User Management

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

NextGEOSS, April 2018
Agenda

• Introduction

• User Management

• Roadmap

• Related Activities
Introduction

NextGEOSS

• High-Level Architecture
DataHub harvest and register data, providing links to original sources

Discovery Enablers empower search on DataHub from users

Access Enablers allow community hubs to create data buckets for access

Enhanced distributed gateway from research and operational infrastructures

Processing Enablers allow community hubs to deploy distributed ICT technologies

Publishing Appliances deliver to the community hubs processed results

Community Portals register selected products and services to GEOSS
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](https://eo-sso-idp.eo.esa.int), NASA-[https://urs.earthdata.nasa.gov/](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
  - Initiating user's login session (√)
  - Not responsible for collecting user consent (×)
  - High-security identity tokens (SAML only) (√)
  - Distributed and aggregated claims (×)
  - Dynamic introduction (OpenID only) (√)
  - Session timeout (×)

- OAuth 2.0
  - Not responsible for session initiation (×)
  - Collecting user's consent to share attributes (√)
  - No identity tokens per se (×)
  - No claims per se; protects arbitrary APIs (×)
  - Client onboarding is static (×)

- OpenID Connect
  - Initiating user's login session (√)
  - Collecting user's consent to share attributes (√)
  - No identity tokens per se (√)
  - Dynamic introduction (√)
  - Session timeout (in the works) (√)

Authentication/Authorization viewpoint

UMA
- You can grant access to apps operated by anyone
- You control access to a variety of protected resources
- You can grant access by setting policies and terms ahead of time
- The authorization function is standard and centralizable

OpenID Connect
- You achieve federated single sign-on and login-time attribute exchange
- You control access to claims about you

OAuth 2.0
- You grant access by consenting to terms at run time
- You can grant access to apps operated by you
- The authorization function is local to protected resources
- Apps can use a variety of access token types
- You control access to web APIs
Architecture and Protocols

Based on claims/scopes
<table>
<thead>
<tr>
<th>#</th>
<th>Key Performance Indicator</th>
<th>Definition of indicator</th>
<th>Type of data required</th>
<th>Source</th>
<th>Baseline at start of NextGEOS</th>
<th>Target at the end of NextGEOS</th>
<th>Frequency of Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>T5.4.1</td>
<td>Functionality: Management of federated entities (Identity Providers)</td>
<td>Number of entities in the authentication federation including social network</td>
<td>List of entities in the authentication federation, including Identity providers from social network services (Google, Facebook, Twitter, LinkedIn) and from GEDSS-related institutions (ESA, NASA)</td>
<td>User Management configuration files</td>
<td>0</td>
<td>KPI value: 6+ (4+ at EP-1, 5+ at EP-2, 6+ at EP-3)</td>
<td>Weekly</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>KPI percentage = (entities_integrated/6) * 100</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T5.4.2</td>
<td>Usability: Authentication performance</td>
<td>Time to login</td>
<td>Login messages with dates</td>
<td>User Management log files</td>
<td>0</td>
<td>KPI value: &lt;time to login&gt;</td>
<td>Weekly</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>KPI percentage = count(time_to_login&lt;2secs) / count(number_logins)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T5.4.3</td>
<td>Adoption: Number of registered users</td>
<td>Number of users in the Persistence Storage</td>
<td>List of registered users within the NextGEOS user management system</td>
<td>User Management persistence database (LDAP)</td>
<td>0</td>
<td>KPI value: 100+ (cumulative)</td>
<td>Weekly</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>KPI percentage = (entities_integrated/100) * 100</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T5.4.4</td>
<td>Adoption: Number of authentication requests, successful</td>
<td>Number of authentication requests, successful</td>
<td>Login messages with authentication information</td>
<td>User Management log files</td>
<td>0</td>
<td>KPI value: 30+ (5+ at EP-1, 15+ at EP-2, 30+ at EP-3)</td>
<td>Weekly</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>KPI percentage = (entities_integrated/30) * 100</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T5.4.5</td>
<td>Adoption: Number of integrated GEOSS Client Applications</td>
<td>Number of integrated GEOSS Client Applications</td>
<td>List of Client IDs / Applications</td>
<td>User Management log files</td>
<td>0</td>
<td>KPI value: 20+ (cumulative)</td>
<td>Weekly</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>KPI percentage = (entities_integrated/20) * 100</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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!
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)
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 is currently on its Alpha version. Please contact us if you experience any issues.
• 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

▪ 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.
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?