OGC Innovation Program
Testbed-14

Security Tasks

Héctor Rodríguez

Demo Day
January 2019

OGC®
Making location count.

deimos
elecnor group

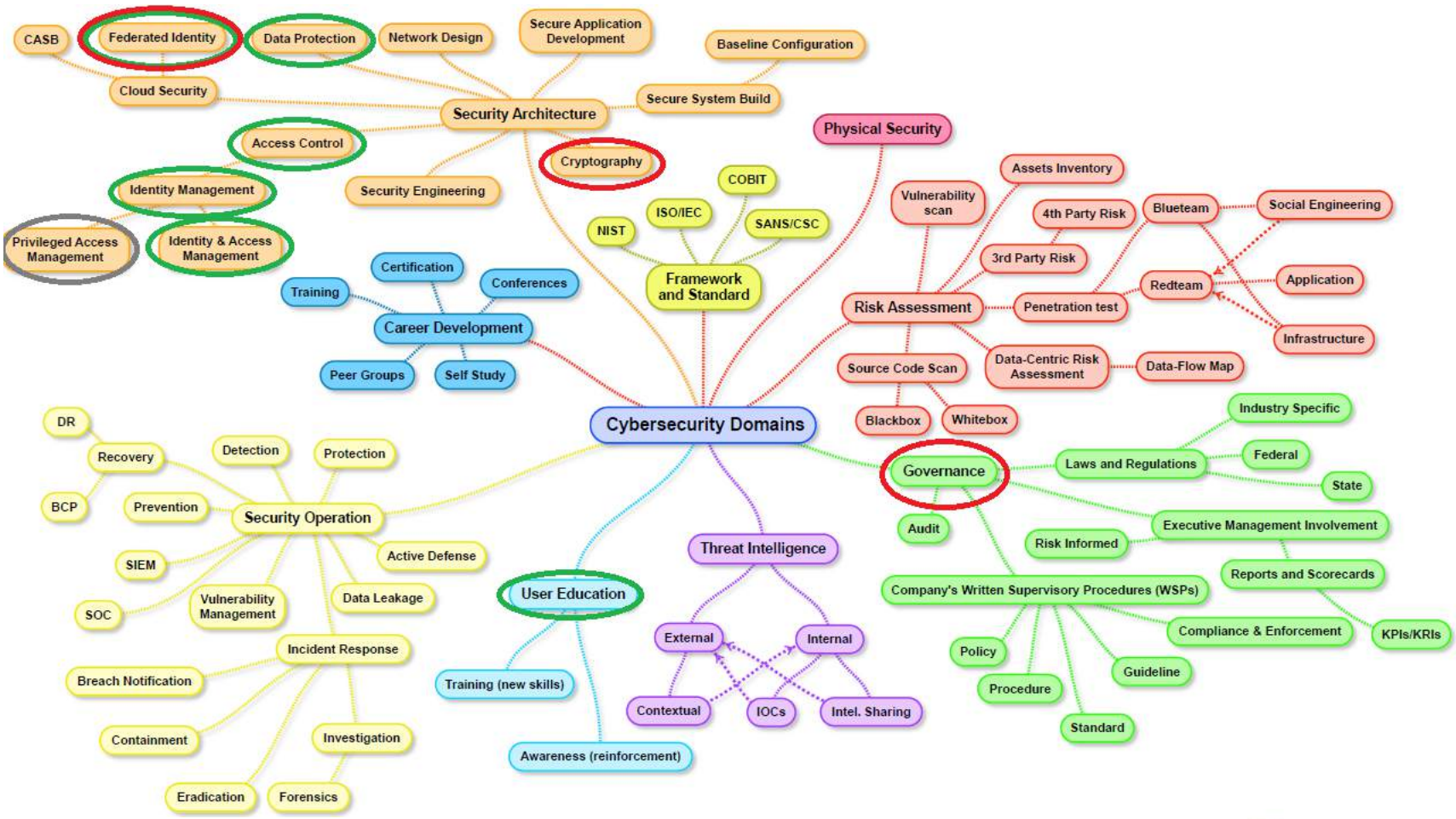
Overall activities

- Provide a clear view on the topic of Security for Spatial Data Infrastructures
- Coordinate and document all aspects related to the Security Task
- Collect security related results and include an extensive security discussion for the following items:
  - D147 – Mediation Service
  - D151 – Authorization Server
  - D021 – Next Generation Web APIs – WFS 3.0 ER
  - D023 – Federated Clouds ER
  - D026 – BPMN Workflow ER (originally Workflows ER)

OGC®

deimos elecnor group

A disclaimer regarding“Security”



Security Mindmap - Henry Jiang (Security expert for Bank of America)

Work Accomplished

- **State-of-the-art analysis on the security topic**, covering and comparing standards and how they fulfill security requirements.
- Design the **Authentication and Authorization server** based on OAuth2.0 and OpenID Connect and the interfaces with clients and services such as WFS 3.0.
- Design the **Mediation Service** for allowing access from other security environments.
- Interactions with the **Workflows and Federated Clouds** section of this program, aiming at more mature security architectures, within so called “Administrative Domains”.
- Work is documented in the **Security ER** containing also an Integration guide for developers.

OGC®

deimos elecnor group

State-of-the-art analysis on the security topic (I)

- Testbed-14 Security ER provides an **extensive state-of-the-art analysis, identifying key needs and technologies** that could enable the desired functionality

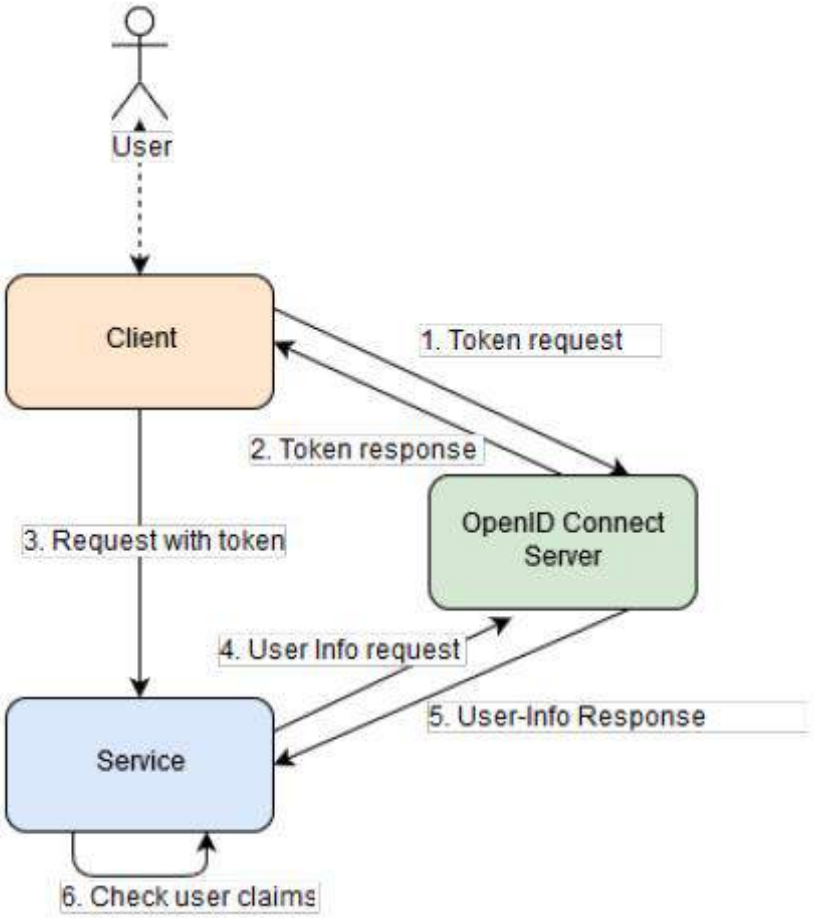
- **OpenID Connect and OAuth2.0** are used in order to reduce the development and integration impact on applications, services and users (while also allowing centralized authentication and authorization with Single Sign-On).

OGC®

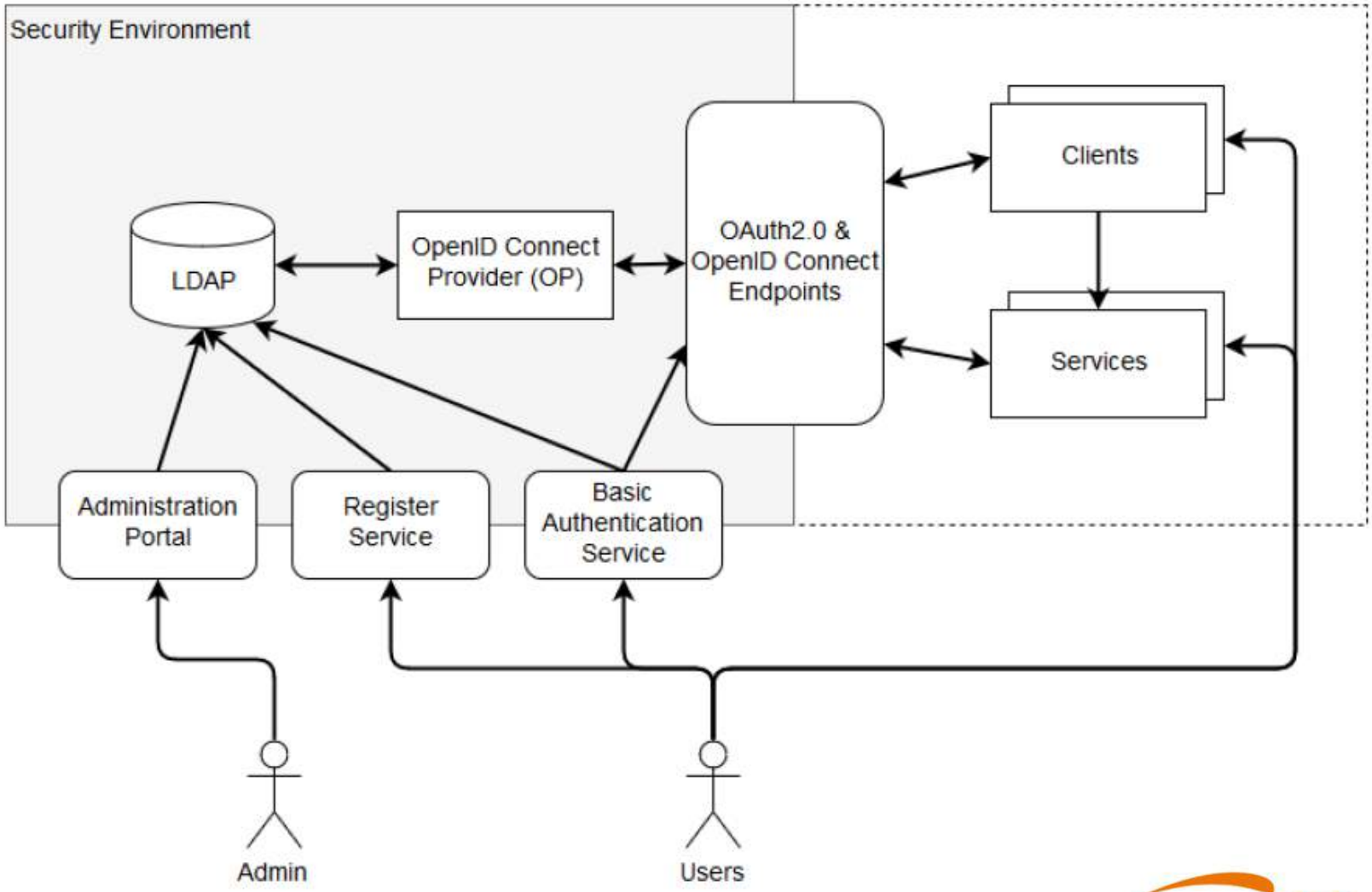
deimos elecnor group

State-of-the-art analysis on the security topic (II)

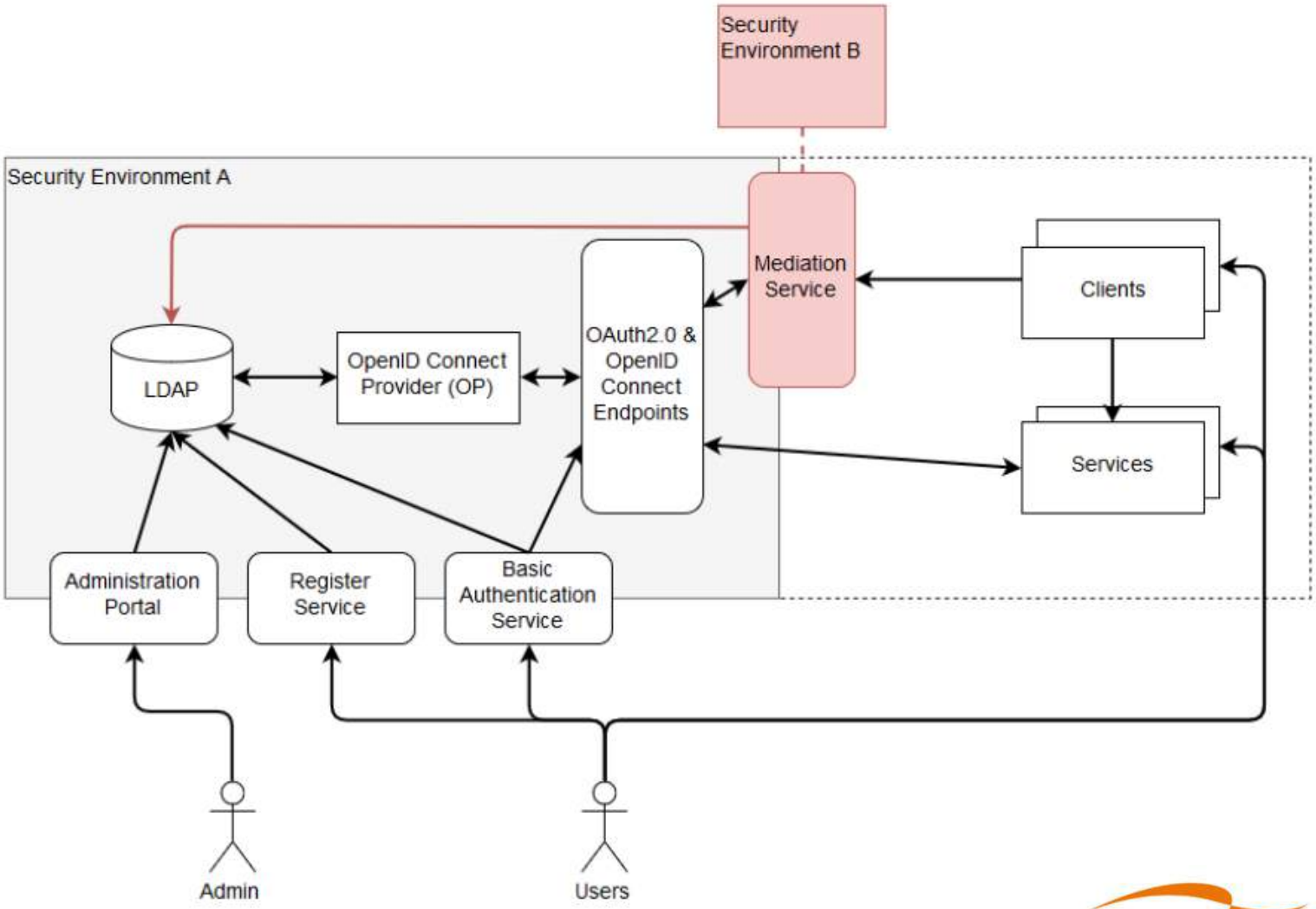
- Testbed14 focuses mainly on the usage of OAuth2.0 and OpenID Connect as security standards.
- OAuth2.0 / OpenID requires the usage of tokens as a mean of identifying users.
- Clients need to acquire a token (methods discussed on the ER)
- Services need to validate token and extract user information



Authentication and Authorization server: Design



Mediation Service: Design



Workflows securitization

- During this Testbed a NextGen client made use of the security infrastructure in order to provide BPMN powered execution workflows.

- After a successful securitization on a basic level, two main issues were raised:
  - Difficulty in the application of granular authorization for access to resources.
  - Secured relaying of information within the workflow

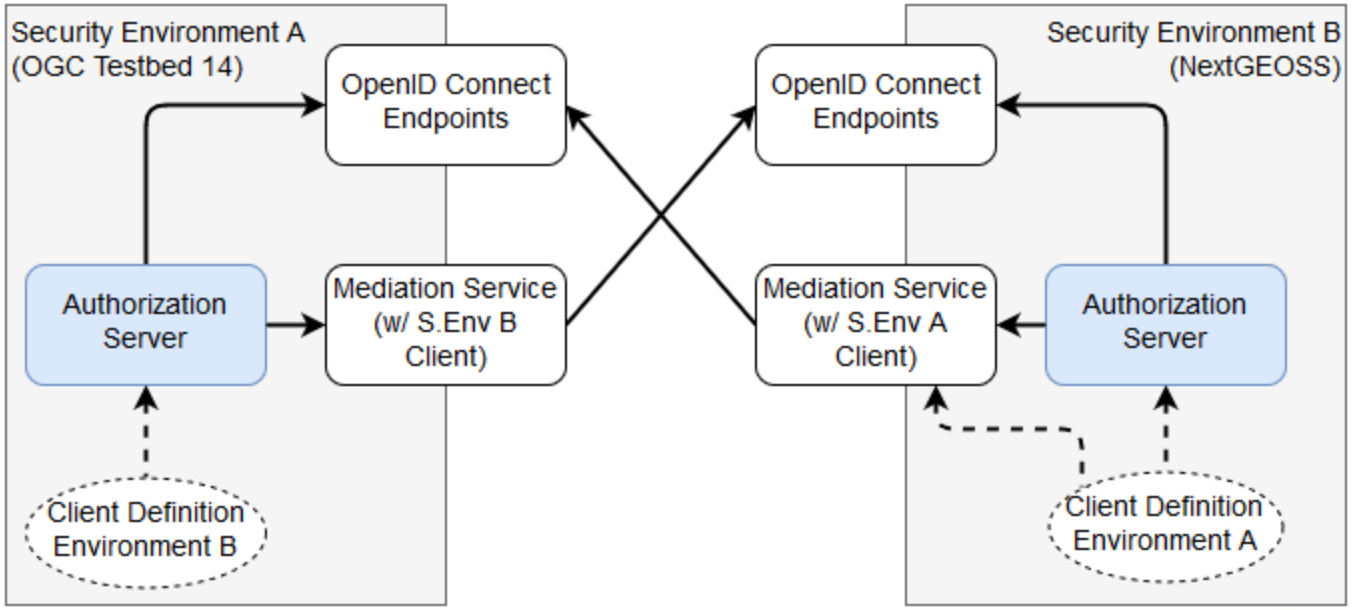
- Workflows can greatly benefit from the usage of UMA in order to protect generation, storage and access of processed data.

OGC®

deimos elecnor group

Federated Clouds

- A simple case of **two-way federation with NextGEOSS** has been demostrated during this Testbed.
- This served as a baseline for a critical review by the **Federated Clouds ER**. Main objective: to **identify and analyze governance and resource discovery needs.**



Future Work on Security topic

- Demonstration of social network login
- Demonstration of SSO based on OAuth2 and SAML (i.e. eduGAIN)
- Demonstration of fine-grained authorization based on OIDC or UMA standards (PEP/PDP adaptations)
- Demonstration of fine-grained accounting based on UMA standard
- Analyse and prototype the usage of the Client Credentials and Resource Owner grants
- Utilize JSON Web Tokens for propagation of user claims
- Design a Federation Manager capable of allowing management of resources on the owner side in order to facilitate solving governance issues

Thank you!

OGC®
Making location count.

deimos
elecnor group