ESA EO
Federated Identity Management Activities

Albrecht Schmidt
ESA/ESRIN

4 April 2017

Albrecht.Schmidt@esa.int

Agenda

1. FIM Pilot: EO Data Service and Ecosystem
2. ESA EO - Copernicus Federation
3. Exploratory Activities

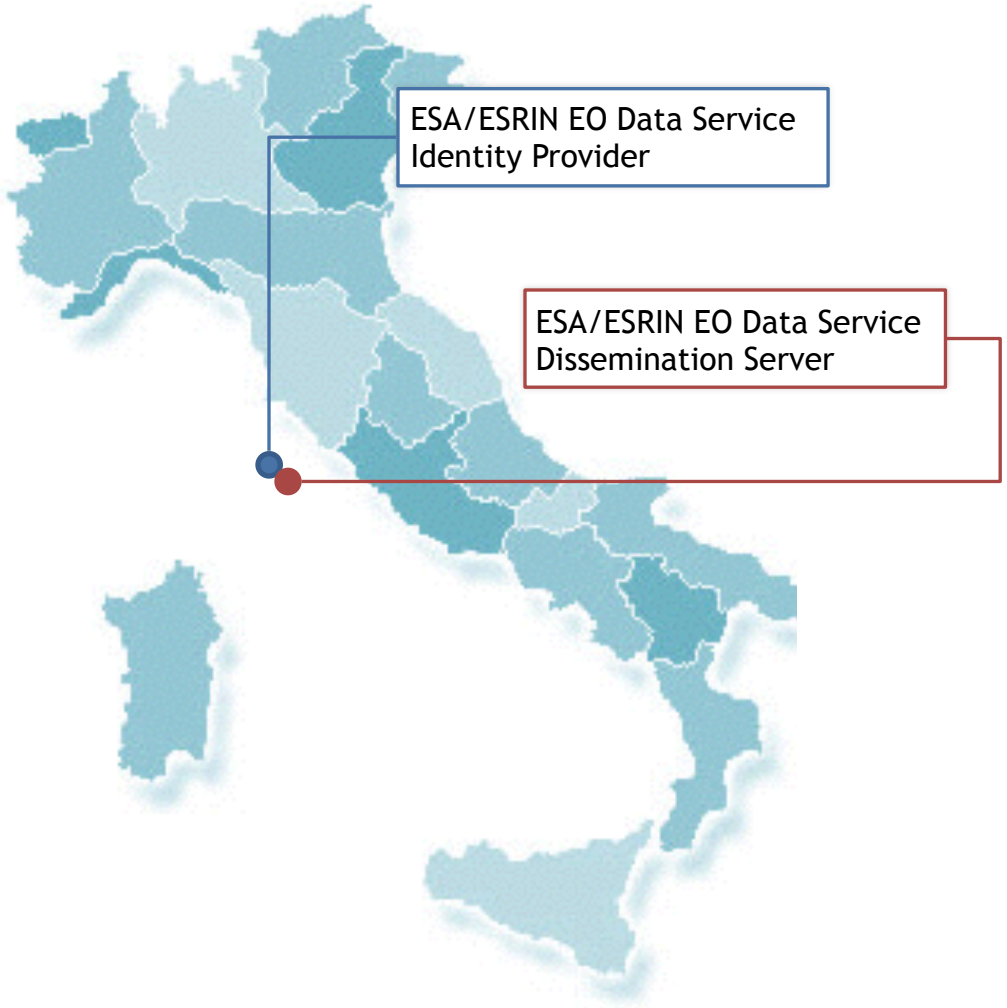
FIM Pilot

- The EO Data Service / EO IPT IDP is a pathfinder activity which implements a general architecture defined by GÉANT known as “FaaS”, Federation as a Service.
- The EO Data Service is a pathfinder Federated Identity Management infrastructure deployed on the EO Innovation Platform Testbed (IPT) in Poland. It is made of:
  - A vanilla Shibboleth dissemination service providing online access to Sentinel-2 MSI Level 1C products. Access is provided to authorised users only.
  - A vanilla Shibboleth Identity Provider providing authentication, user attributes and single sign-on functionalities. Only a selected set of users internal to the project is registered into this Identity Provider, for the time being.
  - Various tools for the management of the infrastructure (resource registry, metadata aggregator, discovery service).

FIM Pilot

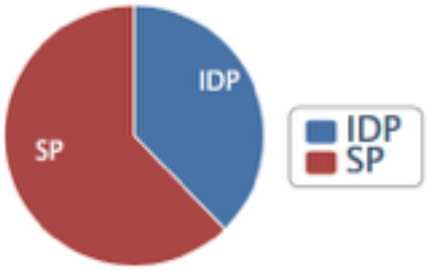
- The EO Data dissemination service is available both to local users and to federated users coming from IDEM and eduGAIN federations. Federated login is supported by a discovery service that allows:
  - Local users to login on the EO Data Service Identity Provider
  - Federated users to login on their home organisations' Identity Providers
- Deployment and integration with IDEM/eduGAIN federations
  - Mainly administrative and interoperability challenges
- A tool for co-operation with partners in the space sector:
  - Pilot with Eumetsat to let their users access the EO Data Service pilot
  - Pilot scheduled with DLR to evaluate IPT and CodeDE
  - Other partners such as CNES and NASA have been involved in discussions.
- Operation use, as defined usually by ESA, to be further consolidated
  - Refine elements such as SLAs, availability, operational procedures, configuration management, TRLs, …

IDEM/GARR Italian Federation Status (October 2016)

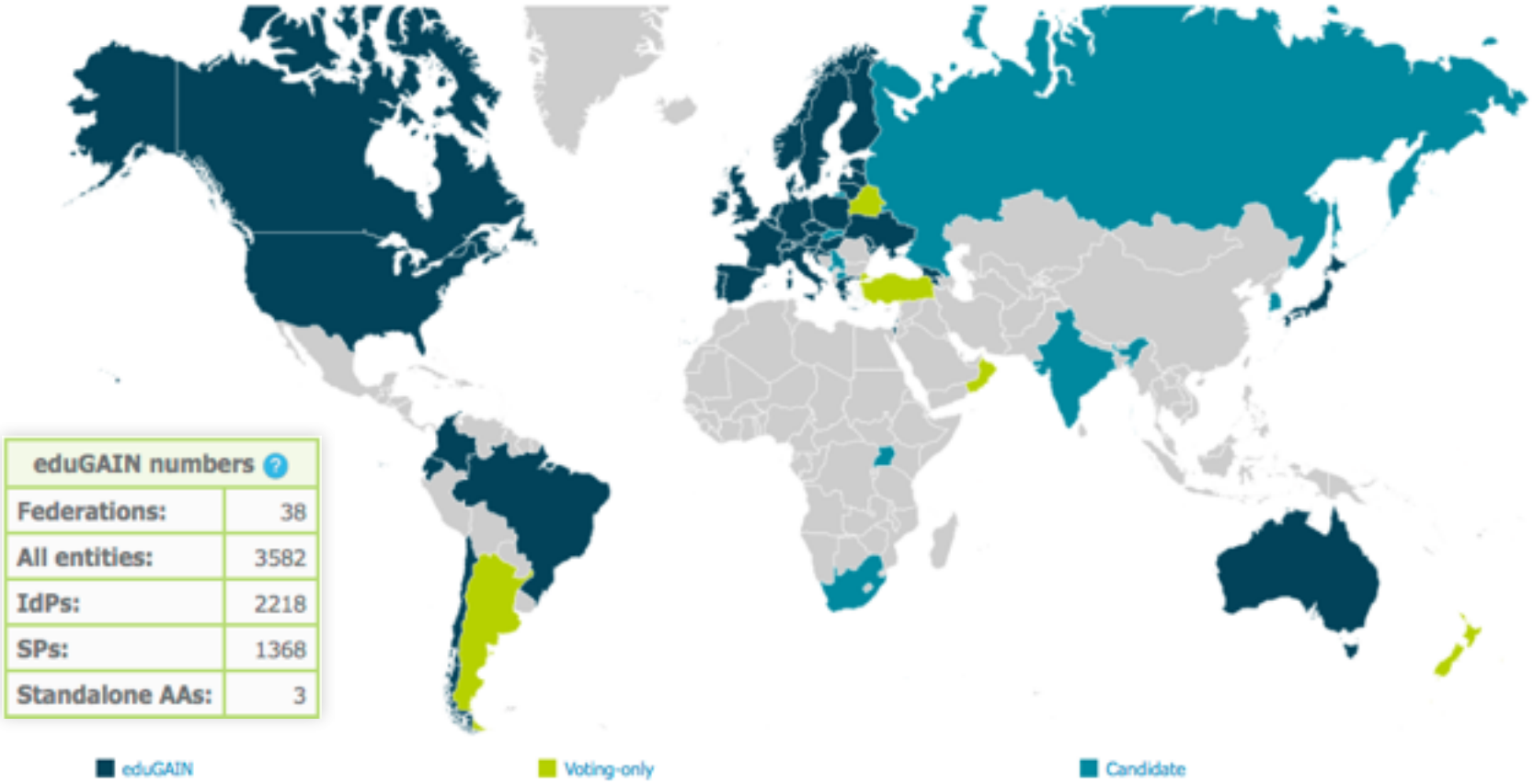


IDEM Summary

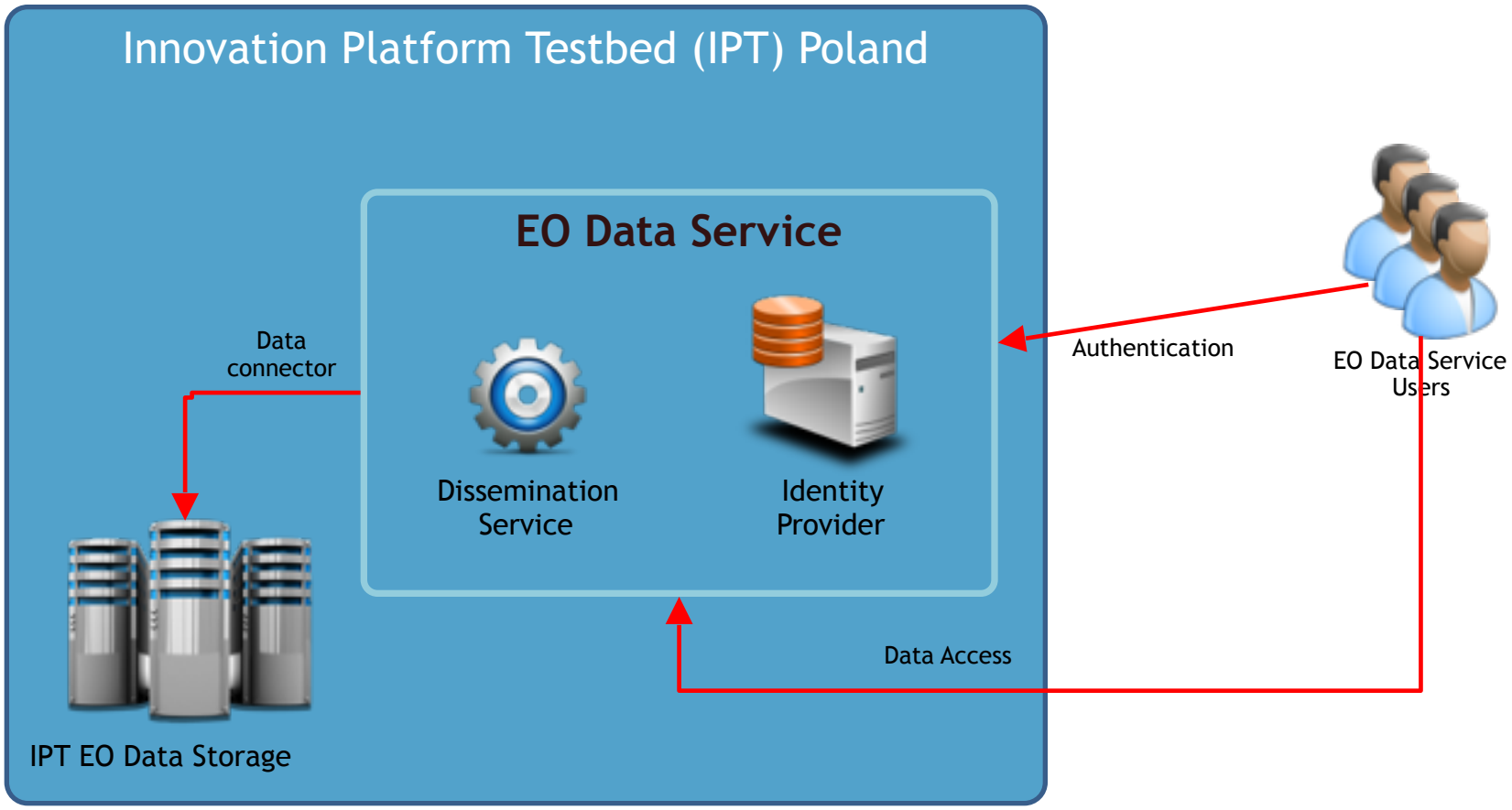
- All entities: 191
- Identity Providers: 72
- Service Providers: 119



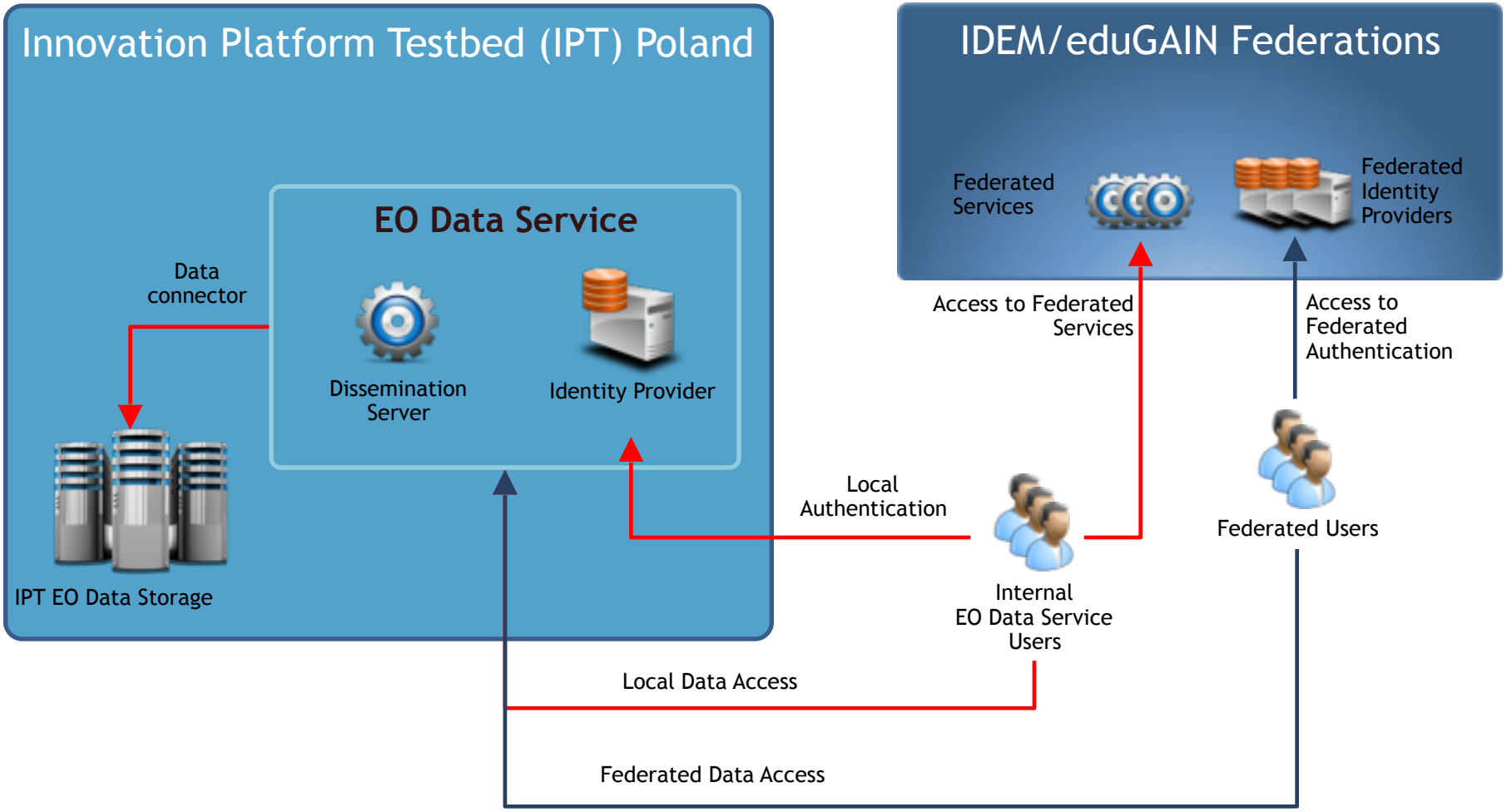
eduGAIN Federation Status (October 2016)



FIM Pilot: “EO Data Service”



FIM Pilot: “EO Data Service”



ESA EO - Copernicus Federation

- Since the ESA EO SSO software is used for both ESA EO and EC / Copernicus services, a federation between the two user communities would be natural.
- There are actual use cases which we desire to implement to support this for selected services, especially, uni-directionally.
- There are differences in the procedural setup of the two federation members.
  - However, level of trust or assurance is very high in such a controlled environment.
- Technically, the federation is based on Shibboleth / SAML and an Attribute Authority. Service providers will have to add a discovery facility to let users choose their home IDP.
- The development placed an emphasis on standard tools and configurations.

Current Exploratory Activities

- OAuth2 & OIDC:
  - Open ID Connect often seen as a more modern alternative to SAML.
  - The ability to generate, validate, pass on and consume tokens is the basis for machine to machine communication outside the browser world.
  - Preferred option would be to support parallel SAML and OIDC resource protection.
  - There have been experiments with ECP but little uptake.
  - There has been an STS/PEP-based solution which is used on the Copernicus side and proposed for the upcoming OGC Testbed 13.
- User Management Tools and Processes:
  - Anonymous users are principal community. Challenge to procedures, standards, and services.
  - Once they are registered, they might submit project proposals, for example, and get better know (higher level of assurance).

The End

Thank-You!