61c03b0f-7e2c-3e5f-9f60-a1674f8bb3ec",
    "auth_time": 1683708373,
    "name": "John Silver",
    "family_name": "Silver",
    "given_name": "John",
    "preferred_username": "John Long Silver",
    "email": "[redacted]",
    "email_verified": true
}
```

Figure 12: Application has received exactly the authorized information

A logout sends a command to the AS to expire all access tokens and issues a logout to the IdP used for login. This can be triggered via the LOGOUT button. In case the no logout is executed, another application will receive personal information based on the active login session.

2.3 Authorization Server – developer guidelines

The AS can be used for authentication in almost all types of applications that are based on the following OAuth2 flows:

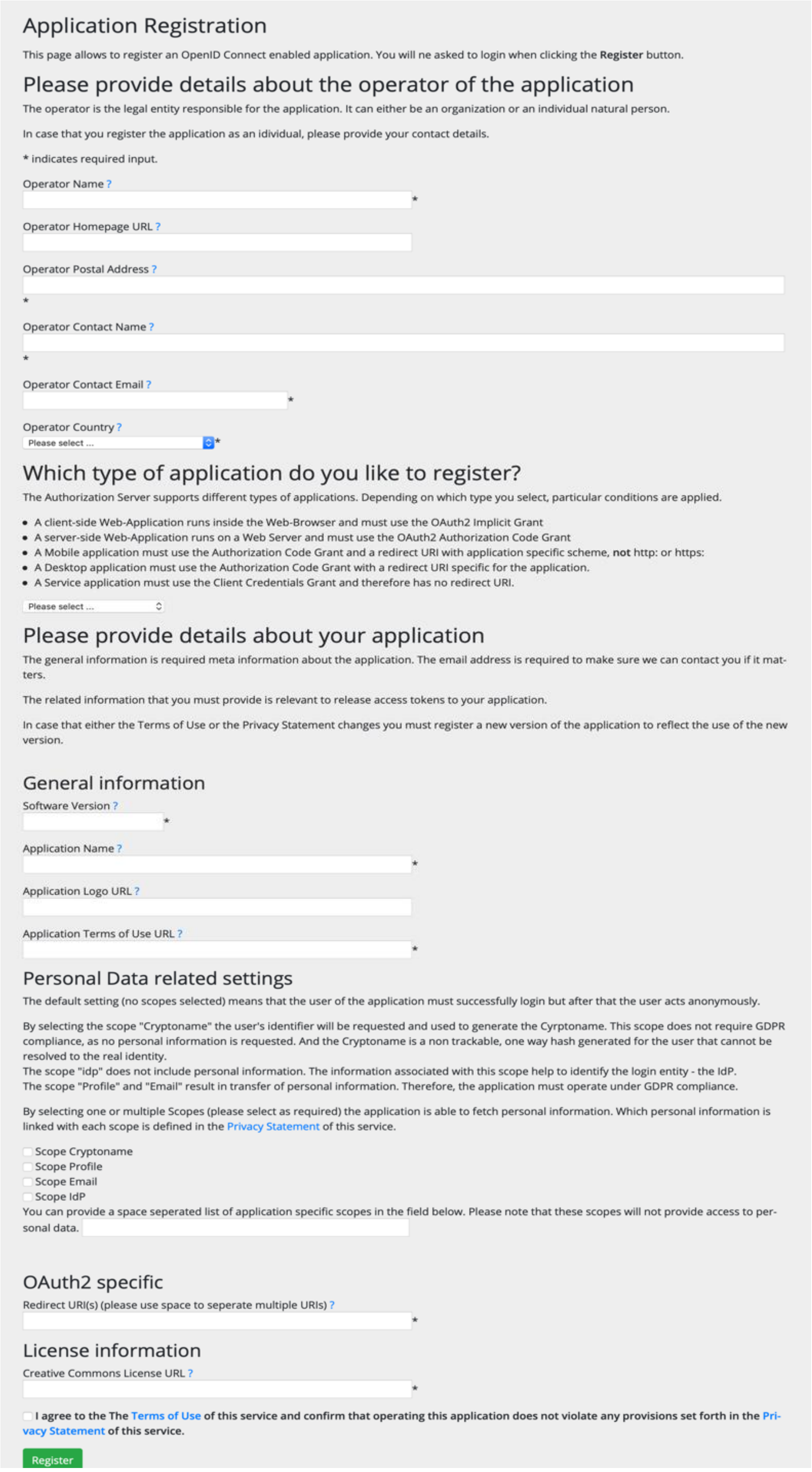
- **Implicit:** Web-Browser based applications that undertake user authentication via JavaScript
- **Authorization Code:**
    - Web-Server based applications that undertake user authentication on the server
    - Mobile applications that leverage a Web-Browser for authentication or a Web-View

It is important to note that the AS does not support the Resource Owner Profile. Without going into details, this flow is not suitable to be implemented with federated login as supported by the AS.

Before an application can leverage the AS for authentication, the application must get registered. The AS supports manual and dynamic client registration based on RFC 7591.

2.3.1 Manual application registration

The manual registration is supported via a HTML form, where the developer or operator of the application must fill in the required (and optional) information. Registration of the application is shown in Figure 13. The user that registers an application must select a policy that reflects the ability regarding retrieval of personal information. The diagram in Figure 14 illustrates the core activities of manual application registration and focuses in particular on the actions, relevant to GDPR.



Application Registration

This page allows to register an OpenID Connect enabled application. You will ne asked to login when clicking the **Register** button.

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 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 with a redirect URI specific for the application.
- A Service application must use the Client Credentials Grant and therefore has no redirect URI.

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 ? *

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 "Cryptoname" the user's identifier will be requested and used to generate the Cyrptoname. This scope does not require GDPR compliance, as no personal information is requested. And the Cryptoname is a non trackable, one way hash generated for the user that cannot be resolved to the real identity.
The scope "idp" does not include personal information. The information associated with this scope help to identify the login entity - the IdP.
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 IdP
You can provide a space seperated list of application specific scopes in the field below. Please note that these scopes will not provide access to personal data.

OAuth2 specific

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

License information

Creative Commons License URL ? *

□ **I agree to the 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.**

Figure 13: Application registration form

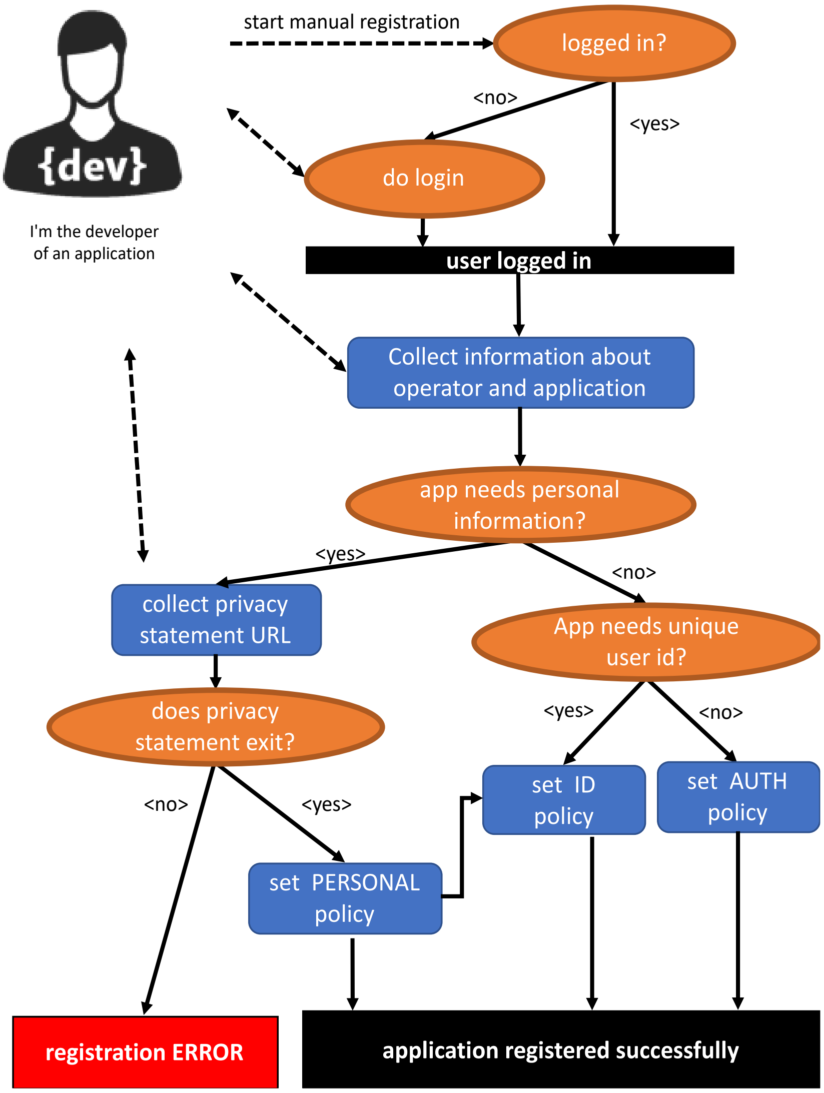
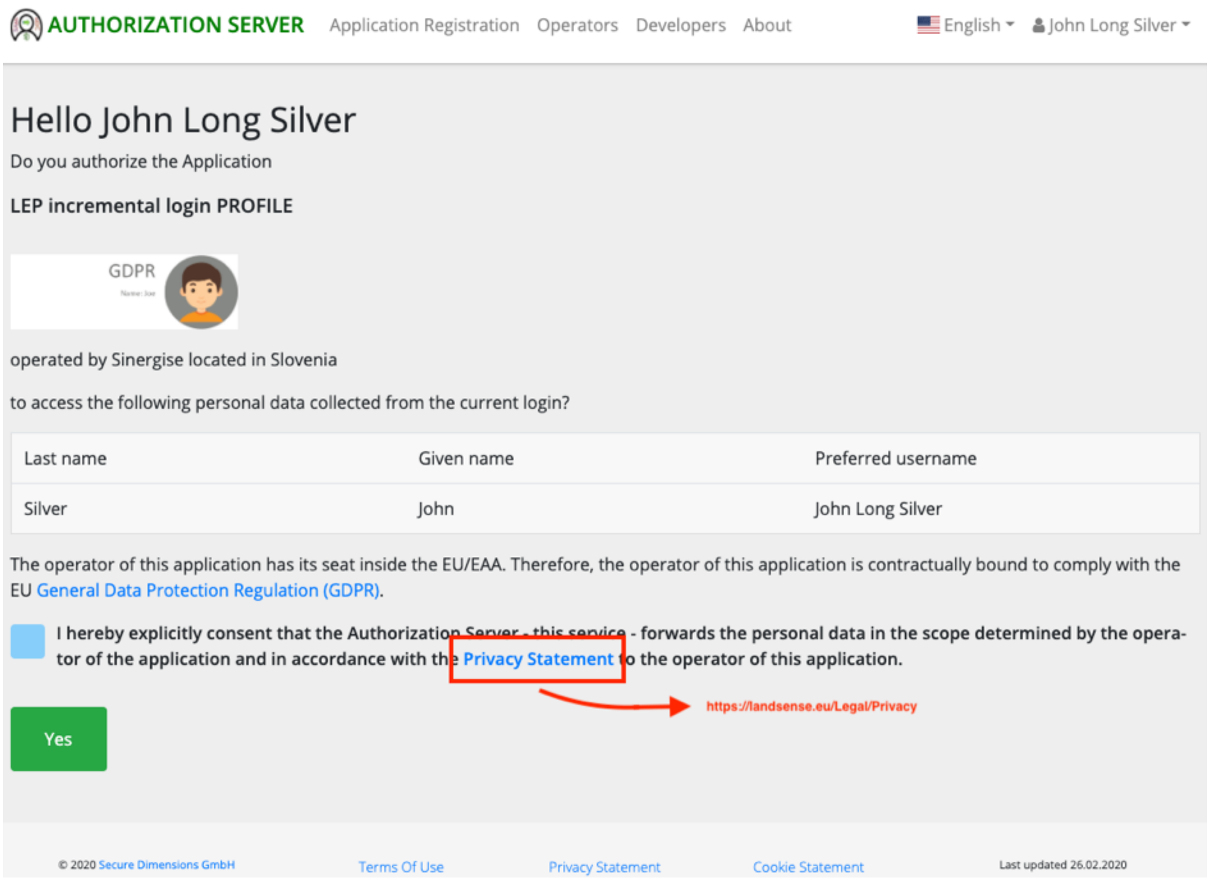

start manual registration
logged in?
<no>
<yes>
{dev}
I'm the developer of an application
do login
user logged in
Collect information about operator and application
app needs personal information?
<yes>
<no>
collect privacy statement URL
App needs unique user id?
does privacy statement exit?
<yes>
<no>
<no>
<yes>
set ID policy
set AUTH policy
set PERSONAL policy
registration ERROR
application registered successfully

Figure 14: Manual registration activity

As illustrated in the Figure 14 above, the person registering the application must determine the appropriate policy regarding personal information. The default is that the AUTH Policy. In case the registering person selects the “profile” or “email” scopes (or both), the PI Policy is used for registration. In that case, a URL to the privacy statement must be provided (Figure 15). The URL for the privacy statement will be checked for existence, but the content is not checked during registration. However, as illustrated in the figures for “Incremental Login Test” (Figure 7, Figure 9 and Figure 11), a user would have the opportunity to follow the provided link to read the privacy statement prior to consent on the personal data release.

For the “Incremental Login Test” for scope profile, the following link is registered with the application: https://landsense.eu/Legal/Privacy.



Hello John Long Silver

Do you authorize the Application

LEP incremental login PROFILE

operated by Sinergise located in Slovenia

to access the following personal data collected from the current login?

Last name	Given name	Preferred username
Silver	John	John Long 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.**

Figure 15: Consent request with link to registered Privacy Statement

2.3.2 Automatic application registration

The developer can also decide to have the application register itself once started by the user. This is useful for native applications (mobile or desktop) where a static (manual) registration is not meaningful. The AS supports automatic registration via an RFC 7591 compliant endpoint. Such an automated registered of the application is anonymous and will expire automatically after 30 days. Any application registered this way cannot leverage the PI Policy.

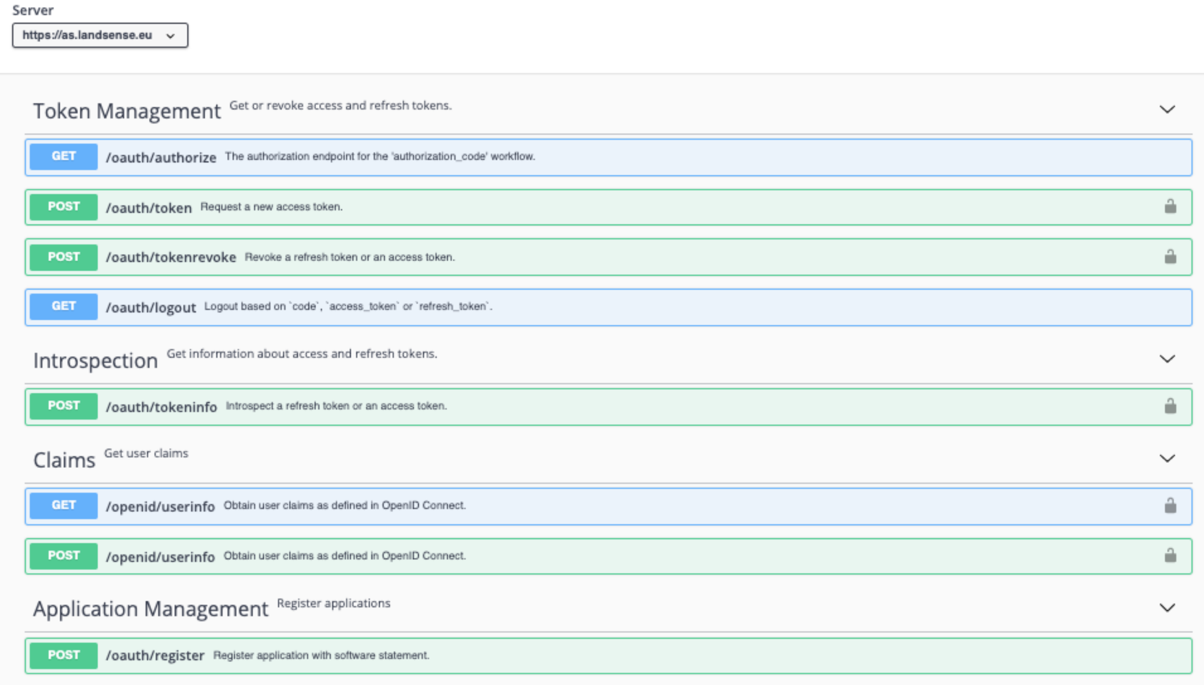
In order to achieve a persistent registration via the RFC7591 endpoint, the application must be registered via a digitally signed software statement describing the application. Such a digitally signed software statement can be requested from the operator of the AS – Secure Dimensions.

Note: A future version of the AS will allow the developer to register a public key so that digitally signed software statements can be verified by the AS automatically. Any application registered via a digitally signed software statement can use the PI Policy, as all application metadata – in particular the URL to the privacy statement – are vouched by the signing party. Also, a future version of the AS will also support to register a personal copy of the application. This requires the user to obtain an access token for the purpose of dynamic client registration. Such a personal copy of an application will not expire and can use the PI Policy.

2.3.3 Using the AS in your application

The integration of the AS into an application allows to leverage the Authentication as a Service. The actual implementation depends on the foreseen architecture. Because the AS provides standardized OAuth2 and OpenID Connect endpoints, the implementation can leverage any standard development kit (SDK). The OpenID Connect website lists different compliant products for various architectures: https://openid.net/developers/certified/

To better understand and eventually test the integration of the AS into an application, the AS endpoints are described via OpenAPI: https://as.landsense.eu/api. The endpoints can be seen in Figure 16.



Server
https://as.landsense.eu

Token Management Get or revoke access and refresh tokens.

GET /oauth/authorize The authorization endpoint for the 'authorization_code' workflow.

POST /oauth/token Request a new access token. 🔒

POST /oauth/tokenrevoke Revoke a refresh token or an access token. 🔒

GET /oauth/logout Logout based on `code`, `access_token` or `refresh_token`.

Introspection Get information about access and refresh tokens.

POST /oauth/tokeninfo Introspect a refresh token or an access token. 🔒

Claims Get user claims

GET /openid/userinfo Obtain user claims as defined in OpenID Connect. 🔒

POST /openid/userinfo Obtain user claims as defined in OpenID Connect. 🔒

Application Management Register applications

POST /oauth/register Register application with software statement.

Figure 16: Authorization service endpoints, described in OpenAPI document at https://as.landsense.eu/api

For leveraging the AS for user login / logout and authentication, existing SDKs can be used. To explore the variety of options, this page provides a great overview: https://openid.net/developers/certified/

To better understand the core options, some examples got created that illustrate the AS integration into different types of applications.

2.3.3.1 Web-Browser (AJAX) based application

An AJAX application is considered a "1-page" application that is loaded when the Web-Browser loads the given URL. For such an application, all functionality exists in JavaScript. Therefore, the following example extends an OpenLayers client with the HelloJS library. The HelloJS library fulfills the integration of the AS. The example is available on GitHub: https://github.com/LandSense/AuthorizationClientDemo

2.3.3.2 Service protection running ASP.NET

A backend service can be protected via access tokens, released by the AS. The following example illustrate the protection via ASP.NET: https://github.com/LandSense/Security

2.3.3.3 Web-Server based application protection via Apache (Httpd) Web Server

Any endpoint hosted on an Apache (Httpd) Web-Server can be protected via the OpenID Connect module provided here: https://github.com/zmartzone/mod_auth_openidc

The following Apache 2.4 configuration example snippet illustrates the approach:

```
LoadModule auth_openidc_module modules/mod_auth_openidc.so

OIDCProviderMetadataURL https://as.landsense.eu/.well-known/openid-configuration
OIDCClientID <your application’s client_id>
OIDCClientSecret <your application’s client_secret>

OIDCRedirectURI <your application’s redirect_uri>
OIDCCryptoPassphrase some_secure_text

OIDCScope "openid profile offline_access"
OIDCResponseType "code id_token"
OIDCResponseMode query
OIDCClaimPrefix landsense-
OIDCPKCEMethod S256
OIDCCookieSameSite On

<Location ~ "/secure">
  AuthType openid-connect
  Require valid-user
</Location>
```

2.4 The user's perspective

From a user's perspective, an application that integrates the AS for authentication interacts with the user to

i. fulfill login and
ii. request user's consent prior to releasing personal information (for the first time).

The Figure 17 illustrates the activities from a user's perspective, focusing on the interactions related to the processing of personal information.

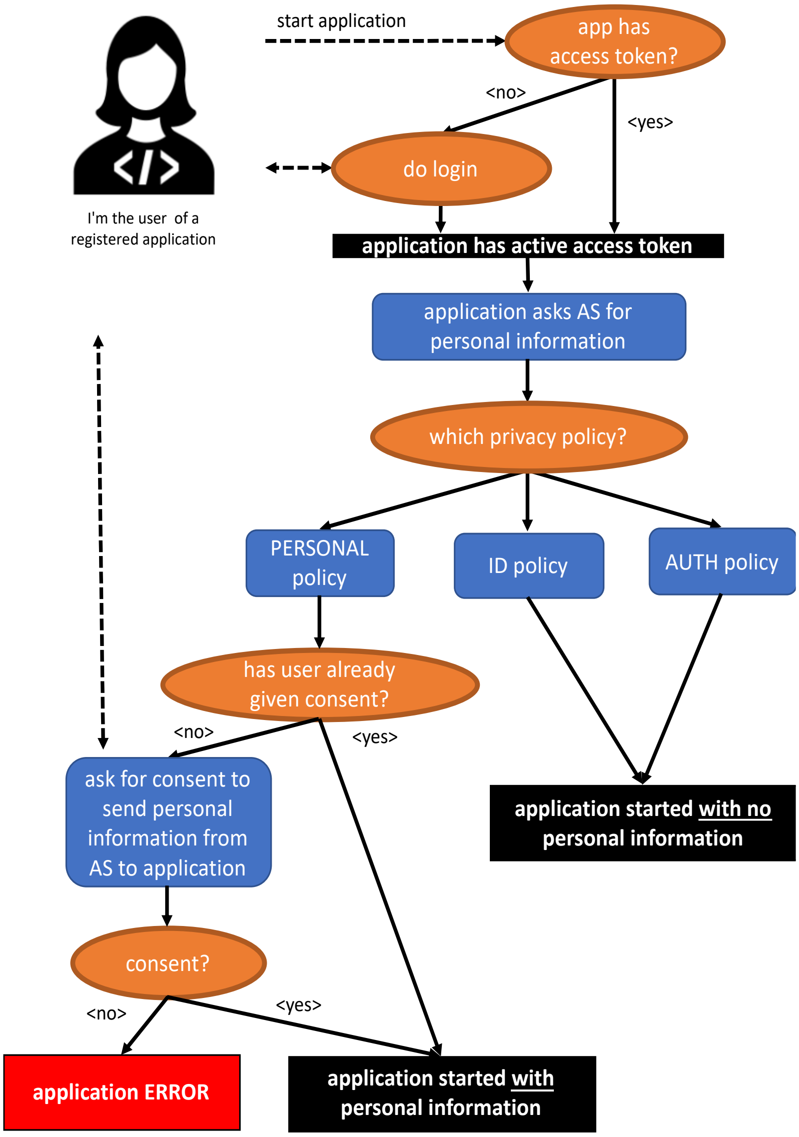

start application
app has access token?
<no>
<yes>
do login
I'm the user of a registered application
application has active access token
application asks AS for personal information
which privacy policy?
PERSONAL policy
ID policy
AUTH policy
has user already given consent?
<no>
<yes>
ask for consent to send personal information from AS to application
application started with no personal information
consent?
<no>
<yes>
application ERROR
application started with personal information

Figure 17: Activity flow for a user to start an application that integrates the AS

3 LandSense Change Detection services

The LandSense EO-based CD services consist of several services, split by topics:

- Subsection 3.1 presents the CD service used for agriculture,
- Subsection 3.2 CD service for urban areas and
- Subsection 3.3 presents the CD service for monitoring forest areas.

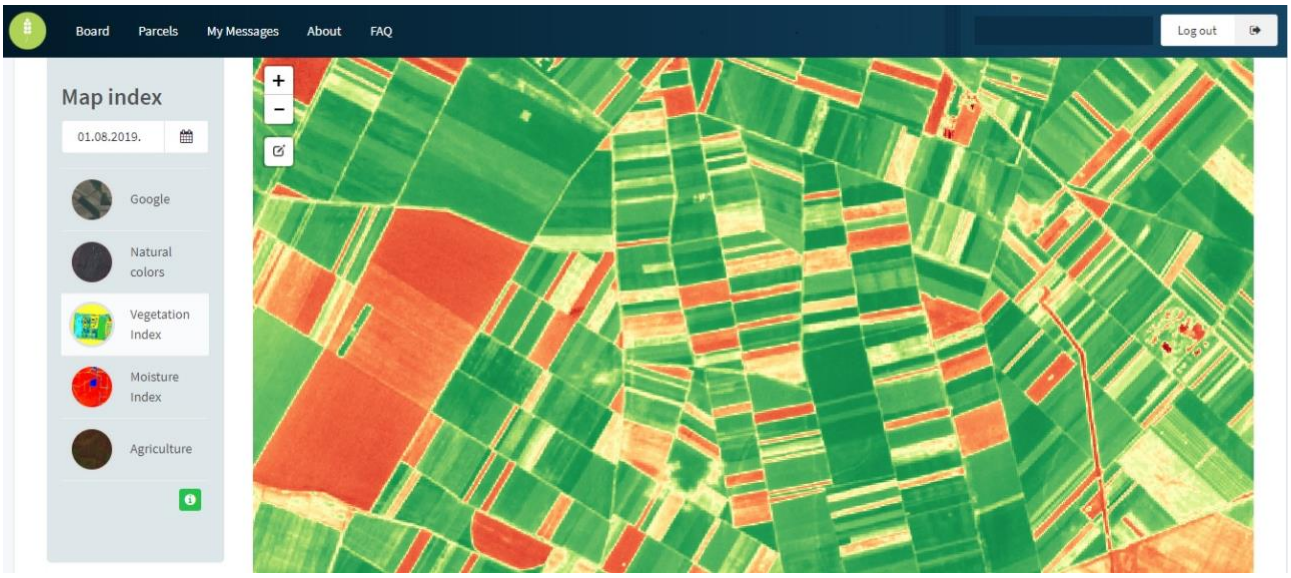


Figure 18: CropSupport application screenshot with available Sentinel-2 data from Sentinel Hub.

Within the LandSense consortium access to EO data was provided by [Sentinel-Hub] from Sinergise. Within some of the LandSense campaigns the EO data was additionally used in web/mobile applications to provide users with additional visual insights, e.g., visualizing Normalized Difference Vegetation Index (NDVI) within the agricultural pilot, shown in Figure 18, or visualization of Landsat-8 thermal band for assessing temperatures in Vienna within the City Oasis application, shown in Figure 19. This report will not give any guidelines on how to use Sentinel-Hub services; the reader is kindly invited to have a look at a number of tutorials and guidelines provided by the service itself, e.g.,

- https://www.sentinel-hub.com/explore/education/
- https://www.sentinel-hub.com/develop/api/
- https://sentinelhub-py.readthedocs.io/en/latest/examples.html
- https://eo-learn.readthedocs.io/en/latest/examples.html

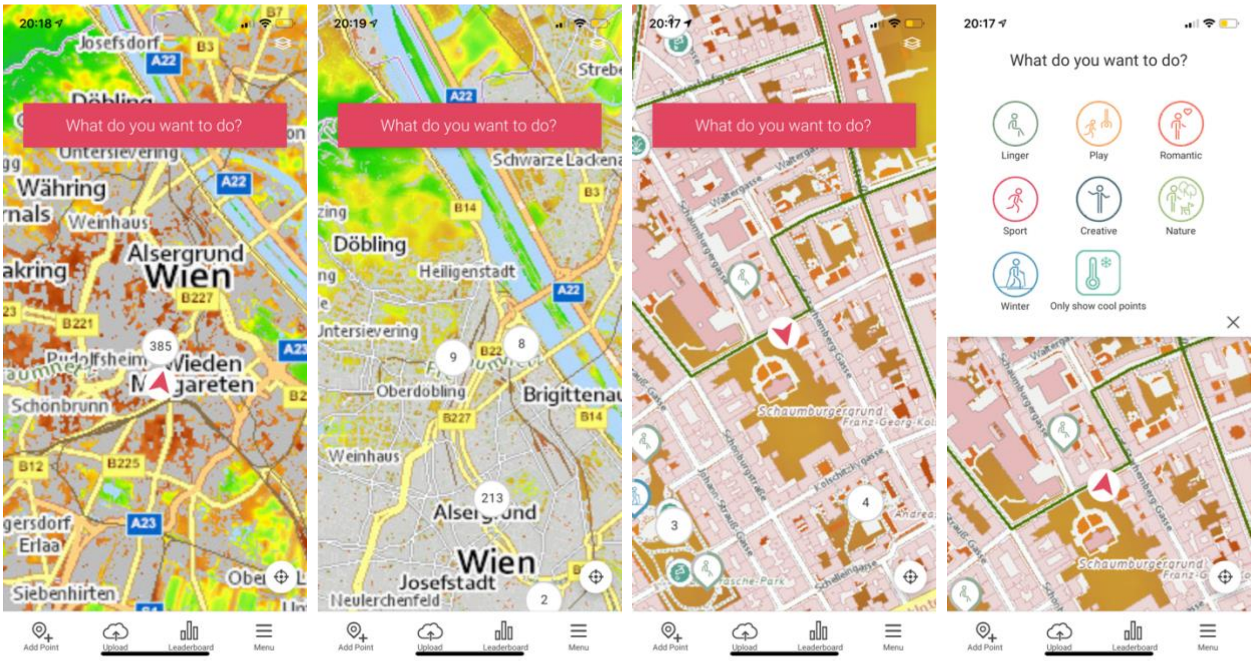


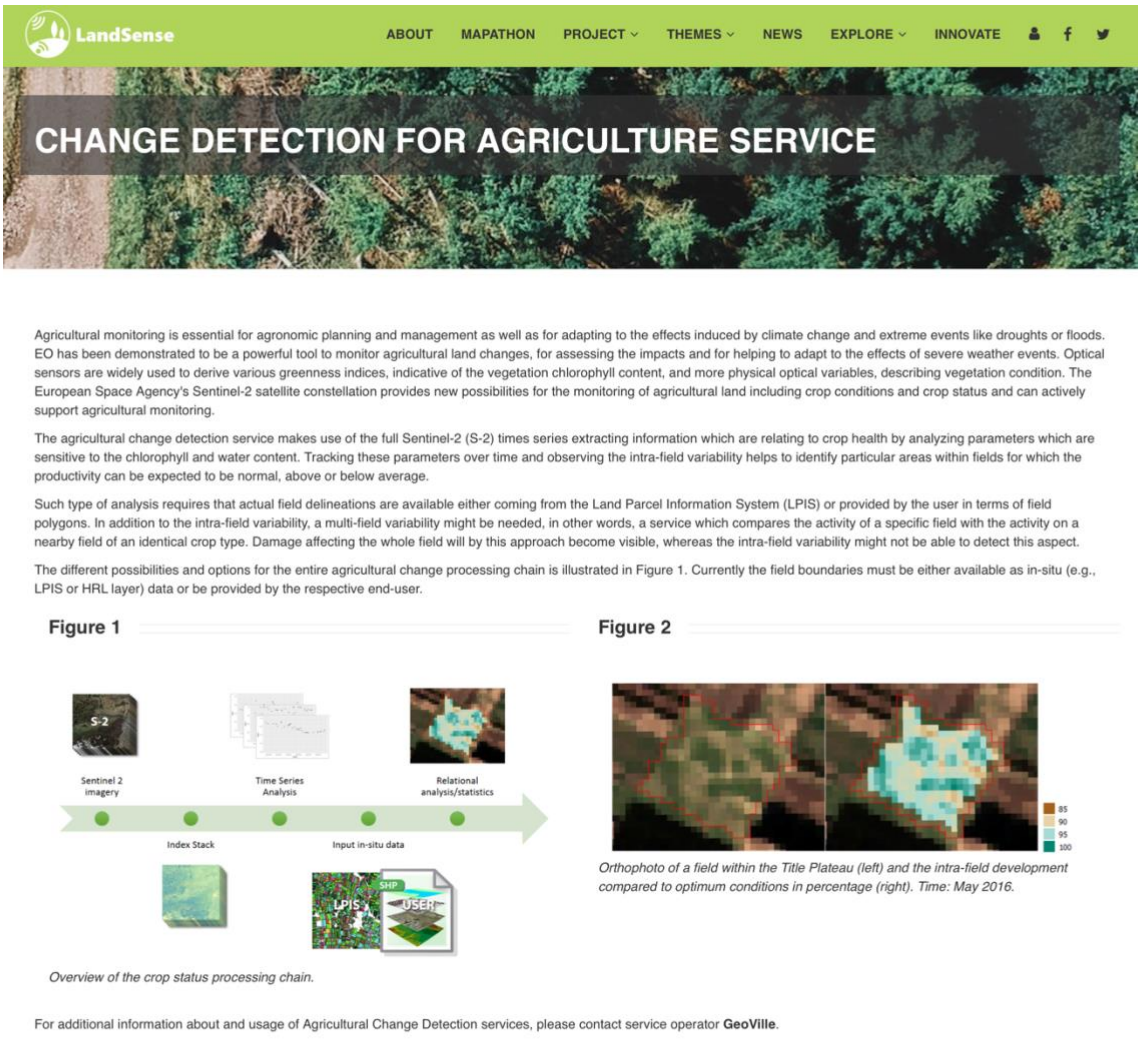
Figure 19: CityOases application with Landsat-8 thermal data. From left to right the user zooms from wider Vienna region into the location of interest, and then starts with contribution.

3.1 Agriculture change detection

The Agricultural Land Use pilot within LandSense is focused on the Vojvodina province of Serbia. The CropSupport platform allows its users to access valuable information about their land – namely, weather forecast for the micro locations of their parcels as well as NDVI, vegetation and moisture indexes from Sentinel-Hub. Even more useful insights for the users are provided with the use of the agricultural change detection service, provided by GeoVille.

The agricultural CD service, depicted in Figure 20, makes use of the full Sentinel-2 (S-2) times series extracting information, which are relating to crop health by analyzing parameters which are sensitive to the moisture and nitrogen content. The time series approach allows for the consideration of the growth history and the spatial variability of the vegetation indices within each field is obtained using statistical approaches. Tracking these parameters over time and observing the intra-field variability helps to identify particular areas within fields for which the productivity can be expected to be normal, above or below average.

GeoVille has identified the algorithm and service, described therein, as a possible business service offering based on use-case. As such, potential customers of the service should contact GeoVille directly.



CHANGE DETECTION FOR AGRICULTURE SERVICE

Agricultural monitoring is essential for agronomic planning and management as well as for adapting to the effects induced by climate change and extreme events like droughts or floods. EO has been demonstrated to be a powerful tool to monitor agricultural land changes, for assessing the impacts and for helping to adapt to the effects of severe weather events. Optical sensors are widely used to derive various greenness indices, indicative of the vegetation chlorophyll content, and more physical optical variables, describing vegetation condition. The European Space Agency's Sentinel-2 satellite constellation provides new possibilities for the monitoring of agricultural land including crop conditions and crop status and can actively support agricultural monitoring.

The agricultural change detection service makes use of the full Sentinel-2 (S-2) times series extracting information which are relating to crop health by analyzing parameters which are sensitive to the chlorophyll and water content. Tracking these parameters over time and observing the intra-field variability helps to identify particular areas within fields for which the productivity can be expected to be normal, above or below average.

Such type of analysis requires that actual field delineations are available either coming from the Land Parcel Information System (LPIS) or provided by the user in terms of field polygons. In addition to the intra-field variability, a multi-field variability might be needed, in other words, a service which compares the activity of a specific field with the activity on a nearby field of an identical crop type. Damage affecting the whole field will by this approach become visible, whereas the intra-field variability might not be able to detect this aspect.

The different possibilities and options for the entire agricultural change processing chain is illustrated in Figure 1. Currently the field boundaries must be either available as in-situ (e.g., LPIS or HRL layer) data or be provided by the respective end-user.

Figure 1

Overview of the crop status processing chain.

Figure 2

Orthophoto of a field within the Title Plateau (left) and the intra-field development compared to optimum conditions in percentage (right). Time: May 2016.

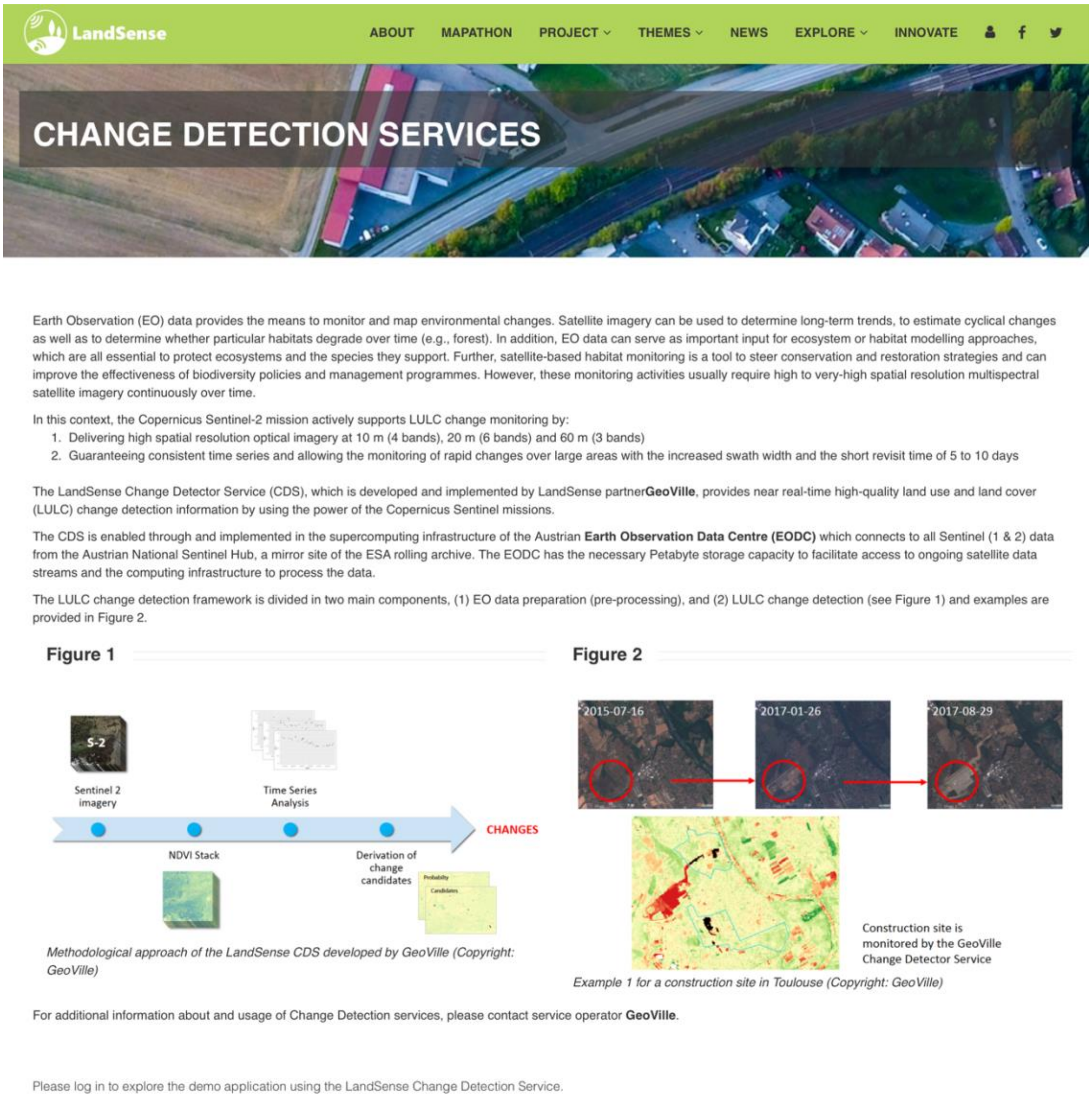
For additional information about and usage of Agricultural Change Detection services, please contact service operator **GeoVille**.

Figure 20: Agriculture change detection service on LandSense Engagement Platform (direct link)

More information about the demonstration pilot in Vojvodina can be found in D2.3 - Engagement action plans and campaign strategies for LandSense demonstration cases and D4.6 - Demo 2: Monitoring agricultural land use and provision of value-added agricultural services II.

3.2 Urban change detection

The Urban Change Detector Service provides near real-time high-quality land use and land cover (LULC) change detection information by performing a change analysis throughout the years. It is a computationally intensive process and was – for the purpose of the “Urban Landscape Dynamics” theme – run on the supercomputer infrastructure at the Earth Observation Data Centre (EODC) in Vienna by GeoVille. GeoVille has identified the algorithm and service, described therein, as a possible business service offering based on use-case run together with IGN-France. Interested parties can get more information about change detection service contacting GeoVille directly.



CHANGE DETECTION SERVICES

Earth Observation (EO) data provides the means to monitor and map environmental changes. Satellite imagery can be used to determine long-term trends, to estimate cyclical changes as well as to determine whether particular habitats degrade over time (e.g., forest). In addition, EO data can serve as important input for ecosystem or habitat modelling approaches, which are all essential to protect ecosystems and the species they support. Further, satellite-based habitat monitoring is a tool to steer conservation and restoration strategies and can improve the effectiveness of biodiversity policies and management programmes. However, these monitoring activities usually require high to very-high spatial resolution multispectral satellite imagery continuously over time.

In this context, the Copernicus Sentinel-2 mission actively supports LULC change monitoring by:

1. Delivering high spatial resolution optical imagery at 10 m (4 bands), 20 m (6 bands) and 60 m (3 bands)
2. Guaranteeing consistent time series and allowing the monitoring of rapid changes over large areas with the increased swath width and the short revisit time of 5 to 10 days

The LandSense Change Detector Service (CDS), which is developed and implemented by LandSense partner**GeoVille**, provides near real-time high-quality land use and land cover (LULC) change detection information by using the power of the Copernicus Sentinel missions.

The CDS is enabled through and implemented in the supercomputing infrastructure of the Austrian **Earth Observation Data Centre (EODC)** which connects to all Sentinel (1 & 2) data from the Austrian National Sentinel Hub, a mirror site of the ESA rolling archive. The EODC has the necessary Petabyte storage capacity to facilitate access to ongoing satellite data streams and the computing infrastructure to process the data.

The LULC change detection framework is divided in two main components, (1) EO data preparation (pre-processing), and (2) LULC change detection (see Figure 1) and examples are provided in Figure 2.

Figure 1

Methodological approach of the LandSense CDS developed by GeoVille (Copyright: GeoVille)

Figure 2

2015-07-16
2017-01-26
2017-08-29
Construction site is monitored by the GeoVille Change Detector Service

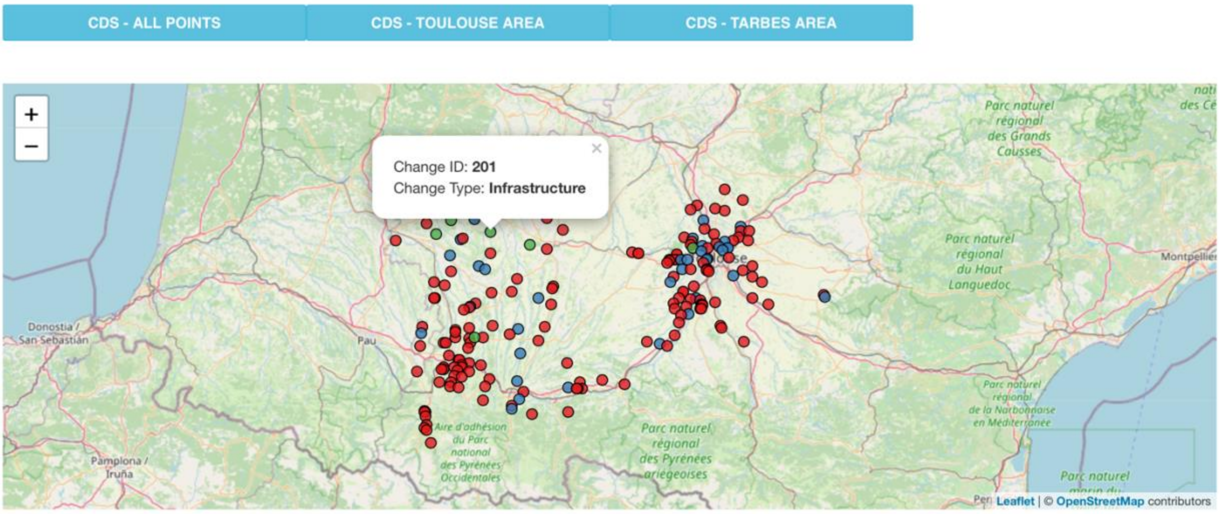
Example 1 for a construction site in Toulouse (Copyright: GeoVille)

For additional information about and usage of Change Detection services, please contact service operator **GeoVille**.

Please log in to explore the demo application using the LandSense Change Detection Service.

Figure 21: Urban change detection service on LandSense Engagement Platform (direct link).

Nevertheless, a demonstration tool on LEP, depicted in Figure 21, showcases the (exemplary) results of the detection done in collaboration with IGN-France. Note that to interact with results, users have to log-in to retrieve them from the service.



Change ID: **201**
Change Type: **Infrastructure**

CDS - ALL POINTS
CDS - TOULOUSE AREA
CDS - TARBES AREA
+
−
Donostia / San Sebastián
Pau
Pamplona / Iruña
Aire d'adhésion du Parc national des Pyrénées Occidentales
Parc naturel régional des Pyrénées ariégeoises
Parc naturel régional des Grands Causses
Parc naturel régional du Haut Languedoc
Montpellier
Parc naturel régional de la Narbonnaise en Méditerranée
Parc naturel
Leaflet | © OpenStreetMap contributors

Figure 22: Demonstration of the change detection services - results of detecting changes in urban areas in France.

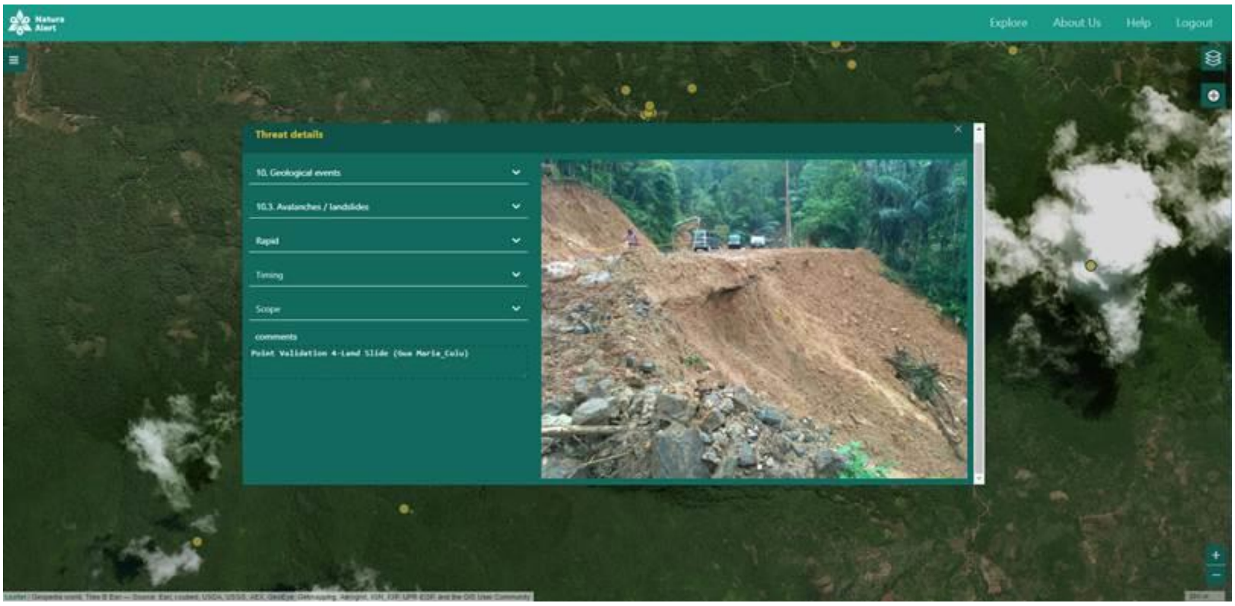
More information about the demonstration pilot in Vojvodina can be found in D2.3 - Engagement action plans and campaign strategies for LandSense demonstration cases.

3.3 Forest change detection

To support the “Forest and the Habitat monitoring” theme, particularly with activities in Indonesia, Sinergise implemented a processing chain using Sentinel-2 multispectral imagery with the BFAST Monitor method[1]. The support for this use-case was later on transferred to partners from Wageningen University and their service.

The results of forest CD service have been used within Natura Alert application (https://www.natura-alert.net); they served as input to the validation campaign during a workshop with local stakeholders in Indonesia. As part of the workshop programme, a group of 13-14 people collected ground truth data on several locations with detected changes. Attendees took photographs, videos and added comments to explain what has happened and if the detected change is a threat to the forest or not, storing attributes with Natura Alert, as shown in Figure 23.

[1] Verbesselt, J., Hyndman, R., Newnham, G. & Culvenor, D. Detecting trend and seasonal changes in satellite image time series. *Remote Sensing of Environment* **114,** 106–115 (2010).



Threat details

10. Geological events

10.3. Avalanches / landslides

Rapid

Timing

Scope

comments

Point Validation 4-Land Slide (Sao Maria_Colu)

Figure 23: Details about changes taken at the location of the detected change.

Operating change detection services that provide useful results and insights anywhere in the world out of the box is nearly impossible, so the consortium has focused its resources to support of pilots and campaigns run within LandSense themes and partners have decided to keep the services running for interested parties through their own infrastructure. The approach from Sinergise, using Sentinel Hub services to get the whole Sentinel-2 data history and BFAST on top of it, shows that a simplified approach can still produce meaningful results and has been open-sourced to the public as part of the LandSense output. An overview of how to make use of it is described in the following subsections.

The public repository is available at https://github.com/LandSense/SH-bfast and comes with a minimal working example of using Sentinel-Hub services together with BFast monitor to detect forest change. The repository has everything needed for a user to prepare software and run the Jupyter notebook.

3.3.1 Data access

The access to Sentinel-2 imagery is done through the Sentinel-Hub services, particularly by using Python libraries sentinelhub-py and eo-learn. In this example, we have used an area of interest in Brazil.

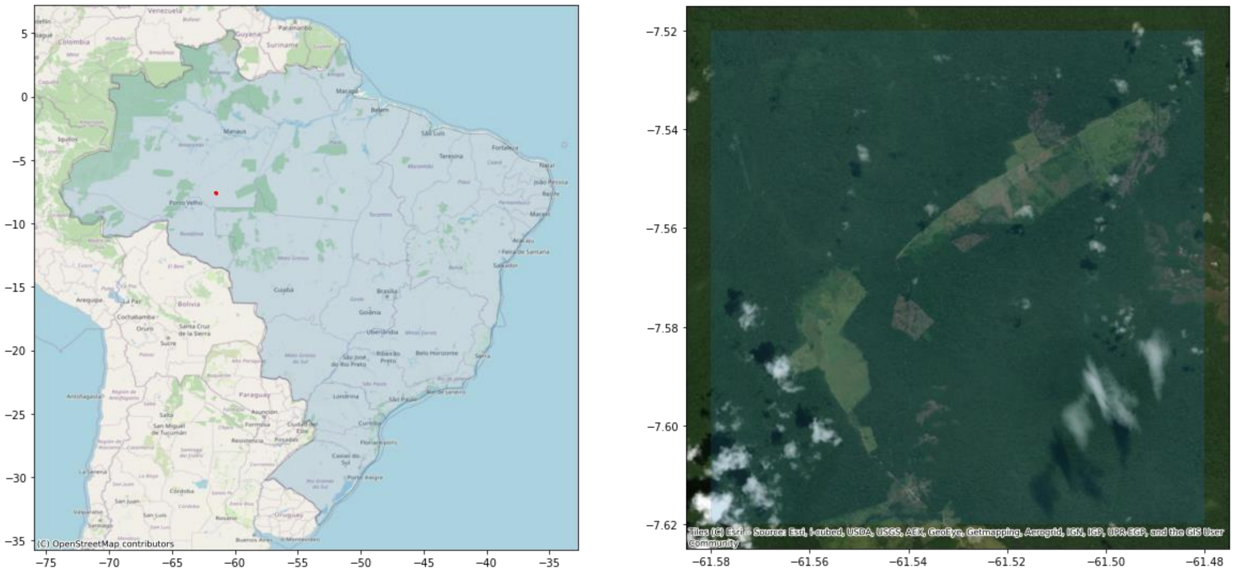

5
0
−5
−10
−15
−20
−25
−30
−35
−75
−70
−65
−60
−55
−50
−45
−40
−35
(C) OpenStreetMap contributors
−7.52
−7.54
−7.56
−7.58
−7.60
−7.62
−61.58
−61.56
−61.54
−61.52
−61.50
−61.48
Tiles (C) Esri — Source: Esri, i-cubed, USDA, USGS, AEX, GeoEye, Getmapping, Aerogrid, IGN, IGP, UPR-EGP, and the GIS User Community

Figure 24: Area of interest in the forest change detection example. The image on the left shows the approximate location, while the image on the right shows the area over a true-color imagery, showing the well-known issue of clouds.

3.3.2 Super-pixels

The approach in this example will first create super-pixels of the area. The algorithm used is [Felzenszwalb's method of segmentation](), and will segment the area of interest into super-pixels that have similar (spectral) properties both in spatial as well in temporal dimensions. The resulting super-pixels are vectorized to provide a placeholder for results from BFast.

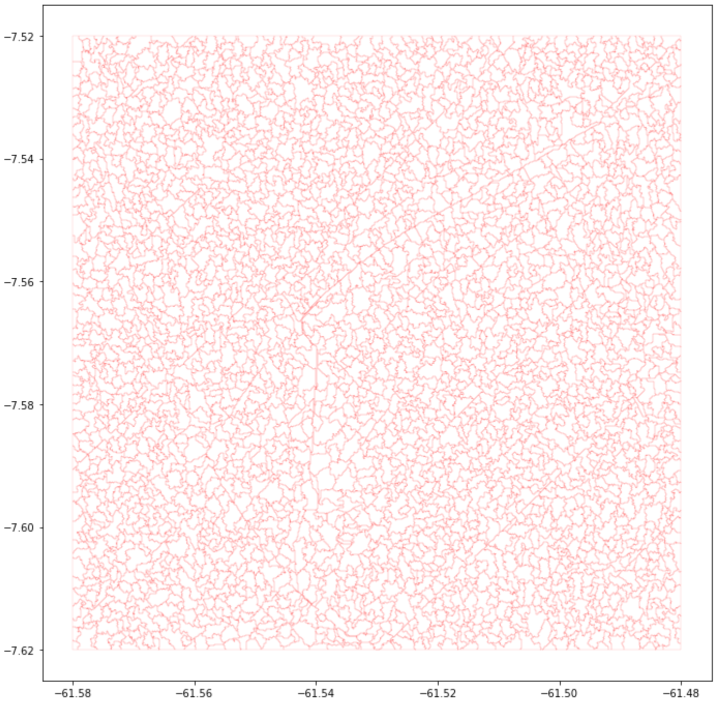


Figure 25: Super-pixels over our area of interest.

3.3.3 Running BFast

BFast monitor is then run on super-pixels, for a monitoring period provided by the user. We have wrapped the calls to R into a Python function, as all the needed packages for running BFast are available in the docker image.

Table 2: Data frame with BFast results over super-pixel geometries.

geometry	breakpoint	magnitude
POLYGON ((-61.55977 -7.52000, -61.55796 -7.520...	2020-02-09	0.030134

Positive magnitude values, signal vegetation growth/improvement, while large negative magnitudes represent the loss of vegetation.

Having results like this allow as visualize the changes immediately (Figure 26), find the breakpoints when the largest changes happened (Table 3) informing us that there were significant changes in June 2020.

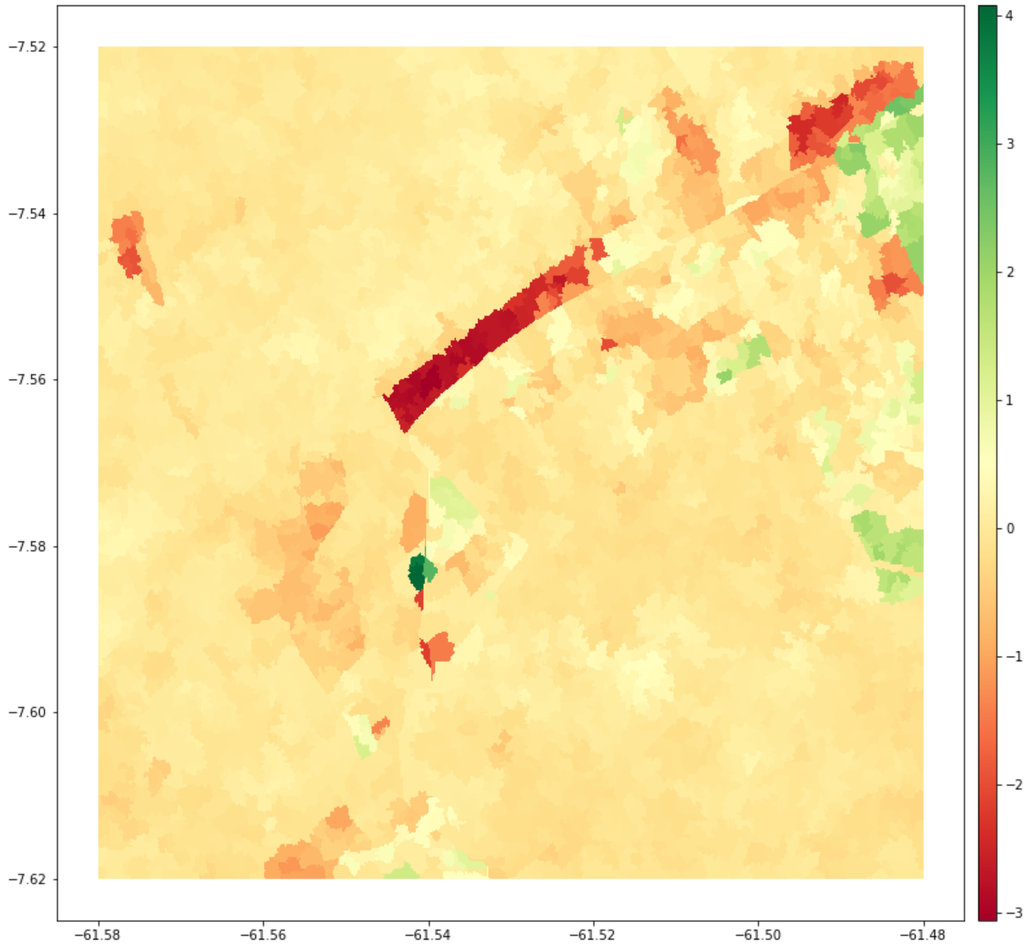


Figure 26: Magnitude of changes and their breakpoints.

Table 3: Breakpoints in time with the largest changes.

breakpoint	magnitude_min	magnitude_max
2020-03-22	-3.038306	0.333422
2020-06-04	-2.798667	3.808013
2020-06-08	-3.028984	1.055913
2020-06-13	-3.055240	0.832247
2020-06-23	-2.473472	4.082850

3.3.4 Visualize changes

Now that we know when the changes happened, we can visually appraise what happens, again using the Sentinel-Hub services to get the true-color imagery of before/after. The images clearly show change. If one looks to the image on the right, there are still some smoke plumes visible, (top right of the picture on the right), pointing to changes being detected probably due to burning agricultural practices.

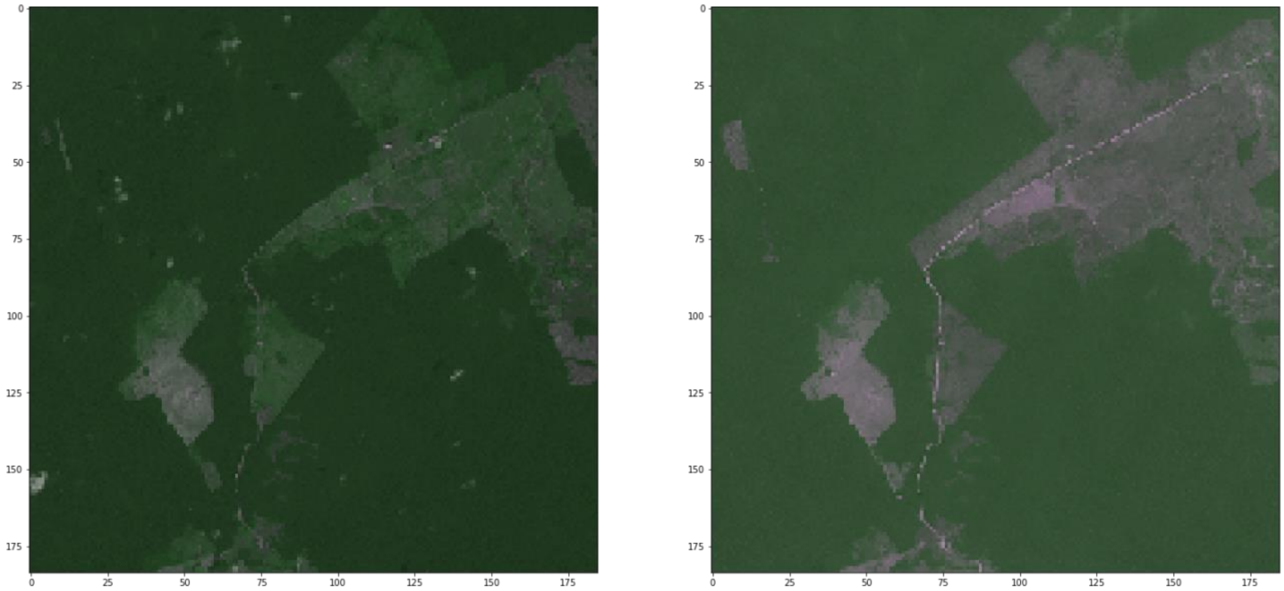


Figure 27: True-color visualization of area of interest before / after June 2020.

4 LandSense Quality Assurance and Control services

This section describes the Quality Assurance (QA) and Control service, provided as one of the main tools and services within the LandSense federation. The service is being used within several LandSense demonstration pilots for both assessing the quality of citizen-based observations, as well as assuring GDPR compliance for data dissemination.

To facilitate the exploitation of the QA services within the scope of good practice guidelines for citizen science collected data, we have open-sourced the QA platform. Subsection 4.1 provides the instructions to set up and run the service, while subsection 4.2 shortly describes available QA tests and is oriented towards users of the service.

4.1 LandSense QA service

The LandSense GitHub repositories (QA-Platform and QA R[2] scripts), have been open-sourced and can be accessed via GitHub or the LandSense Zenodo community repository:

- https://github.com/LandSense/QA-Platform
- https://github.com/LandSense/QA-R-Scripts
- https://zenodo.org/communities/landsense/

The main service includes a Java servlet-based framework based on Swagger (OpenAPI)[3] implementation, providing a simple deployment of REST endpoints for the QA tools presented in Section 4.2.These endpoints expose QA functionality as a single entry-point that can be interacted with, using any REST client software.

[2] https://www.r-project.org

[3] https://swagger.io/specification/

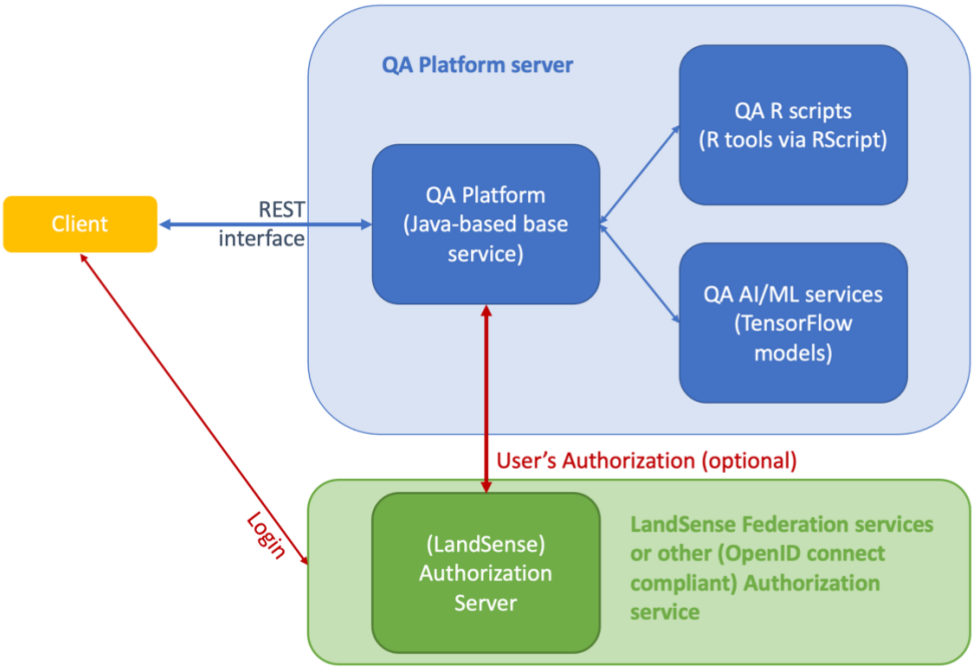

QA Platform server
QA R scripts (R tools via RScript)
QA Platform (Java-based base service)
QA AI/ML services (TensorFlow models)
Client
REST interface
User's Authorization (optional)
Login
(LandSense) Authorization Server
LandSense Federation services or other (OpenID connect compliant) Authorization service

Figure 28: Illustration of the QA platform server.

Figure 28 shows the general design of the LandSense quality assurance services and how it is coupled with the LandSense Federation for the purposes of authentication and authorization. As the operator of the service might not want such coupling, the repository includes instructions on how to sever the ties with Authorization service (or use any other OpenID Connect conformant service).

The QA Platform Server contains procedures directly implemented in Java and R, as well as a Docker[4] image that includes software for facial recognition and license plate blurring. The exact nature of these approaches is opaque to the user, who interacts only through the REST endpoint.

QA-Platform repository contains a maven module for the service (wps-rest), Java QA / processing algorithms (wps-app) and QA-R-Scripts (which run locally). The R scripts are already cloned from the QA-R-Script repository into the resources of wps-rest. Integration with a separate HTTP service for detecting faces in photographs is through configuration of FaceDetectorHTTPService.java class.

4.1.1 Requirements

For running the QA-Platform:

- Java.
- Tomcat (or other servlet container).

To support running the scripts from QA-R-Scripts (optional):

[4] https://www.docker.com

- R. The RScript binary, which should come with the standard R distribution, must be configured as an environment variable (i.e. RScript can be called from any shell location).

To support running the face detection (for blurring) service (optional):

- The Dockerized-Object-Recognition service should be running somewhere.

To support running the vehicle license plate detection (for blurring) (optional):

- OpenALPR needs to be installed locally. This project was tested with v2.3.0 (on Windows) and uses the OpenALPR java bindings. Download a binary OpenALPR Releases, unzip to somewhere on the local system and add as a system path variable (e.g., C:\openalpr_64).

4.1.2 Installation on headless server

The following steps guide the operator through the installation process on a server with (previously defined) requirements. The steps are rather straightforward for someone versatile with operating (developing and running) web services.

1. Clone the QA-Platform repository.
2. Build the code with Maven

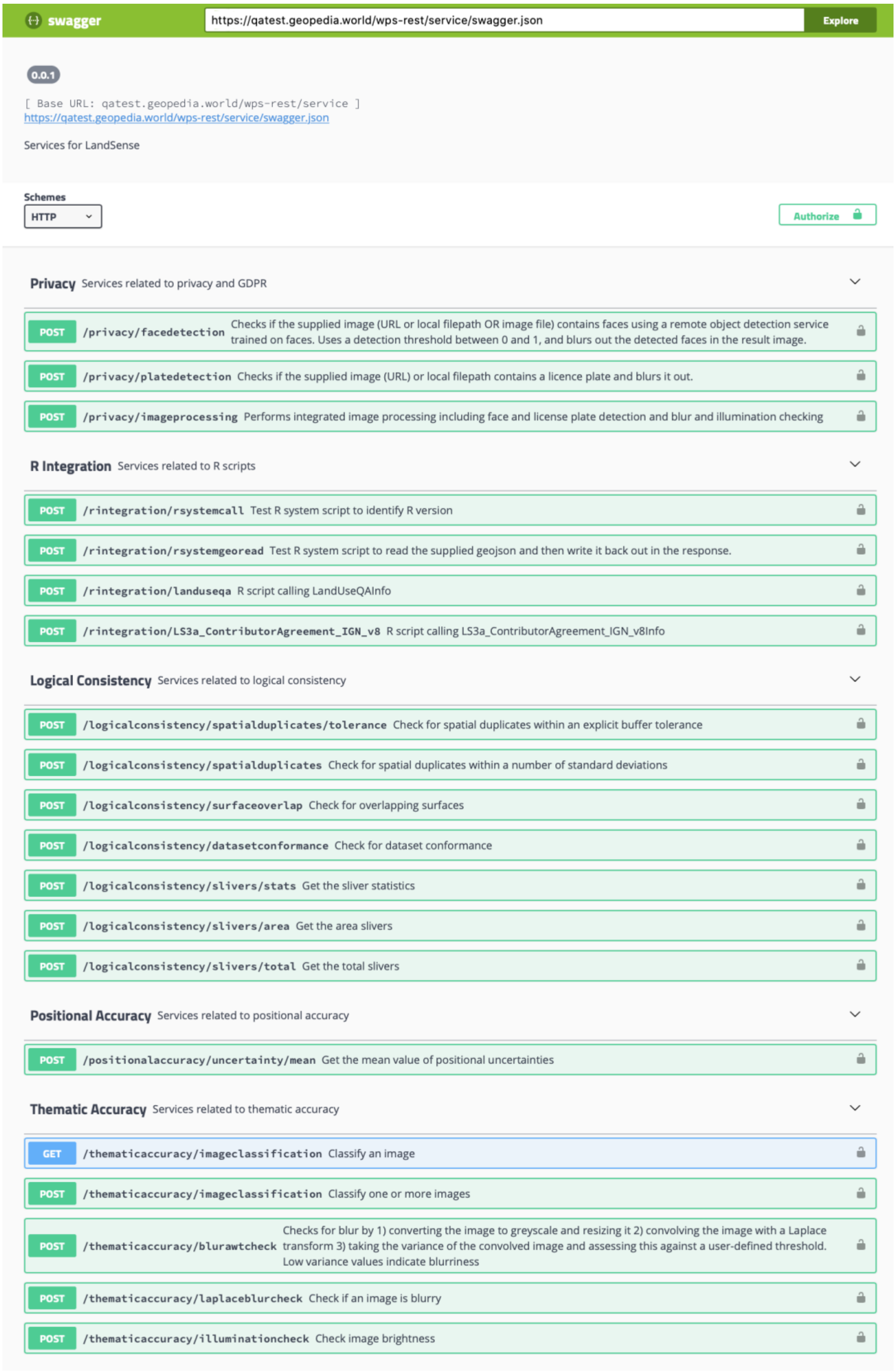
   ```
   sudo mvn -Dmaven.test.skip=true package
   ```

3. Deploy the war with servlet container, e.g., Tomcat

   ```
   sudo mv QA-Platform/wps-rest/target/wps-rest.war /opt/tomcat/apache-tomcat-7.0.90/webapps/
   ```

4. Modify the web.xml swagger configuration (e.g /opt/tomcat/apache-tomcat-7.0.90/webapps/wps-rest/WEB-INF/) to have the correct host (e.g. not localhost).
5. Restart the Tomcat if needed

   ```
   sudo /opt/tomcat/apache-tomcat-7.0.90/bin/startup.sh
   ```



https://qatest.geopedia.world/wps-rest/service/swagger.json

0.0.1

[Base URL: qatest.geopedia.world/wps-rest/service]
https://qatest.geopedia.world/wps-rest/service/swagger.json

Services for LandSense

Schemes
HTTP

Privacy Services related to privacy and GDPR

- POST `/privacy/facedetection` Checks if the supplied image (URL or local filepath OR image file) contains faces using a remote object detection service trained on faces. Uses a detection threshold between 0 and 1, and blurs out the detected faces in the result image.
- POST `/privacy/platedetection` Checks if the supplied image (URL) or local filepath contains a licence plate and blurs it out.
- POST `/privacy/imageprocessing` Performs integrated image processing including face and license plate detection and blur and illumination checking

R Integration Services related to R scripts

- POST `/rintegration/rsystemcall` Test R system script to identify R version
- POST `/rintegration/rsystemgeoread` Test R system script to read the supplied geojson and then write it back out in the response.
- POST `/rintegration/landuseqa` R script calling LandUseQAInfo
- POST `/rintegration/LS3a_ContributorAgreement_IGN_v8` R script calling LS3a_ContributorAgreement_IGN_v8Info

Logical Consistency Services related to logical consistency

- POST `/logicalconsistency/spatialduplicates/tolerance` Check for spatial duplicates within an explicit buffer tolerance
- POST `/logicalconsistency/spatialduplicates` Check for spatial duplicates within a number of standard deviations
- POST `/logicalconsistency/surfaceoverlap` Check for overlapping surfaces
- POST `/logicalconsistency/datasetconformance` Check for dataset conformance
- POST `/logicalconsistency/slivers/stats` Get the sliver statistics
- POST `/logicalconsistency/slivers/area` Get the area slivers
- POST `/logicalconsistency/slivers/total` Get the total slivers

Positional Accuracy Services related to positional accuracy

- POST `/positionalaccuracy/uncertainty/mean` Get the mean value of positional uncertainties

Thematic Accuracy Services related to thematic accuracy

- GET `/thematicaccuracy/imageclassification` Classify an image
- POST `/thematicaccuracy/imageclassification` Classify one or more images
- POST `/thematicaccuracy/blurawtcheck` Checks for blur by 1) converting the image to greyscale and resizing it 2) convolving the image with a Laplace transform 3) taking the variance of the convolved image and assessing this against a user-defined threshold. Low variance values indicate blurriness
- POST `/thematicaccuracy/laplaceblurcheck` Check if an image is blurry
- POST `/thematicaccuracy/illuminationcheck` Check image brightness

Figure 29: Swagger documentation, available upon successful installation and deployment of the service.

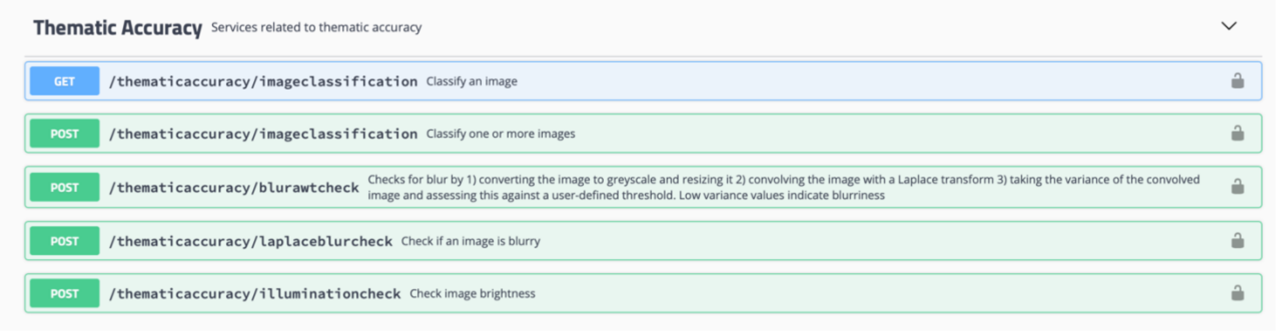
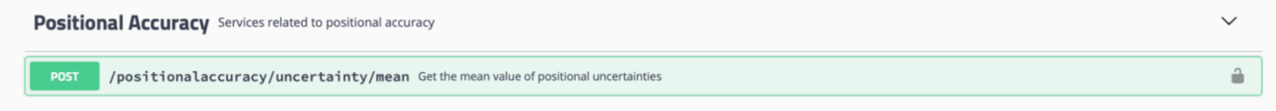
4.1.3 Checking the installation

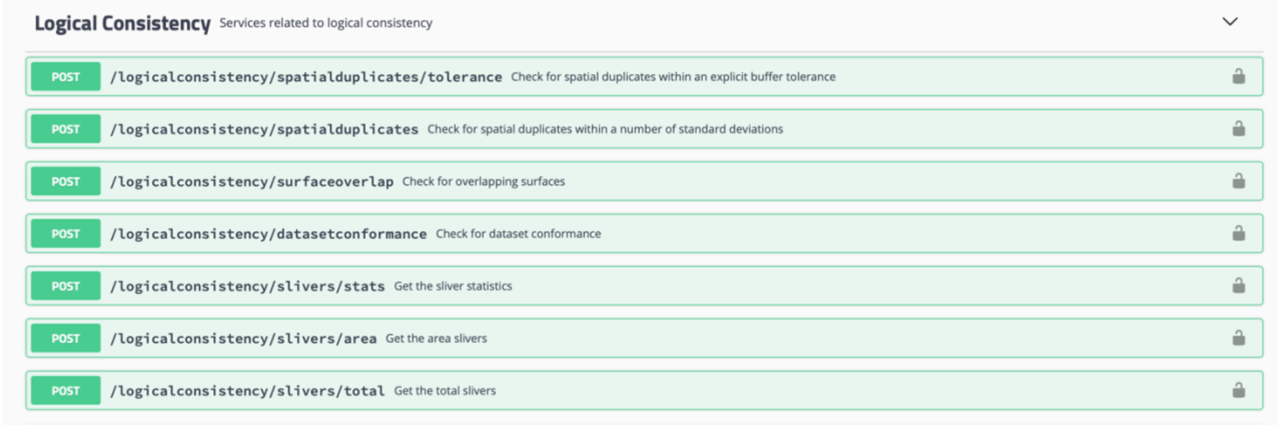
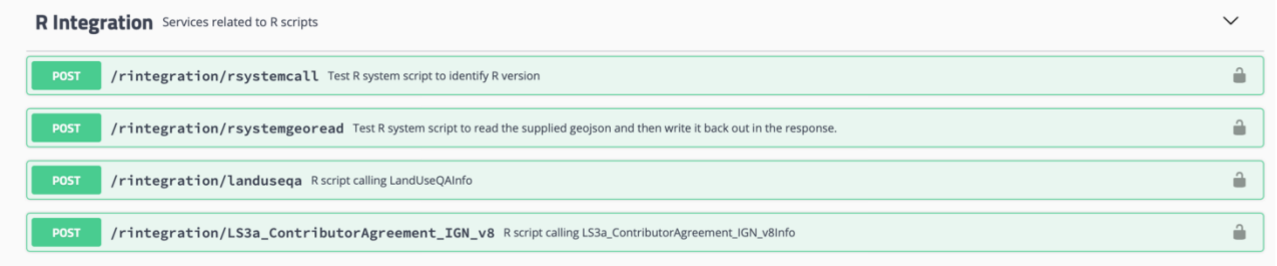
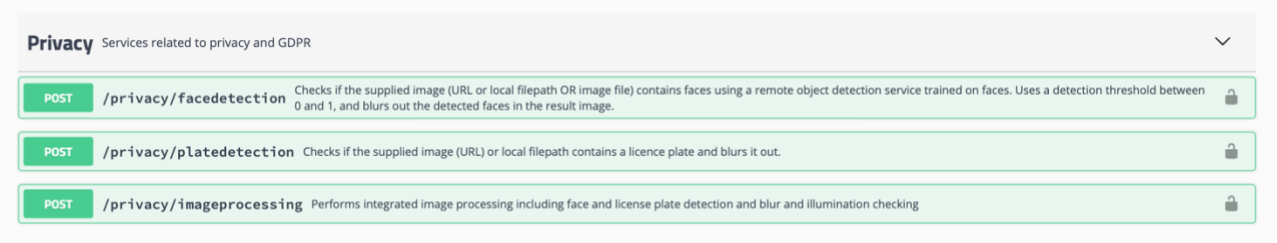
If the installation and startup of the service were successful, the operator can see the documentation on Figure 29, which corresponds to the Swagger documentation of the deployed service (https://qatest.geopedia.world/wps-rest/swagger/index.html), as seen in Figure 29.

4.2 LandSense QA tests

Table 4 lists the components (tests), available within LandSense QA services. They are described in detail in D5.3: Adaptation measures of COBWEB quality assurance service for the LandSense Citizen Observatory, D5.5: Operational workflows for integration of citizen-observed data in authoritative systems and D5.7: Good practice guidelines, protocols and benchmarking standards for quality assurance. The descriptions and API definitions are available through the deployed documentation service (https://qatest.geopedia.world/wps-rest/swagger/index.html).

Table 4: List of QA tests implemented within QA services.

<table>
<tr><th>Tests available within LandSense QA</th><th>Detailed description</th></tr>
<tr><td><b>Thematic accuracy</b></td><td>D5.7, section 3.2</td></tr>
<tr><td colspan="2">Checks for image metrics (blurriness, illumination, size and resolution)

Thematic Accuracy Services related to thematic accuracy
GET /thematicaccuracy/imageclassification Classify an image
POST /thematicaccuracy/imageclassification Classify one or more images
POST /thematicaccuracy/blurawtcheck Checks for blur by 1) converting the image to greyscale and resizing it 2) convolving the image with a Laplace transform 3) taking the variance of the convolved image and assessing this against a user-defined threshold. Low variance values indicate blurriness
POST /thematicaccuracy/laplaceblurcheck Check if an image is blurry
POST /thematicaccuracy/illuminationcheck Check image brightness</td></tr>
<tr><td><b>Positional accuracy</b></td><td>D5.4, D5.4</td></tr>
<tr><td colspan="2">Positional accuracy and offset of measurements

Positional Accuracy Services related to positional accuracy
POST /positionalaccuracy/uncertainty/mean Get the mean value of positional uncertainties</td></tr>
<tr><td><b>Consistency of geometrical data</b></td><td>D5.3 and D5.7, section 3.1</td></tr>
<tr><td colspan="2">Surface (polygon) overlap and correction</td></tr>
</table>

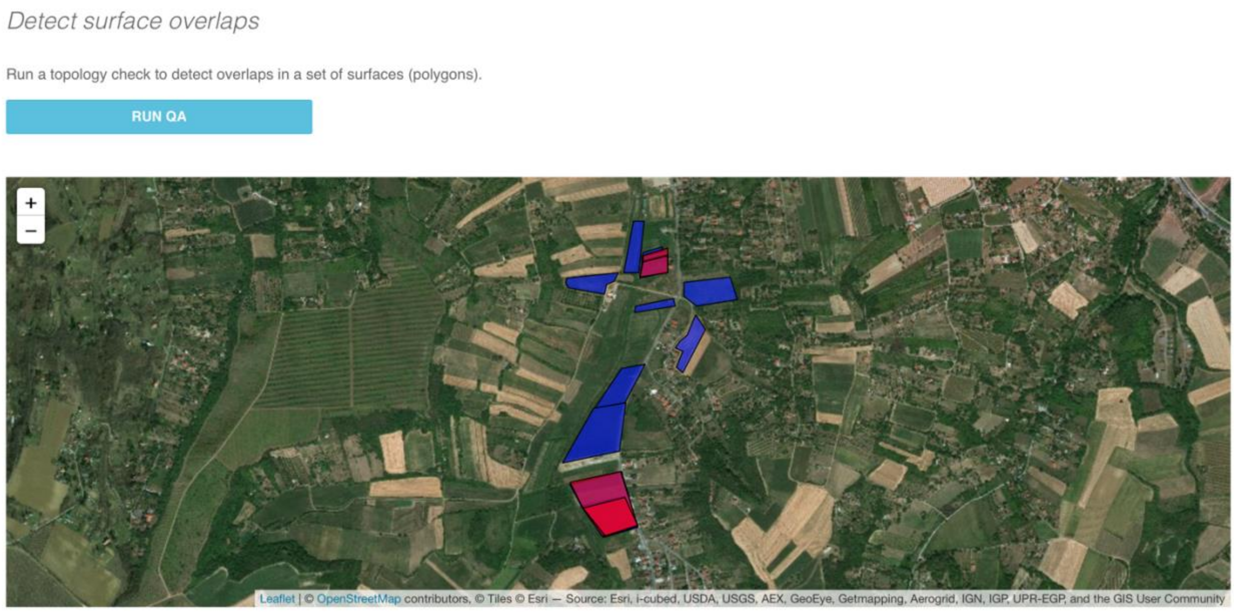
 Logical Consistency Services related to logical consistency POST /logicalconsistency/spatialduplicates/tolerance Check for spatial duplicates within an explicit buffer tolerance POST /logicalconsistency/spatialduplicates Check for spatial duplicates within a number of standard deviations POST /logicalconsistency/surfaceoverlap Check for overlapping surfaces POST /logicalconsistency/datasetconformance Check for dataset conformance POST /logicalconsistency/slivers/stats Get the sliver statistics POST /logicalconsistency/slivers/area Get the area slivers POST /logicalconsistency/slivers/total Get the total slivers	
Contributor agreement	D5.7, section 3.5
How data from different contributors agree  R Integration Services related to R scripts POST /rintegration/rsystemcall Test R system script to identify R version POST /rintegration/rsystemgeoread Test R system script to read the supplied geojson and then write it back out in the response. POST /rintegration/landuseqa R script calling LandUseQAInfo POST /rintegration/LS3a_ContributorAgreement_IGN_v8 R script calling LS3a_ContributorAgreement_IGN_v8Info	
Privacy	D5.7, section 3.3
Privacy related checks on images (face detection, licence-plate detection)  Privacy Services related to privacy and GDPR POST /privacy/facedetection Checks if the supplied image (URL or local filepath OR image file) contains faces using a remote object detection service trained on faces. Uses a detection threshold between 0 and 1, and blurs out the detected faces in the result image. POST /privacy/platedetection Checks if the supplied image (URL) or local filepath contains a licence plate and blurs it out. POST /privacy/imageprocessing Performs integrated image processing including face and license plate detection and blur and illumination checking	
Categorical accuracy	D5.7, section 3.6
Accuracy of attributes	

The QA service deployed for LandSense is operational, so the demonstration applications of some QA tests are available through LEP. The simple user interface is directed for the general public. The three tests implemented and demonstrated are

- Detection of polygon overlap
- Face detection and blurring
- Check image sharpness (detect blur)

The demos are available at https://landsense.eu/Innovate/QA. Because the full "flow" of LandSense federation is used, users who would like to test the service need to log in. Similarly, as with other demonstrators on LEP, anonymous login scope is used.

4.2.1 Polygon overlap detection



Detect surface overlaps

Run a topology check to detect overlaps in a set of surfaces (polygons).

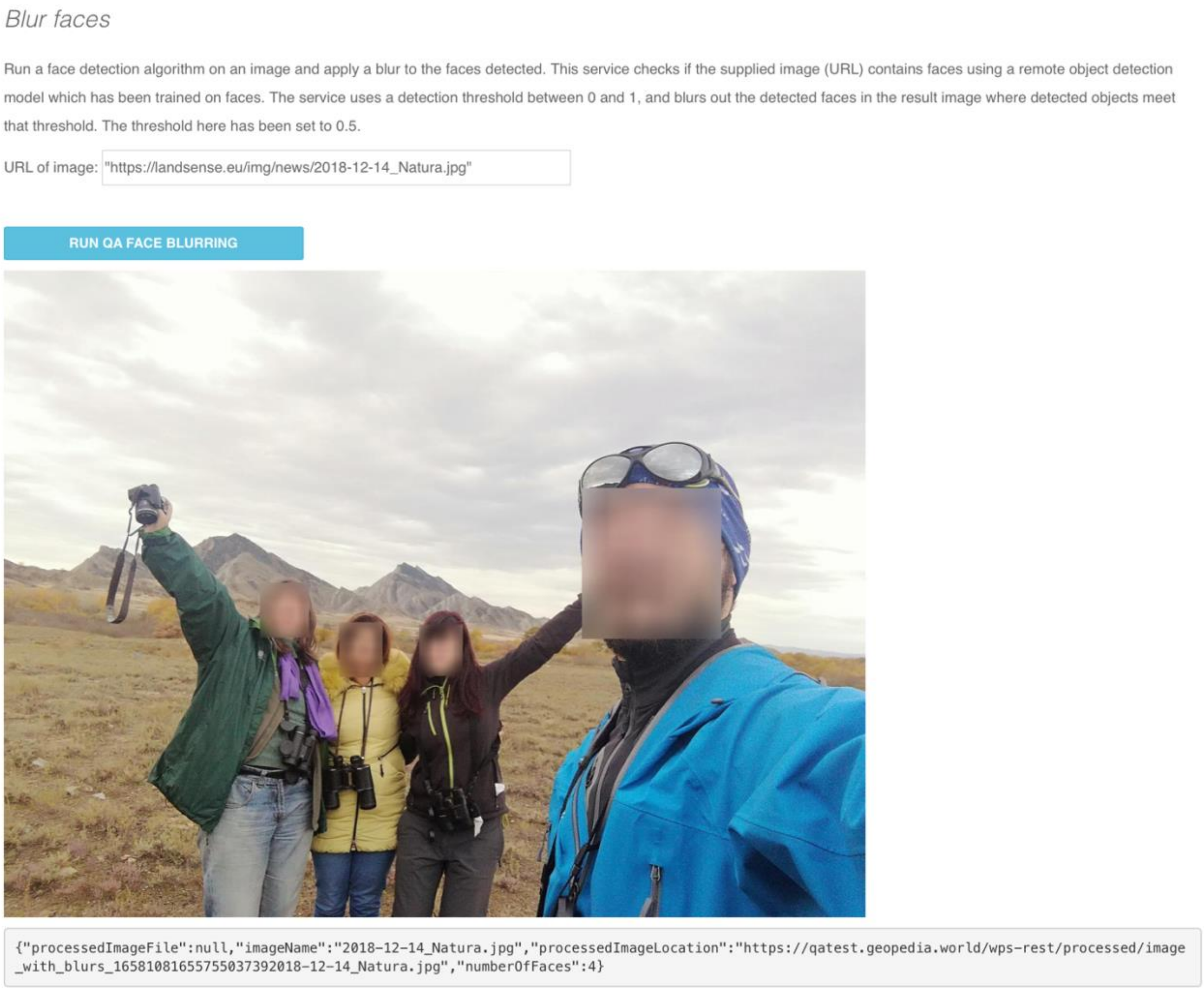
Leaflet | © OpenStreetMap contributors, © Tiles © Esri — Source: Esri, i-cubed, USDA, USGS, AEX, GeoEye, Getmapping, Aerogrid, IGN, IGP, UPR-EGP, and the GIS User Community

Figure 30: Polygon overlap detection demo on the LEP.

The demo displays a list of polygons to the user, and upon clicking "Run QA" sends the list of polygons to the QA Platform server (as geojson payload to the /surfaceoverlap endpoint), where the geometries are checked for overlap, and overlaps returned back to the user. The demo app shows the detected overlaps on the same map, this time styling them in red, as can be seen in Figure 30.

4.2.2 Face blurring

LandSense-based mobile applications such as City Oases and Natura Alert allow the possibility for participants to upload images taken with smartphones. GDPR stipulates that images of individuals should not be stored by a digital service and thus such images should either not be recorded or should be processed to obfuscate faces. Identifying and blurring faces is thus a very important service. The demo on the LEP allows the user to paste the URL of the image to have face blurring performed to the form. The URL is sent to the QA Platform server, where image is retrieved, faces detected and blurred. Figure 31 shows the results of face blurring.



Blur faces

Run a face detection algorithm on an image and apply a blur to the faces detected. This service checks if the supplied image (URL) contains faces using a remote object detection model which has been trained on faces. The service uses a detection threshold between 0 and 1, and blurs out the detected faces in the result image where detected objects meet that threshold. The threshold here has been set to 0.5.

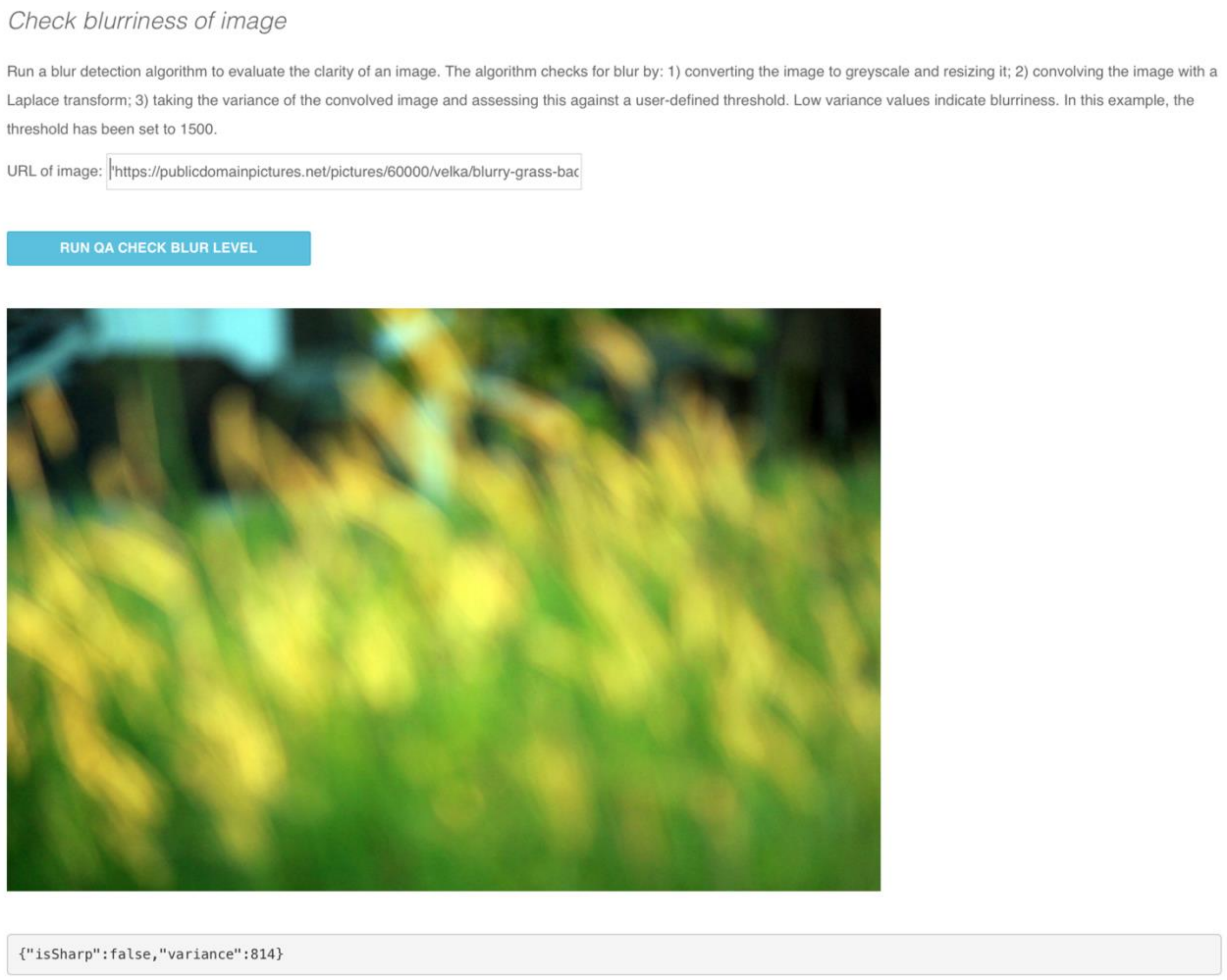
URL of image: "https://landsense.eu/img/news/2018-12-14_Natura.jpg"

```
{"processedImageFile":null,"imageName":"2018-12-14_Natura.jpg","processedImageLocation":"https://qatest.geopedia.world/wps-rest/processed/image
_with_blurs_16581081655755037392018-12-14_Natura.jpg","numberOfFaces":4}
```

Figure 31: Face detection and blurring demo on the LEP.

4.2.3 Image blurriness check

Furthermore, in order to provide high quality data from citizen image-based observations, a check for image quality is mandatory. A simple check for out-of-focus (blurred) images is one of the thematic accuracy checks that are available within QA Platform. The results of this QA demo are shown in Figure 32, indicating that the image is not sharp. If such checks are implemented at the point when the user is submitting the image (e.g., for on-the-spot data collection), the user can be notified the image quality is insufficient for the submission.



Check blurriness of image

Run a blur detection algorithm to evaluate the clarity of an image. The algorithm checks for blur by: 1) converting the image to greyscale and resizing it; 2) convolving the image with a Laplace transform; 3) taking the variance of the convolved image and assessing this against a user-defined threshold. Low variance values indicate blurriness. In this example, the threshold has been set to 1500.

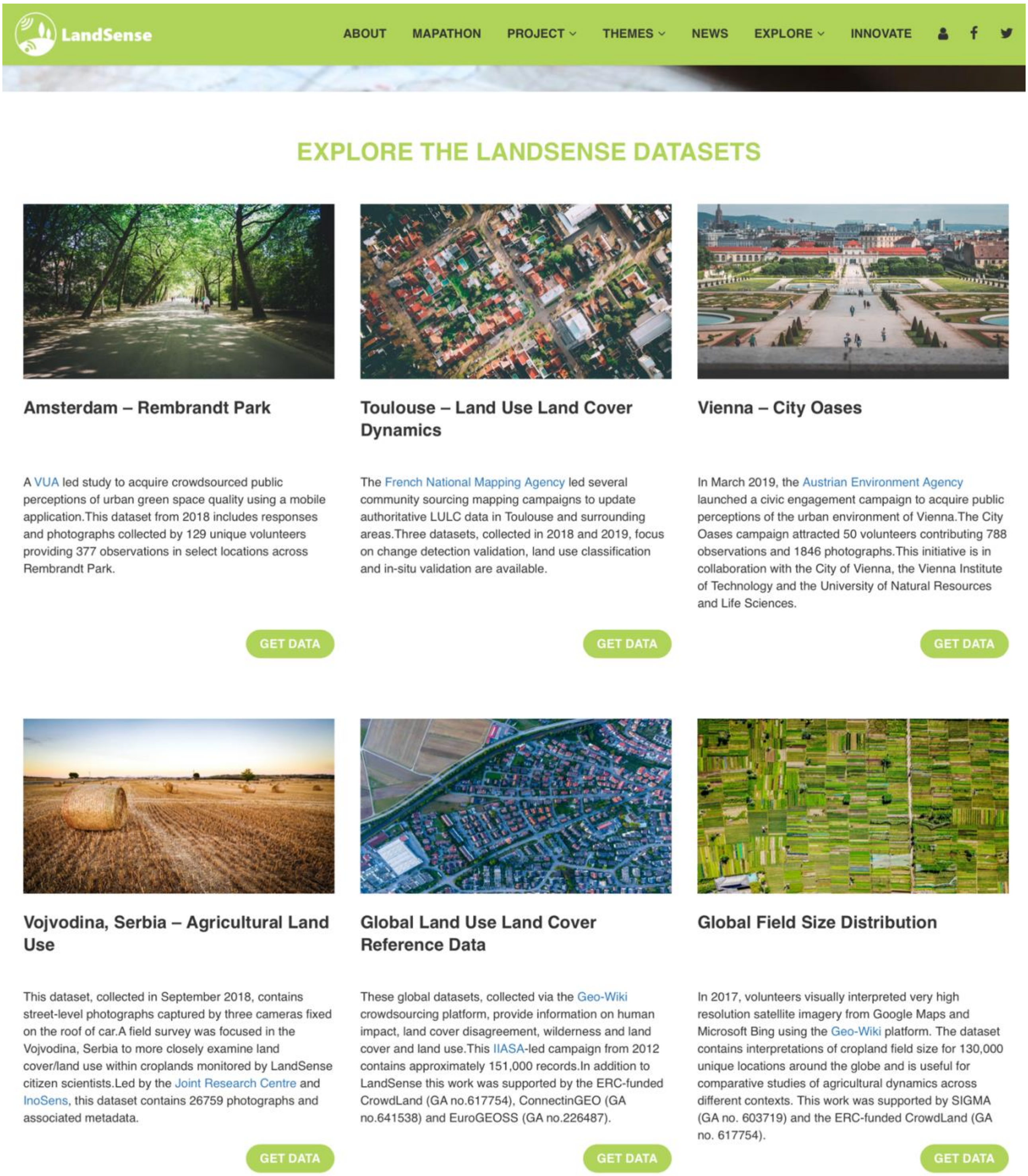
URL of image: 'https://publicdomainpictures.net/pictures/60000/velka/blurry-grass-bac

```
{"isSharp":false,"variance":814}
```

Figure 32: Image blurriness check on the LEP.

4.3 QA services for LandSense collected datasets

The QA service was used to produce final versions of datasets, collected within LandSense project. Table 5 shows which quality assurance analyses were applied to different LandSense pilots in order to produce datasets available through LEP, seen in Figure 33.



EXPLORE THE LANDSENSE DATASETS

Amsterdam – Rembrandt Park

A VUA led study to acquire crowdsourced public perceptions of urban green space quality using a mobile application.This dataset from 2018 includes responses and photographs collected by 129 unique volunteers providing 377 observations in select locations across Rembrandt Park.

Toulouse – Land Use Land Cover Dynamics

The French National Mapping Agency led several community sourcing mapping campaigns to update authoritative LULC data in Toulouse and surrounding areas.Three datasets, collected in 2018 and 2019, focus on change detection validation, land use classification and in-situ validation are available.

Vienna – City Oases

In March 2019, the Austrian Environment Agency launched a civic engagement campaign to acquire public perceptions of the urban environment of Vienna.The City Oases campaign attracted 50 volunteers contributing 788 observations and 1846 photographs.This initiative is in collaboration with the City of Vienna, the Vienna Institute of Technology and the University of Natural Resources and Life Sciences.

Vojvodina, Serbia – Agricultural Land Use

This dataset, collected in September 2018, contains street-level photographs captured by three cameras fixed on the roof of car.A field survey was focused in the Vojvodina, Serbia to more closely examine land cover/land use within croplands monitored by LandSense citizen scientists.Led by the Joint Research Centre and InoSens, this dataset contains 26759 photographs and associated metadata.

Global Land Use Land Cover Reference Data

These global datasets, collected via the Geo-Wiki crowdsourcing platform, provide information on human impact, land cover disagreement, wilderness and land cover and land use.This IIASA-led campaign from 2012 contains approximately 151,000 records.In addition to LandSense this work was supported by the ERC-funded CrowdLand (GA no.617754), ConnectinGEO (GA no.641538) and EuroGEOSS (GA no.226487).

Global Field Size Distribution

In 2017, volunteers visually interpreted very high resolution satellite imagery from Google Maps and Microsoft Bing using the Geo-Wiki platform. The dataset contains interpretations of cropland field size for 130,000 unique locations around the globe and is useful for comparative studies of agricultural dynamics across different contexts. This work was supported by SIGMA (GA no. 603719) and the ERC-funded CrowdLand (GA no. 617754).

Figure 33: LandSense datasets are available through LEP (https://landsense.eu/Explore/Datasets)

Table 5: List of QA tests used to produce LandSense datasets.

	Privacy checks	Contributor agreement	Positional accuracy	Thematic accuracy	Categorical accuracy
Amsterdam – Rembrandt park	✓	✓	✓	✓	✓
Toulouse – Land Use Land Cover Dynamics	✓	✓	✗	✓	✓
Vienna – City Oases	✓	✗	✓	✓	✗
Vojvodina, Serbia – Agricultural Land Use	✓	✗	✓	✓	✗
Vojvodina, Serbia – Street level imagery	✓	✗	✗	✓	✗

5 Tools and applications within LandSense

Different campaigns that were run throughout LandSense had their own dedicated data collection applications for citizen scientists and relevant stakeholders. The campaigns are presented more in details in D2.3: Engagement action plans and campaign strategies for LandSense demonstration cases II. The LEP also provides descriptions, links to applications, etc. for each campaign at https://landsense.eu/Explore/Campaigns. The campaign applications then have integrated user guides and how-tos so that the onboarding of new users is as simple as possible.

Table 6 lists the applications created or used within LandSense and associated links in order to make this deliverable also a concise directory of LandSense "tools".

Table 6: LandSense (campaign) applications

Output	Type	Description
City Oases	Mobile application	CityOases empowers people to report on their subjective perceptions of parks and open spaces in their urban environments. https://landsense.eu/Explore/5
MijnPark	Mobile application	MijnPark promotes sustainable urban development based on citizen insights on the perceptions of green and open spaces https://landsense.eu/Explore/4
Paysages	Mobile/Web application	Integrating expert contributions using crowdsourcing approaches into LULC authoritative databases https://landsense.eu/Explore/7 https://paysages.ign.fr/
Natura Alert	Mobile/Web application	A digital workflow for volunteer reporting, validation and subsequent national level assessments of threats to biodiversity https://natura-alert.net/
OSMLandUse	Web application	A WebGIS application to explore the OpenStreetMap database specifically in terms of landuse and landcover information https://landsense.eu/Mapathon https://osmlanduse.org
Picture Pile	Mobile application	Rapid classification of satellite imagery and photographs to support EO monitoring mechanisms https://geo-wiki.org/games/picturepile/
CropSupport	Mobile/Web application	Leveraging the power of EO systems and crowdsourcing to deliver value added service to farmers https://landsense.inosens.rs

LandSense started with the compendium of tools from various partners, most of which are also being sustained, albeit not as a LandSense federated service. To be concise and provide readers with an overview of these tools, platforms and services, Table 7 below shortly describes them and provides links on where/how to access them.

Table 7: Platforms and services used within LandSense

Output	Type	Description
Geo-Wiki	Web application	The Geo-Wiki platform provides citizens with the means to engage in environmental monitoring of the earth by providing feedback on existing information overlaid on satellite imagery or by contributing entirely new data. https://www.geo-wiki.org/
LACO-Wiki	Web application	LACO-Wiki is a web-based solution for validating land cover and land use maps. Using a variety of reference layers including satellite and aerial imagery from Google and Bing as well as OpenStreetMap, validation is a simple four-step process. After uploading your dataset, generate and validate the samples and create a report with the accuracy assessment. https://laco-wiki.net/en/Welcome
Sentinel Hub	service	Cloud API for satellite imagery. Service-oriented satellite imagery infrastructure takes care of all the complexity of handling satellite imagery archive and makes it available for end-users via easy-to-integrate web services. https://www.sentinel-hub.com
Geopedia	Spatial data infrastructure, web application	Both a spatial data infrastructure as well as a powerful geographic information system (GIS) web editor. https://www.geopedia.world

6 Conclusions

The deliverable lists the tools and applications from the LandSense Engagement Platform and provides users with guidelines and training material on how to use them. The applications and services described have been instrumental towards the successful implementation of the demonstration pilots.

The LandSense Authorization service glues the federation of these tools and services together and provides a GDPR compliant framework for citizen science data collection. The online demonstration application, available on LEP, shows contributors what (personal) data is shared with an application (and between them) based on different scopes. The federated authorization service is now being sustained via the Cos4Cloud project.

Operating a change detection service that provides useful results anywhere in the world out of the box is nearly impossible, so the change detection services will mostly continue operation under the umbrella of particular partner providing them. An open-source solution for forest change detection that uses Sentinel-Hub services for ease-of-access to satellite data has been released showing that such a simplified approach can produce meaningful results.

The quality assurance analyses are of interest to any citizen science or image data collection initiatives mostly due to protecting privacy and compliance with the GDPR. To facilitate reuse of development done and knowledge gained within LandSense, we have open-sourced the QA platform for all interested communities.

The various tools and applications from the demonstrator pilots are outlined. Some of these tools will be sustained via continued investment from partners across new research and development projects, others have been made open source for the benefit of the greater community, via GitHub repositories. We encourage interested parties to contact us for future collaboration on all LandSense related technologies.