NEXTGEOSS
Contributing to the Vision of GEO

deimos
elecnor group

User Management

Juan J. Doval
DEIMOS SPACE S.L.U.

NextGEOSS, April 2018

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 730329

Agenda

- Introduction
- User Management
- Roadmap
- Related Activities

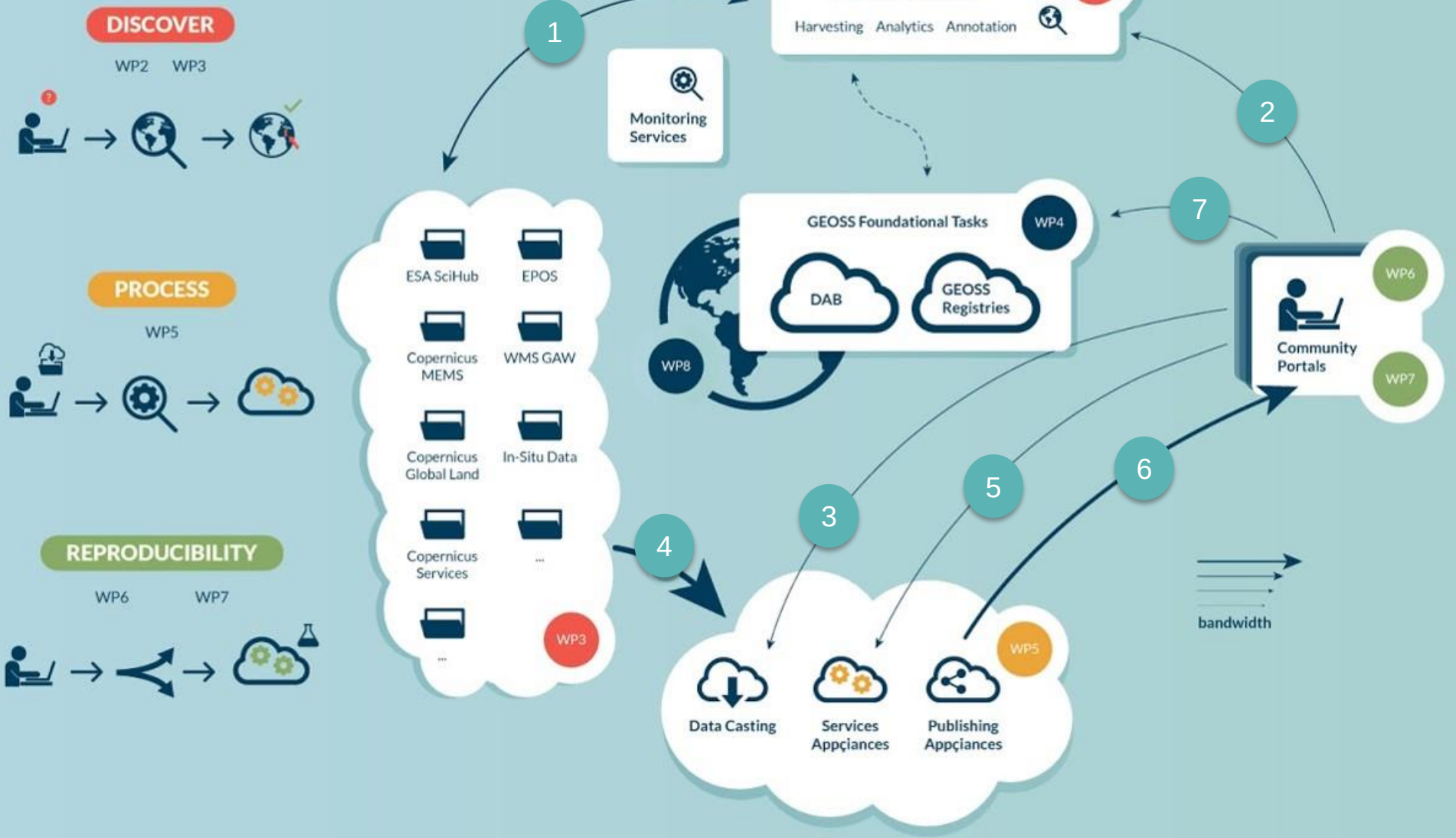
Introduction

NextGEOSS

- High-Level Architecture

NEXTGEOSS

Contributing to the Vision of GEO



1 **DataHub** harvest and register data, providing links to original sources

2 **Discovery Enablers** empower search on DataHub from users

3 **Access Enablers** allow community hubs to create data buckets for access

4 Enhanced distributed gateway from research and operational infrastructures

5 **Processing Enablers** allow community hubs to deploy distributed ICT technologies

6 **Publishing Appliances** deliver to the community hubs processed results

7 **Community Portals** register selected products and services to GEOSS

NEXTGEOSS
Contributing to the Vision of GEO

User Management

- Context - User Stories
- Main Functionality
- State-of-the-art protocols
- Architecture and Protocols
- System Status
- KPI Analytics

Context – User Stories

- As a **GEOSS user**, I want to be able to **register** myself in the GEOSS community so that the user information is provided to a centralized authentication server to support single sign-on (SSO) with GEOSS providers.

- As a **GEOSS user**, I want to be able to **authenticate and authorize** me in the GEOSS community with single sign-on (SSO) so that I can access to resources (data and some services)

A GEOSS user can be a data provider or a final user.

Main functionality

- Allows **registration** of users into the GEOSS community providing user information (user name, family name, email, telephone number, gender, ...)
- Allows **authentication and authorization** mechanisms based on GEOSS user credentials
- Provides **SSO** capability that enables a registered GEOSS user to log in once, and access multiple GEOSS applications without being required to authenticate for each application separately.
- Allows dynamic **client registration** of GEOSS services (i.e. harvesting, discovery, access and processing data) to be able to use the authentication and authorization mechanisms
- Allows integration of **social network login** (Google, Twitter, Facebook, LinkedIn).
- Allows integration of other SSO systems to provide a **federation** (e.g. ESA-https://eo-sso-idp.eo.esa.int, NASA-https://urs.earthdata.nasa.gov/).
- Is compatible with **different protocols**: OIDC, SAML2, Oauth2, ...

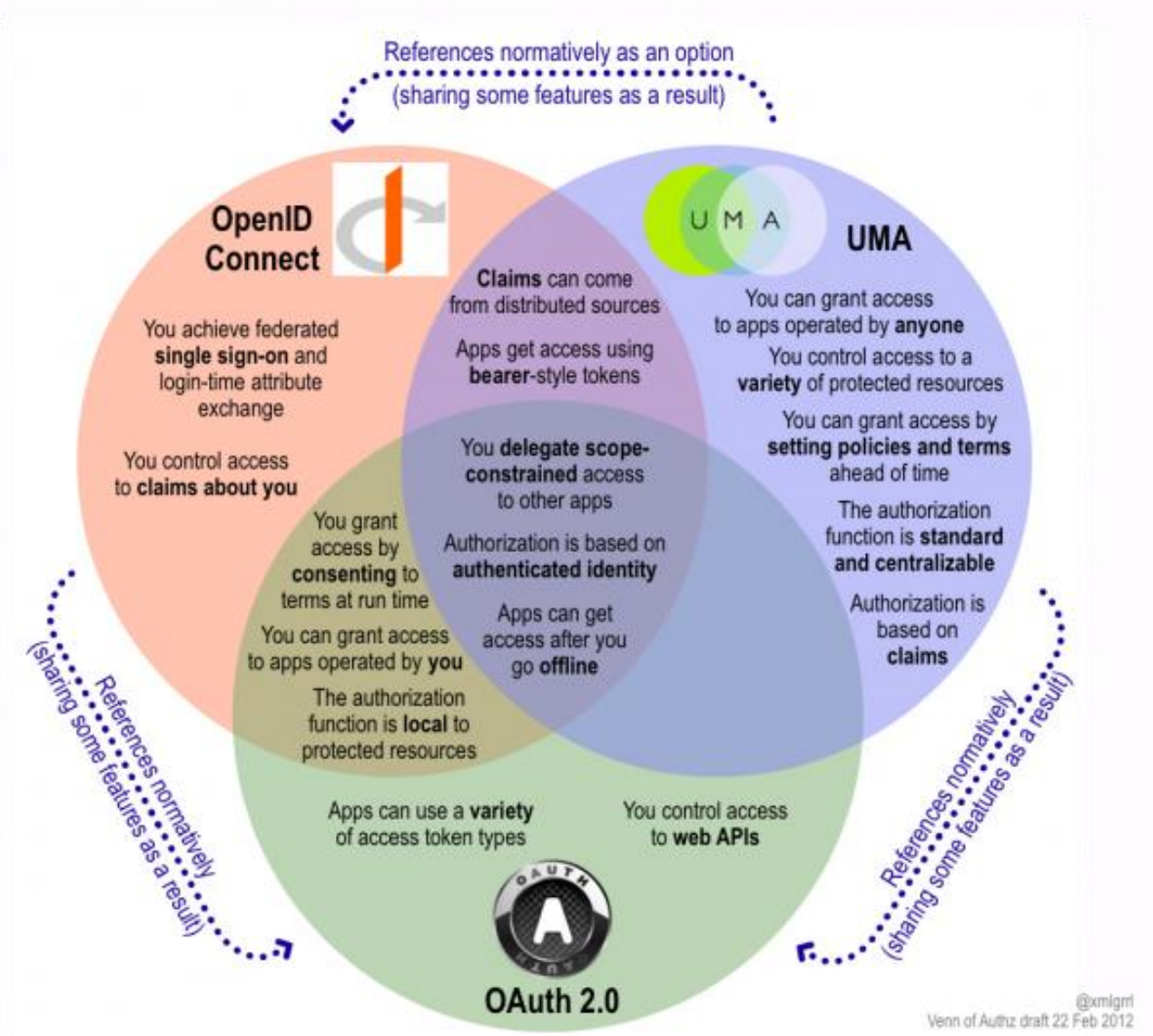
State-of-the-art protocols

Authentication viewpoint

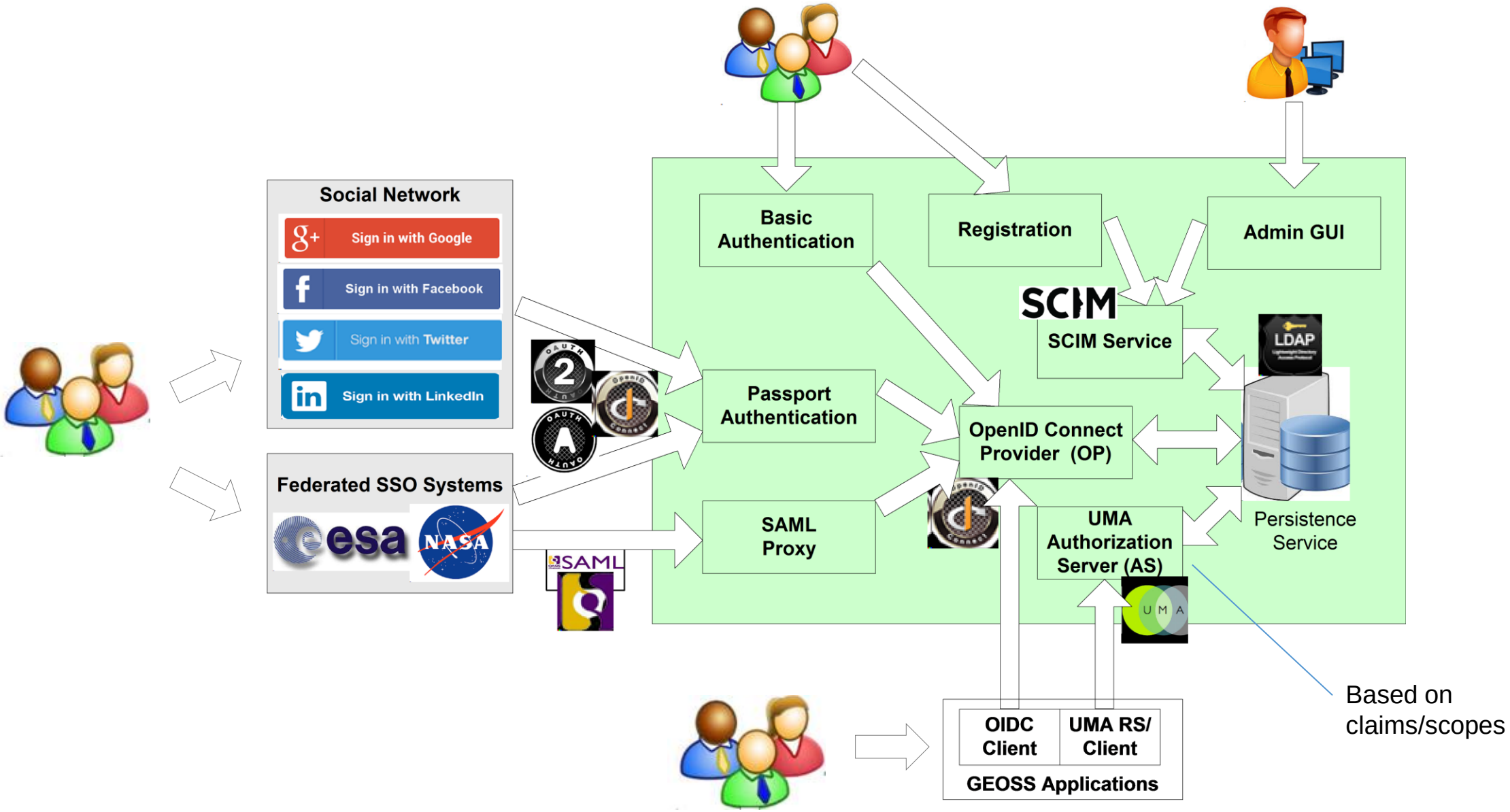
OpenID Connect turns SSO into a standard OAuth-protected identity API

SAML 2.0, OpenID 2.0	OAuth 2.0	OpenID Connect
☑ Initiating user's login session	✗ Not responsible for session initiation	☑ Initiating user's login session
✗ Not responsible for collecting user consent	☑ Collecting user's consent to share attributes	☑ Collecting user's consent to share attributes
☑ High-security identity tokens (*SAML only*)	✗ No identity tokens per se	☑ High-security identity tokens (*using JSON Web Tokens*)
✗ Distributed and aggregated claims	✗ No claims per se; protects arbitrary APIs	☑ Distributed and aggregated claims
☑ Dynamic introduction (*OpenID only*)	✗ Client onboarding is static	☑ Dynamic introduction
✗ Session timeout	✗ No sessions per se	☑ Session timeout (*in the works*)

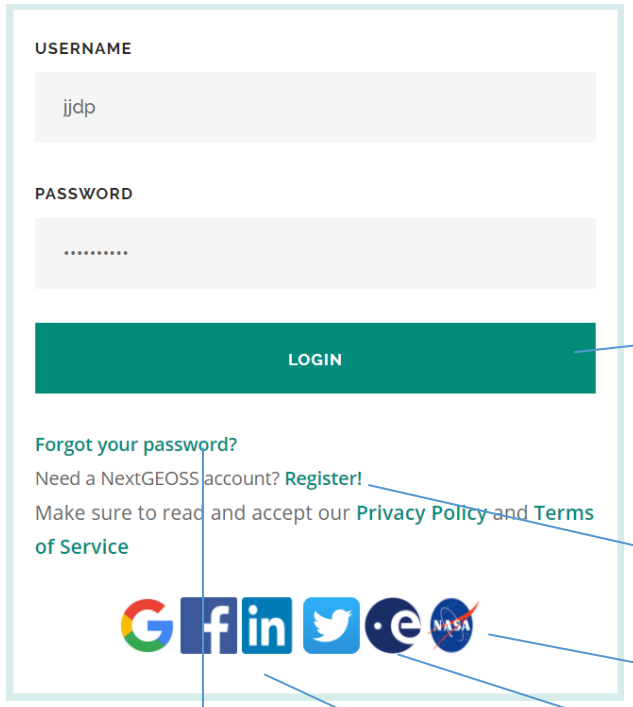
Authentication/Authorization viewpoint

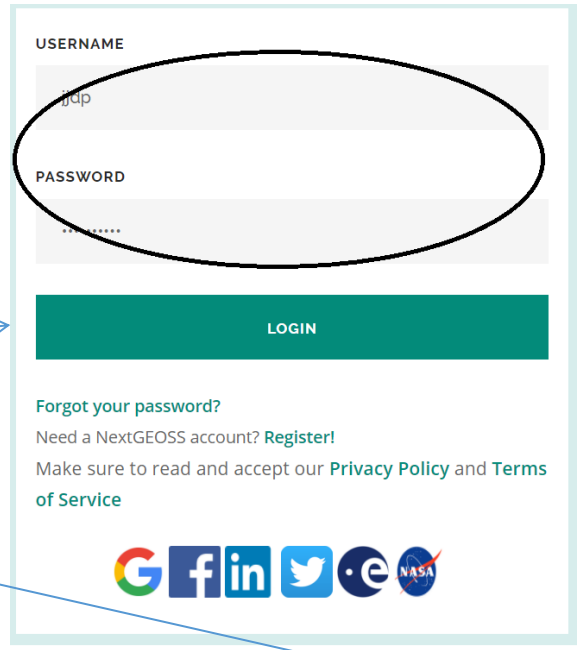


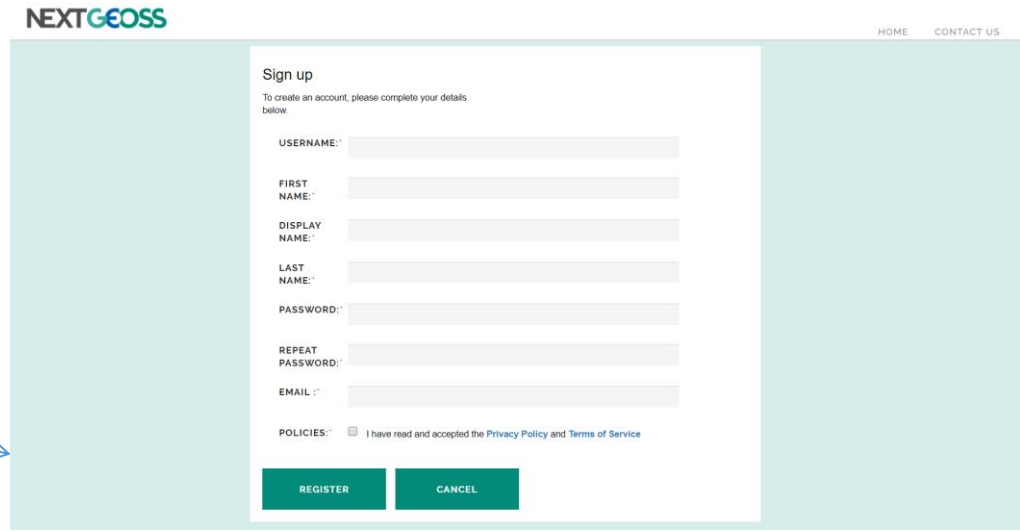
Architecture and Protocols

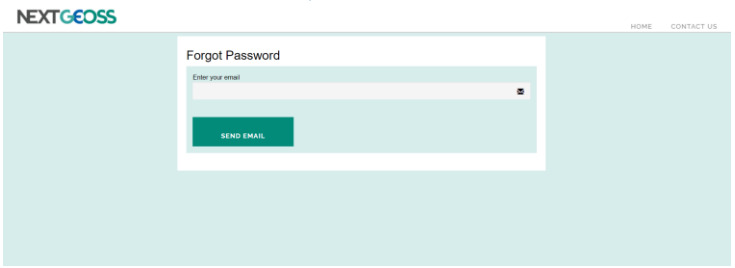


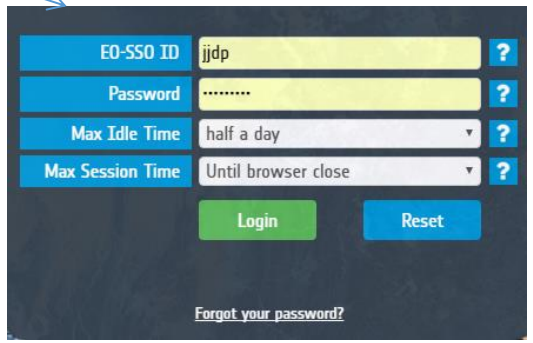
System Status

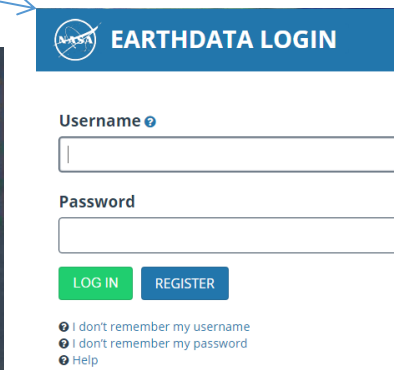












KPIs

#	Key Performance Indicator	Definition of indicator	Type of data required	Source	Baseline at start of NextGEOSS	Target at the end of NextGEOSS	Frequency of Measurement
T5.4.1	Functionality: Management of federated entities (Identity Providers)	Number of entities in the authentication federation including social network	List of entities in the authentication federation, including Identity providers from social network services (Google, Facebook, Twitter, LinkedIn) and from GEOSS-related institutions (ESA, NASA)	User Management configuration files	0	KPI value: 6+ (4+ at EP-1, 5+ at EP-2, 6+ at EP-3) KPI percentage= (entitities_intgrated/6) * 100	Weekly
T5.4.2	Usability: Authentication performance	Time to login	Login messages with dates	User Management log files	0	KPI value: <time to login> KPI percentage= count(time_to_login<2secs) / count(number_logins)	Weekly
T5.4.3	Adoption: Number of registered users	Number of users in the Persistence Storage	List of registered users within the NextGEOSS user management system	User Management persistence database (LDAP)	0	KPI value: 100+ (cumulative) (15+ at EP-1, 50+ at EP-2, 100+ at EP-3) KPI percentage= (entitities_intgrated/100) * 100	Weekly
T5.4.4	Adoption: Number of authentication requests per week	Number of authentication requests, successful	Login messages with authentication information	User Management log files	0	KPI value: 30+ (5+ at EP-1, 15+ at EP-2, 30+ at EP-3) KPI percentage= (entitities_intgrated/30) * 100	Weekly
T5.4.5	Adoption: Number of integrated GEOSS Client Applications	Number of integrated GEOSS Client Applications	List of Client IDs / Applications	User Management log files	0	KPI value: 20+ (cumulative) (4+ at EP-1, 10+ at EP-2, 20+ at EP-3) KPI percentage= (entitities_intgrated/20) * 100	Weekly

KPIs Dashboard

NEXTGEOSS
Contributing to the Vision of GEO

KPI 5.4.1

Goal: 6 IDPs

Current number of IDPs: 4

KPI 5.4.1 Percentage

66%

Current percentage

Authentications by IDP

KPI 5.4.4

Number of user authentications per week

Goal: 30 authentications (100%)

KPI 5.4.4 Percentage

103.33%

Current percentage (This week)

KPI 5.4.2

Percentage of user authentications served in less than 2 seconds.

Goal: 100% of requests under 2s

KPI 5.4.2 Percentage

96.77%

Log-in performance (this week)

KPI 5.4.4 Table

Week	Last totalAuthWeek	Target Percentage
49	31	103.33%
48	21	70%

KPI 5.4.2 Table

Week	#AuthTime < 2s	%AuthTime < 2s
49	30	96.77%
48	20	95.24%

KPI 5.4.5

Number of integrated GEOSS Client Applications

Goal: 20 registered clients (100%)

KPI 5.4.5 Percentage

20%

Current percentage

KPI 5.4.3

Number of registered users

Goal: 100 users

KPI 5.4.3 Percentage

6%

Current percentage

KPI 5.4.5 Table

Week	#Registered Clients	Target Percentage
49	4	20%
48	4	20%
47	1	5%
46	1	5%
42	1	5%

KPI 5.4.3 Table

@timestamp per week	#Registered Users	Target percentage
49	6	6%
48	6	6%
47	2	2%
46	2	2%
45	-	-
44	-	-
43	-	-
42	1	1%

Roadmap

- Short-Term Plan
- Proposed Approach

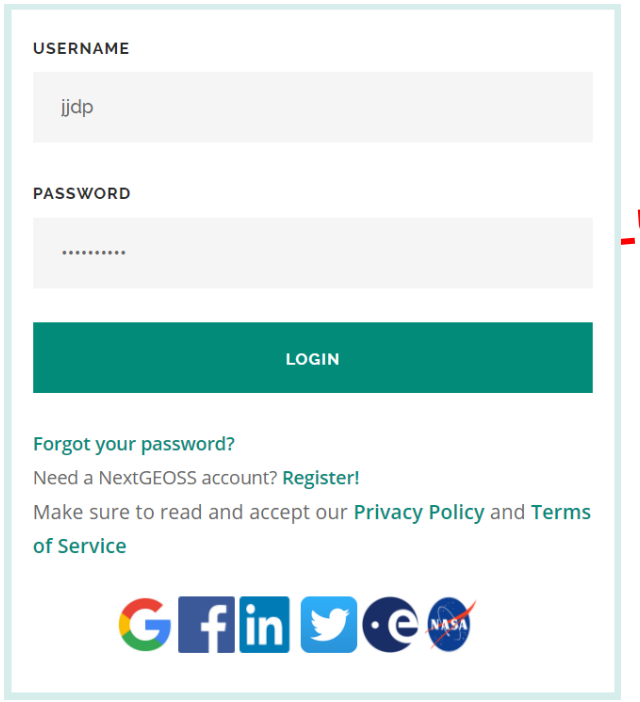
Short-Term Plan

Apps/Services Integration:

- ✓Analytics (i.e. DEIMOS), Community feedback (i.e. CREAF) , Data providers (i.e. CAMS) , Data processing services (i.e. TDUE WPS) , Data discovery 'signed user benefits' (i.e. CKAN API)

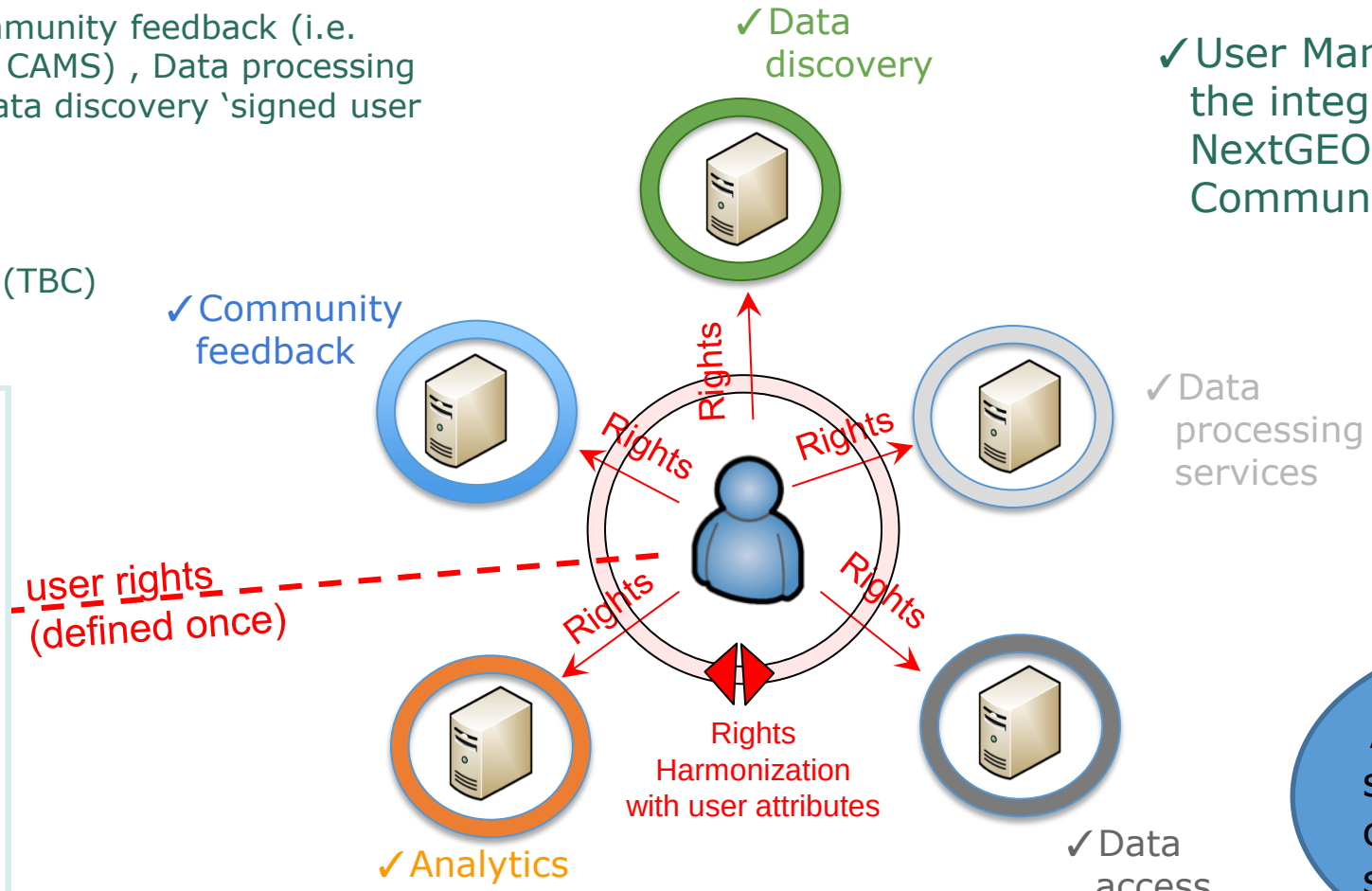
SSO federation:

- ✓ESA, NASA, OGC Testbed 14 (TBC)



NextGEOSS Big picture:

- ✓User Management serves the integration of NextGEOSS services in Community Portals

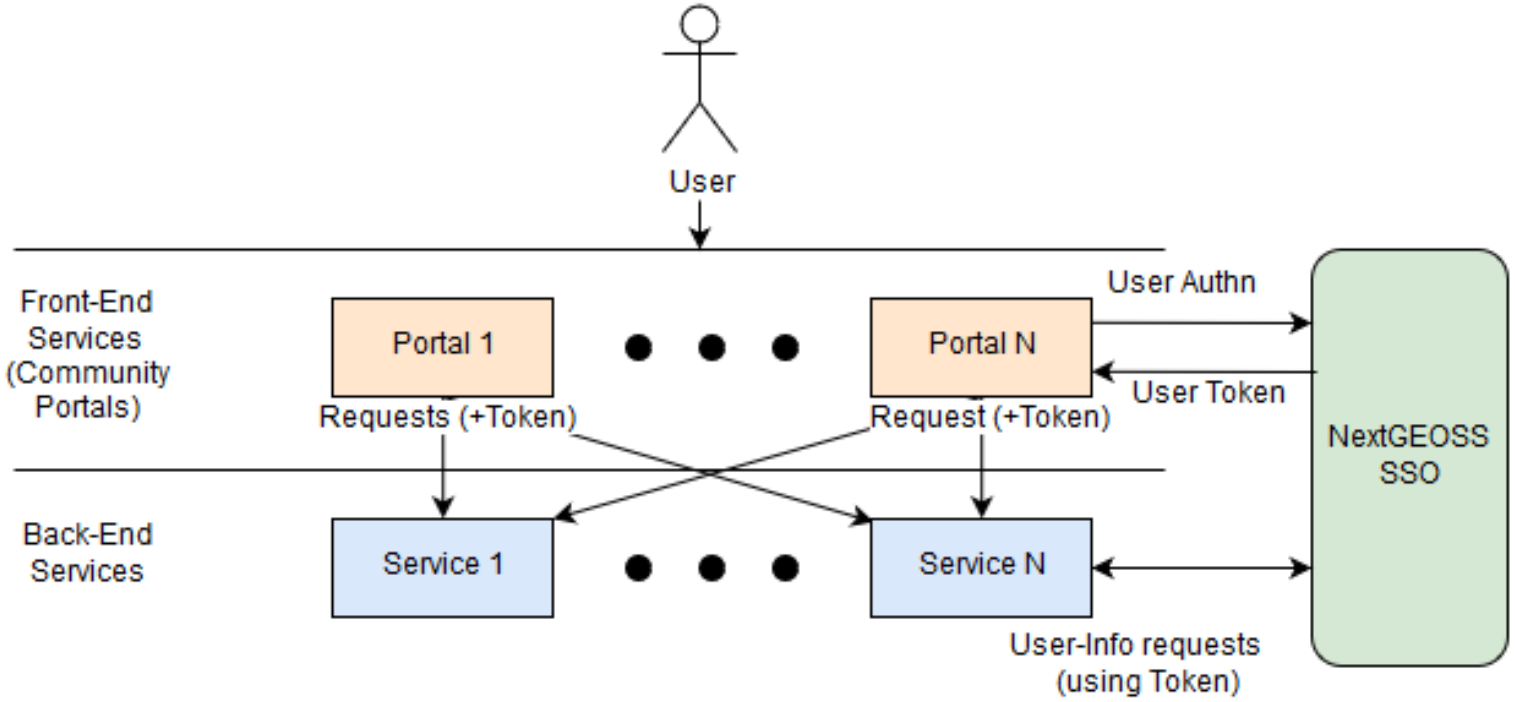


Access rights to services are customized per service provider!

Apps/Services Integration View

User Management serves the integration of NextGEOSS services (i.e. Data Providers, Data Processing, …) in Community Portals based on:

- Authentication: For allowing user login into the Community Portals with SSO
- Authorization: For allowing to restrict user access to resources (data and services)



CP Authentication approach

Community Portals and Services share a common pool of users managed by NextGEOSS UM

For that, NextGEOSS Community Portals require:

- Register and Log-in page that will redirect users to NextGEOSS SSO
- Landing page (callback URL) to receive users already authenticated
- Interaction with NextGEOSS API Endpoints

CP Authentication Methods Demo

NEXTGEOSS
Contributing to the Vision of GEO

NEXTGEOSS

CLIENT APPLICATION

loginRequest

client_id	@!5409.5FE2.395B.B7F2!0001!0A42.EA33!0008!FAF7.7779.B186.4F3B
redirect_uri	http://nextgeoss-sso.deimos-space.com:5000/login-callback.html
response_type	id_token token
scope	openid profile geoss_user uma_authorization uma_protection
state	60642212671241a5bd82c68fa94e69de
nonce	0f1b12da0e714c6aa65b85c98516d1de

AUTHENTICATE

NEXTGEOSS

HOME CONTACT US

USERNAME

PASSWORD

LOGIN

Forgot your password?
Need a NextGEOSS account? Register!
Make sure to read and accept our Privacy Policy and Terms of Service

NextGEOSS is currently on its Alpha version. Please contact us if you experience any issues.

NEXTGEOSS

USER MANAGEMENT CLIENT CALLBACK

loginResponse

id_token	eyJraWQiOiJlODgxYzg0MS0xZGIwLTRiOTktYTRmMS0xMjYxZmM0OTdmZTUiLCJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJodHRwczovL25leHRnZW9zcy1zc28uZGVpbW9zLXNwYWNlLmNvbSIsImF1ZCI6IkAhN
	5xyT4dz0G266QhK1dqh7IwOsAQVeLoUvY6bMXbYZb3HRdIUyxgMaDZbOvXiYd2LoUabSQ_QSfX2qPdc51WhGs1I8encyJJoJs1b1PicpBWGbV3byR7zbn2d6pvDwzYy5vws3kvTG9p8P0JDyCjVYUT0vsotQwTiGvm6eEM_
session_state	3a0ee1fe-447b-478b-99f2-0ff7da440dd9
access_token	49f43ff6-a973-42f5-9d42-1bdf3be09754
token_type	bearer
scope	geoss_user+openid+profile+uma_protection+uma_authorization
expires_at	1496653692

profile

auth_time	1496652665
oxValidationURI	https://nextgeoss-sso.deimos-space.com/oxauth/opiframe
oxOpenIDConnectVersion	openidconnect-1.0
sub	3Gg89Zuvo2eAJzsm9NixNPSqr17zOUYGoNLtBO0Af_E
geoss_user	true
user_name	jjdp
name	Juanjo
given_name	Juan José
family_name	Doval

state

bar	15

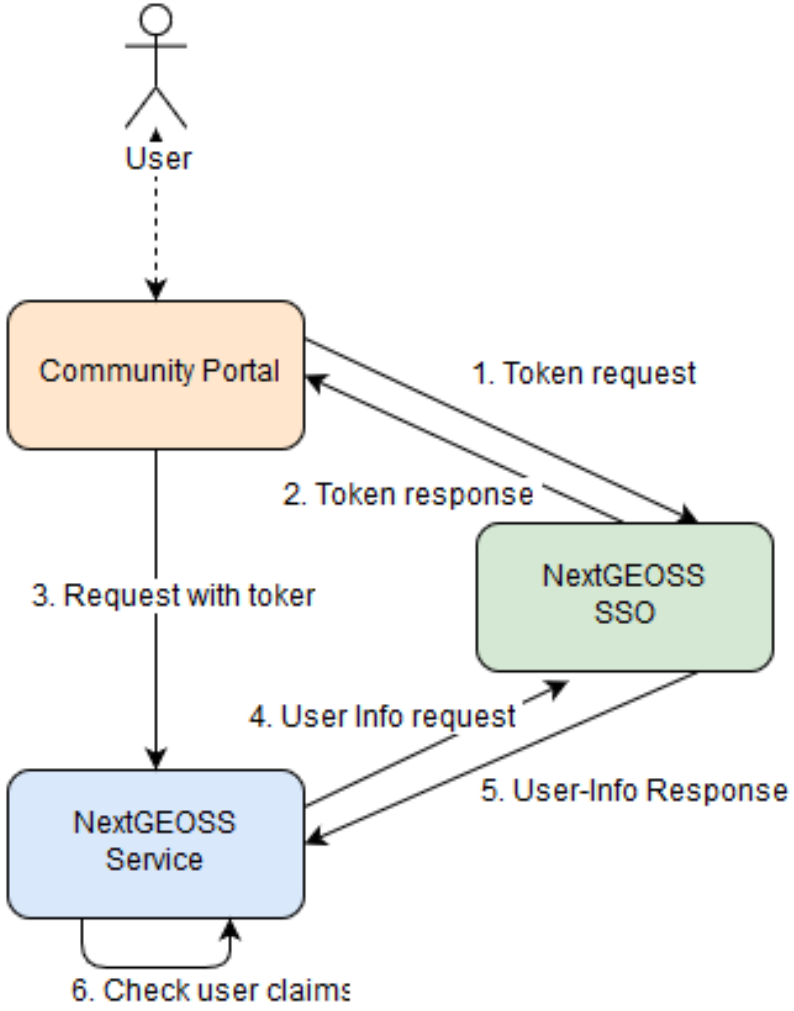
LOGOUT

Token & scopes Information
Profile Information & claims

Logout Operation

Services Authorization approach

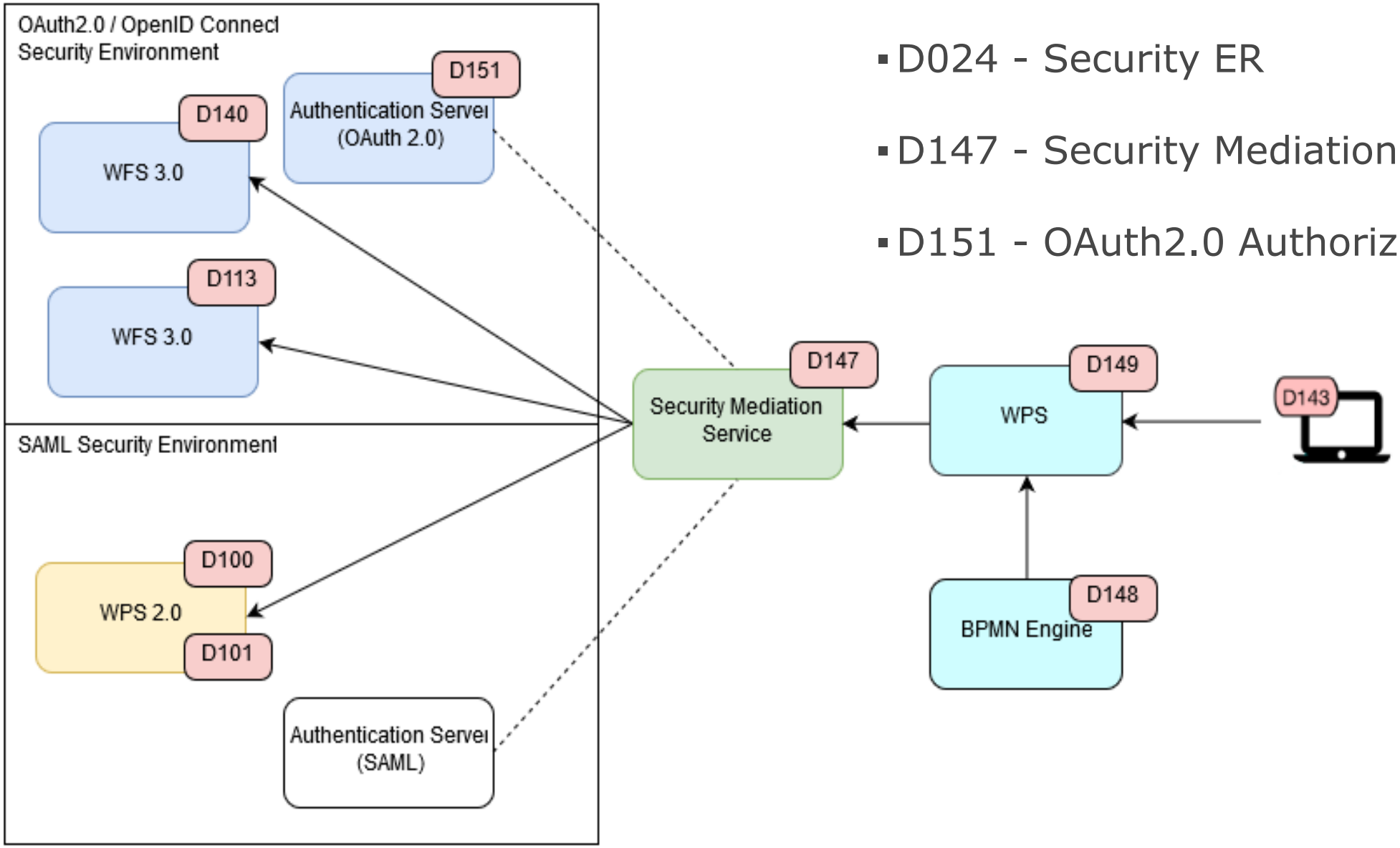
- Authorization is meant for securized NextGEOSS Services: providers, processing…
- Authorization is based on scopes set with default values. The administrator will be able to modify the claim values after request and approval.
- Scope authorization uses the user-info endpoint on NextGEOSS UM side



Related Activities

- OGC TestBed 14
- Proposal for Triple-A For Exploitation Platforms

OGC TestBed 14



- D024 - Security ER
- D147 - Security Mediation Service WPS
- D151 - OAuth2.0 Authorization Server

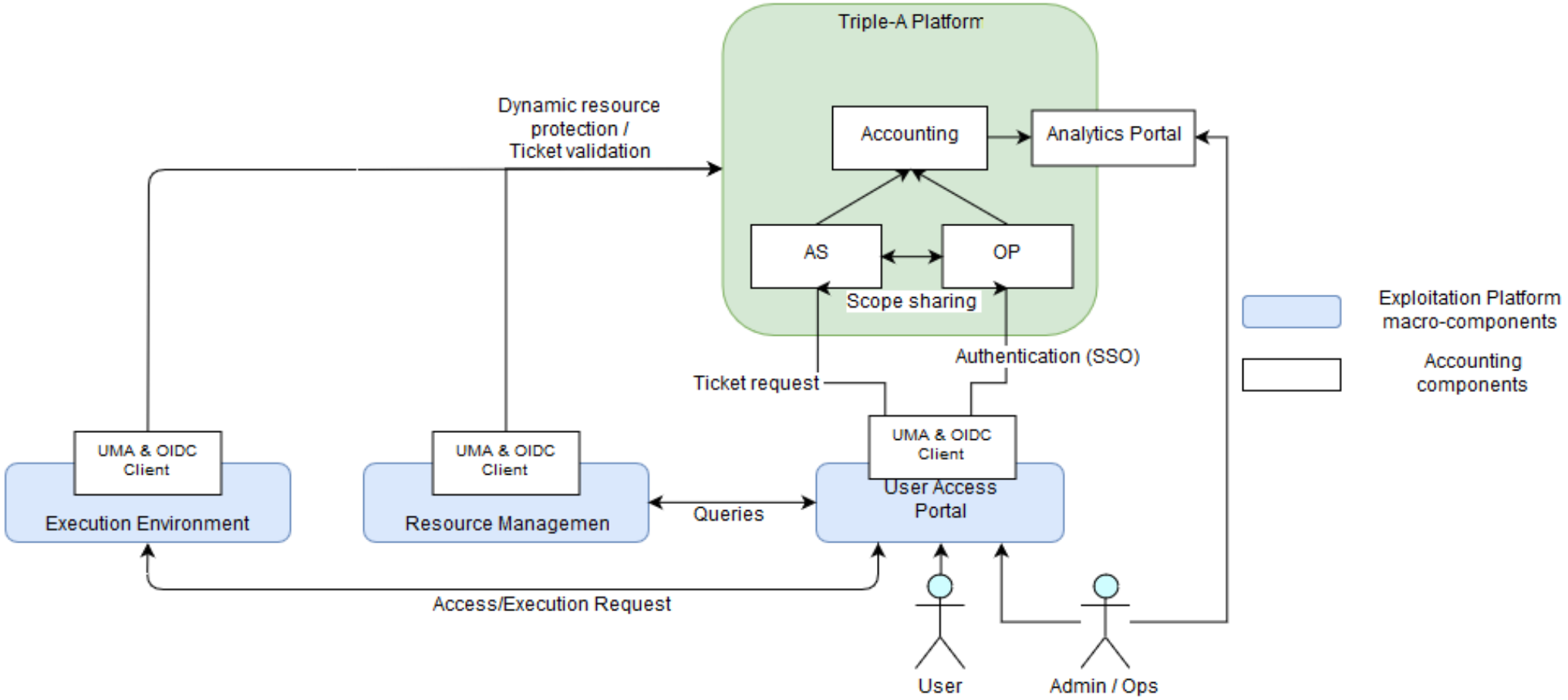
Triple-A For Exploitation Platforms

NEXTGEOSS
Contributing to the Vision of GEO

- Proposal to ESA for the EO SCIENCE FOR SOCIETY.
- Pre-operational demonstration of a Triple-A system (Authentication, Authorization and Accounting) for Exploitation Platforms using OIDC and UMA.
- The proposed solution addresses significant gaps on current AAA systems.
- Nowadays, most of the security environments use SAML standard solving the authentication and Single Sign-On (SSO) requirements and some of them use XACML for authorization managing it at application/service level but are not able to have centralised trace of user access that allows accounting.

Triple-A For Exploitation Platforms

- Focus on enabling accounting of usage for each user, applications and resources but also aims to reduce the development and integration impact on the Exploitation Platforms applications/services and users allowing centralized authentication and authorization with SSO and social login through OIDC and UMA standards.



Thanks!

- Questions ?