esa

ESA EO Federated Identity Management Initiatives

7th FIM4R

A. Baldi ESA: Andrea.Baldi@esa.int

M. Leonardi RHEA: M.Leonardi@rheagroup.com

ESA EO Identity Management Evolution

Authentication

Authorization

User Registration

Password Recovery

Secure Storage

User’s Administration

Security Enforcement

Authentication for Java applications

Easy Deployment

Auditing

Reporting

IT Redundancy

Internal ESA EO Federation:

Attribute Authority, ECP, STS

Short Term
Internal/Inter federation
ESA joining
IDEM/EDUGAIN

Mid/Long Term
Space Identity Management
Federation

Identity Management Infrastructure Enhancements

- Implementation of additional **auditing** and **reporting** services to monitor:
  - Infrastructure behaviour
  - Users' access
  - Data distribution

- AAI **Infrastructure redundancy** for **High Availability**:
  - Multiple IDPs/LDAPs distributed on geographical basis
    - Synchronisation of IDPs and LDAPs at transaction level
    - Load balancing to optimise the resources utilisation

Internal ESA EO Federation (1)

- Split of the current ESA EO domain into different administrative domains (e.g. ESA EO and Copernicus users communities):
  - No users duplication
  - Improvement of the users and services management

- User profile rationalisation and extension for implementing:
  - ESA SPs authorisation attributes for EO data dissemination services
  - Attributes required for the (inter)federations

Internal ESA EO Federation (2)

- Introduction of a ESA EO **Attributes Authority** in charge of:
  - Users' profile management
  - Authorisation attributes provisioning

- Introduction of a **Discovery Service** to support the identification of the Federation Identity Providers.

ECP - Enhanced Client or Proxy Profile

- EOLISA (ESA EO products discovery/download standalone application) currently uses a java "JCL" library to implement the EO-SSO authentication.

- ESA intents to replace the current JCL library with a standard ECP-based implementation for EOLI-SA.

- ESA wants to provide alternative applications (e.g. scripting applications in bash, perl, etc.) to allow users to download EO products via non-web applications.

- The Enhanced Client or Proxy profile is supported by the Shibboleth IDP.

OGC Best Practice

- The OGC - Open Geospatial Consortium has approved the *"User Management Interfaces for EO Services: OGC 07-118"* * document as a new OGC Best Practice.
- The document describes how existing specifications from W3C and OASIS can be used in combination to pass identity information to OGC Web services.
- The document assumes the use of a **Security Token Service** for the implementation

* https://portal.opengeospatial.org/files/?artifact_id=40677&version=2:

Relevant Scenarios from the OGC Best Practice

- The document covers both **B2B** and **C2B** scenarios:
  - **B2B** - Business to Business Authentication & Authorisation via SAML 2 **Security Token Service** between systems.
  - **C2B** **-** Consumer to Business Authentication & Authorisation: Web SSO shall interact with B2B service authorisation environment based on SAML tokens.
- Some of the scenarios described in the document will be implemented to satisfy the requirements coming from the ESA EO FIM project

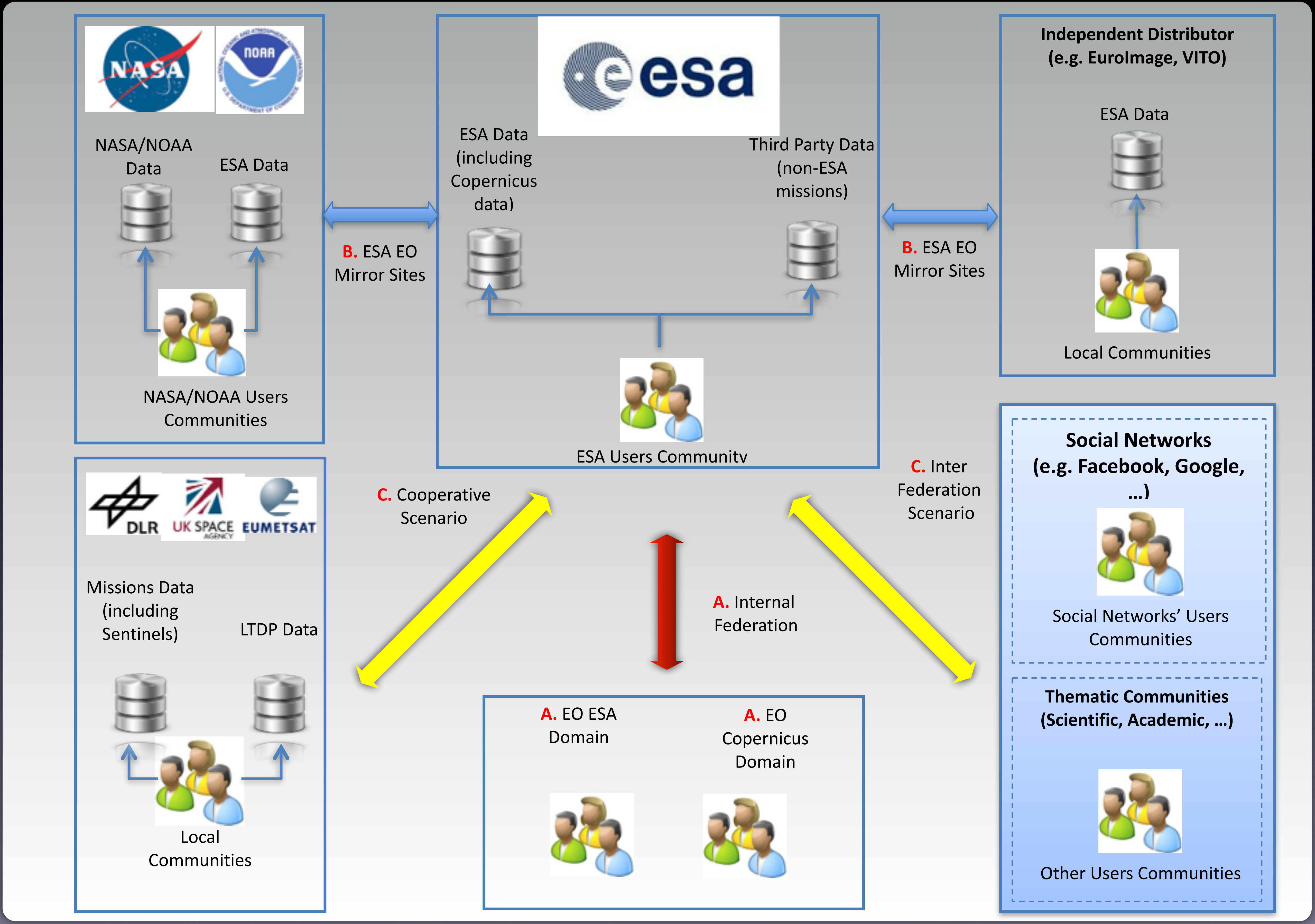
First steps towards the ESA use cases

- Re-organising ESA EO FIM Services
  - ESA EO Federation needs process, procedures and tools to be aligned with FIM best practise:
    - Detailed census of FIM components (IDPs, SPs)
    - Management of IDP and SP metadata, certificates, etc.
    - Rules and policies for the ESA EO Internal Federation

Use cases for ESA

- ESA EO Internal Federation (e.g. ESA Copernicus, etc.)
- ESA EO Mirror Sites:
  - ESA data distributed by 3rd parties (e.g.Nasa, VITO)
  - ESA distributing other organisations' data
- Cooperative Scenario amongst federation partners:
  - Sentinel data access
  - Cooperative LTDP access
  - Exploitation Platform
- Accepting Social Network Users (e.g. OpenID)

Federation Context



NASA/NOAA Data

ESA Data

NASA/NOAA Users Communities

B. ESA EO Mirror Sites

ESA Data (including Copernicus data)

Third Party Data (non-ESA missions)

ESA Users Community

B. ESA EO Mirror Sites

Independent Distributor (e.g. EuroImage, VITO)

ESA Data

Local Communities

Missions Data (including Sentinels)

LTDP Data

Local Communities

C. Cooperative Scenario

A. Internal Federation

C. Inter Federation Scenario

A. EO ESA Domain

A. EO Copernicus Domain

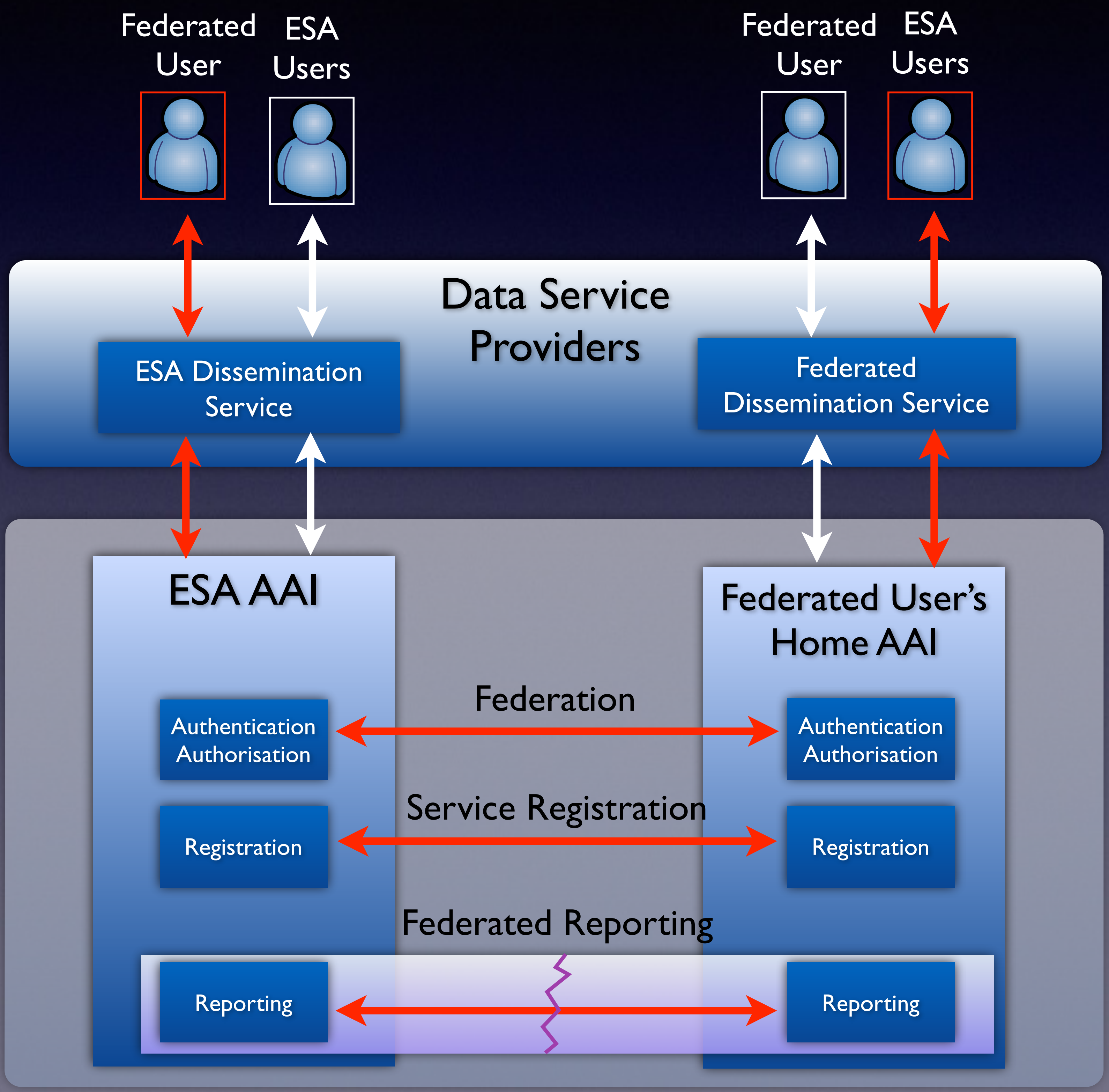
Social Networks (e.g. Facebook, Google, …)

Social Networks' Users Communities

Thematic Communities (Scientific, Academic, …)

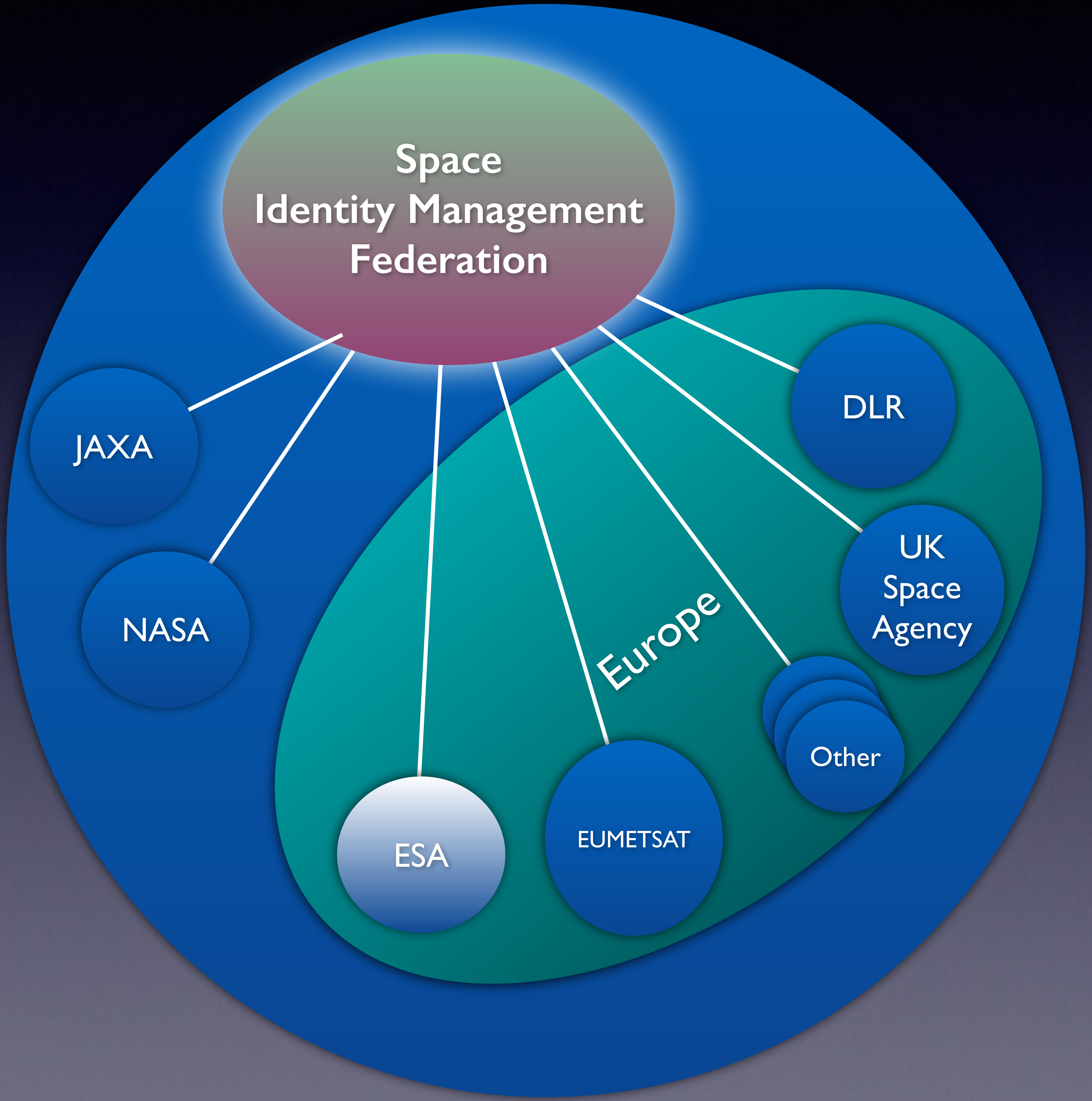
Other Users Communities

Cooperative Scenario



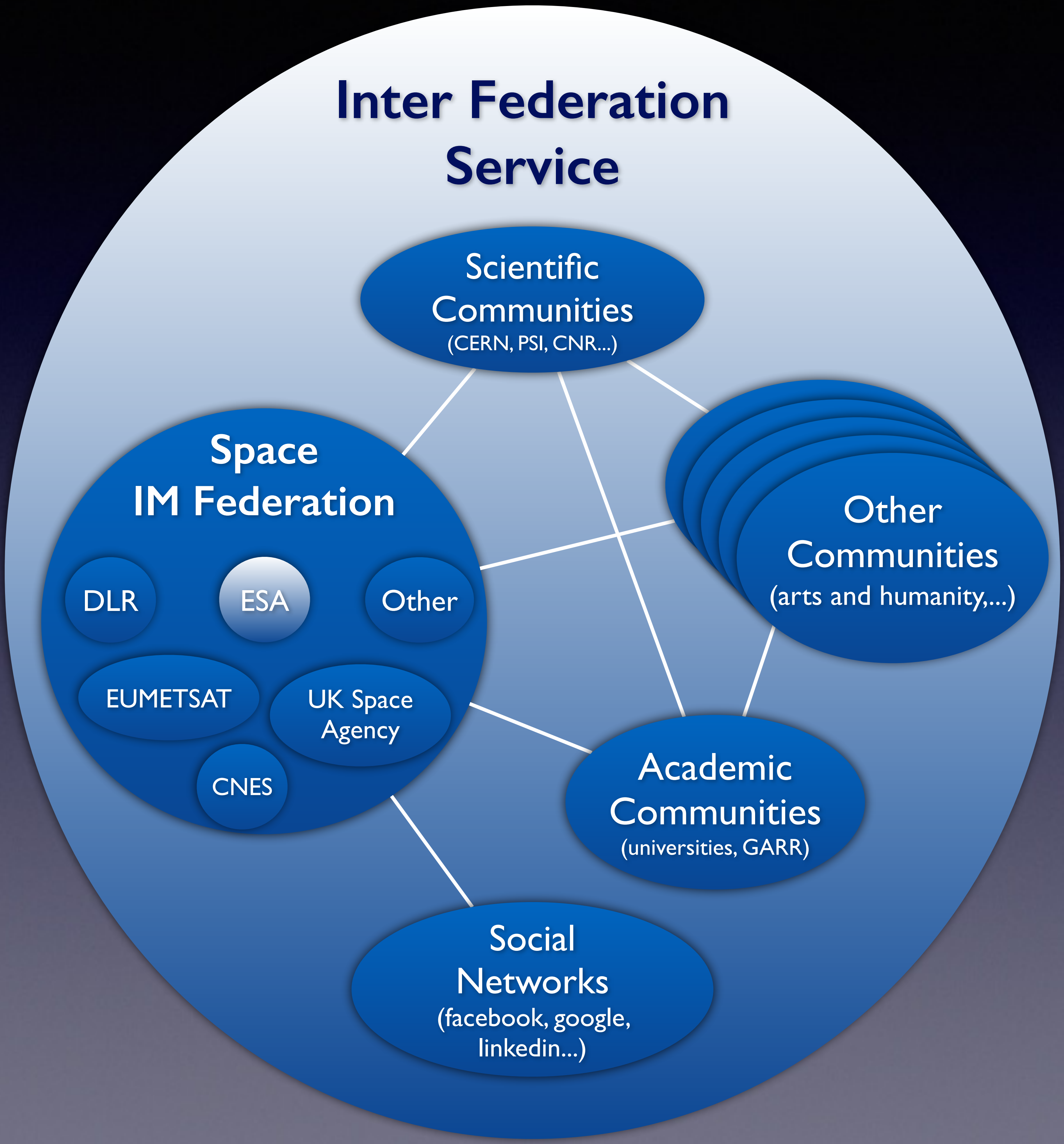
- Organisations provide their own data and services to any federation members
- Data Policy Agreements shall be established and implemented within the federation.
- Users registered at any federated organisation can access data of any other federated member (e.g. **Sentinel data**)
- Users always authenticate via their own organisation
- Users' access Reporting in agreement with federation policies

Space Identity Management Federation Context



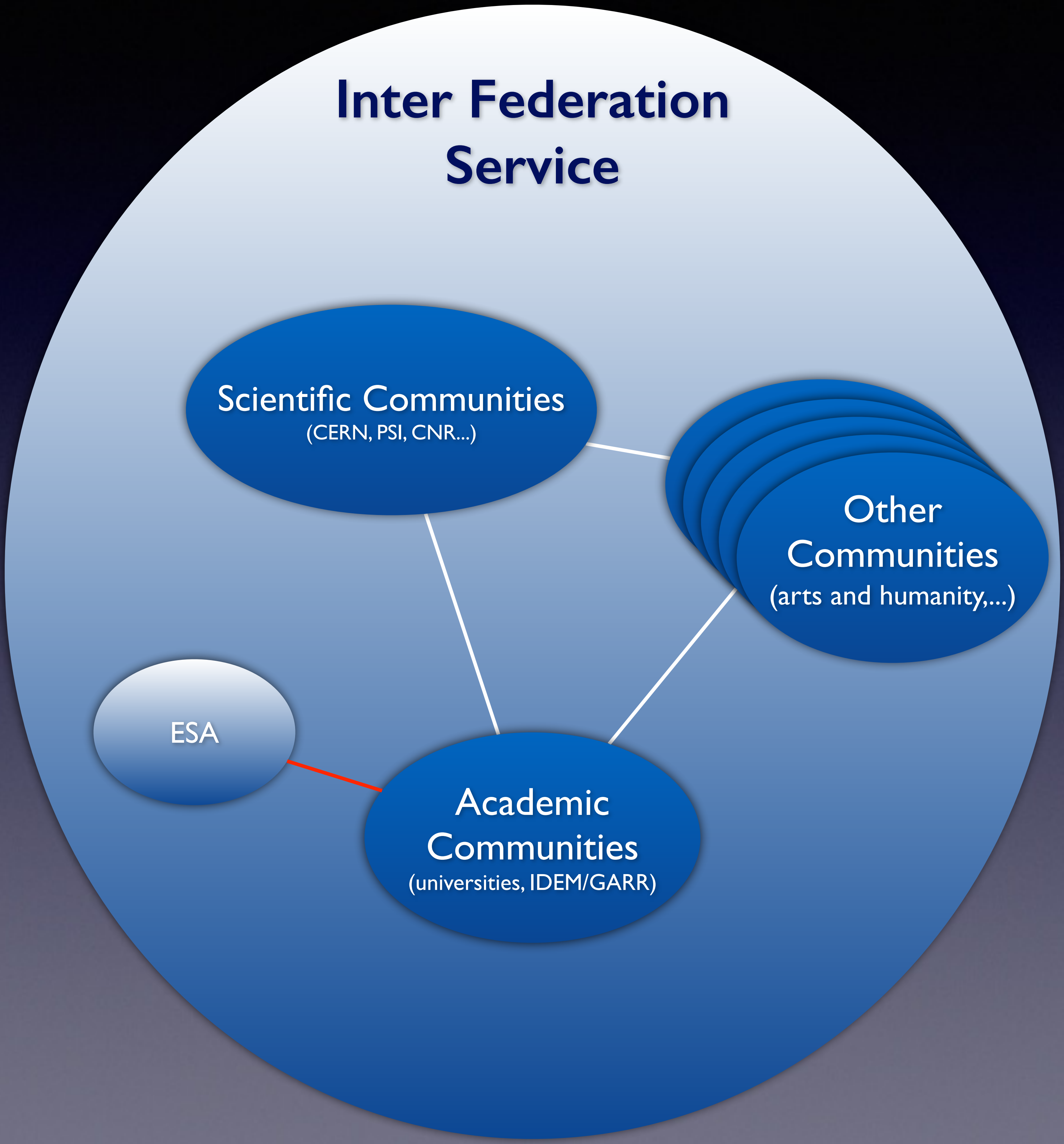
- Single Sign On for any service supplied by federated space organisations
- Priority is European Organisations
- **Interoperability** of users' among different space organisations
- Easy access to data and services offered by federated space organisations
- Expanding users access to EO services with no overhead for user management
- Assure the level of trust among space federation partners
- Shorter time-to-market for new services deployment within the space federation
- GSCB as forum for Space federation discussions

Inter Federation Context


Inter Federation Service
Scientific Communities (CERN, PSI, CNR...)
Space IM Federation
DLR
ESA
Other
EUMETSAT
UK Space Agency
CNES
Other Communities (arts and humanity,...)
Academic Communities (universities, GARR)
Social Networks (facebook, google, linkedin...)

- Extends the already mentioned federation benefits one level more by joining existing federations
- How to join:
  - Be a federation: **Space IM Federation**
  - Join an existing federation:
    - Scientific
    - Academic
- Social Networks
  - Users can access data with their google/facebook/linkedin accounts
  - Users don't need to remember their specific credentials
  - Level of trust not assured

Joining EDUGAIN Via IDEM



- Joining EDUGAIN
- ESA plans to join the Italian Federation (IDEM) in order to be part of EDUGAIN
  - Pilot project in place:
    - Kick off 30 April
    - Will connect:
      - A clone IDP
      - A data dissemination server SP
    - Test Scenario:
      - a selection of ESA user accessing community services
      - provide a sample of ESA EO data to EDUGAIN members
    - Goals:
      - assess ESA EO profile structure/ attributes and services to be interoperable.
      - Go in the exercise of becoming part of an inter federation
      - Be ready to have EO SSO Copernicus Domain ready for federation

What next?

- ESA is going to support user requirements via internal projects and collaborations with international partners:
  - Kick-off FIM internal project for completing the baseline for Identity Management Federation (30/April):
    - Design and implementation of new building blocks for FIM
    - Establish Internal ESA EO Federation (e.g. Copernicus, Multi Mission, Earth Explorer,s etc)
    - Build capabilities to join existing federations (e.g. IDEM/ EDUGAIN)
  - Establish technical contact points for preparing the Space FIM:
    - exchange technical information about AAI used by the participant organisations
    - discuss programmatic aspects of a Space FIM (e.g. rules ,policy, trust, framework, etc)
    - plan for an implementation.
  - Continue collaboration with FIM4R partners to share ideas/plans