eIDAS cross-sector interoperability

Christos Kanellopoulos

GRNET

eduGAIN SG

October 13th, 2016

Background information

- **2013 - STORK-2 collaboration (GN3Plus)**
- 2014-07 – Adoption of the eIDAS Regulation
- **2014-09 – eduGAIN – STORK-2 Profile comparison and interoperation scenarios (GN3Plus)**
- **2015 - Proof of concept pilot of the eduPEPS Proxy (GN4-1)**
  - Access an SP at GRNET federation using a spanish eID via the eduPEPS Proxy
  - Access a STORK-2 SP in Spain using an account at the GRNET VHO IdP via the eduPEPS Proxy
- **2015-09 – Uses cases involving eIDs for International Research Collaboration (AARC)**
  - Use of eIDS as a potential solution for Guest Identities
  - Use of eIDs for use cases that require high level of assurance
- 2015-11 – eIDAS Proxy production deployment at the MS
  - 2018-09 – Cross border recognition of eID means

Cross-sector interoperation with eIDAS

- **2016-07 – 1st meeting in Brussels between AARC, GN4 and eIDAS Reps**
  - Investigate the possibility of an interoperation pilot between eduGAIN and eIDAS
- **2016-09 – 2nd meeting in London (AARC, GN4, Internet2, eIDAS Reps)**
  - Draft proposal for an interoperability pilot between
  - 3 Use cases:
    - Use case 1: authenticate to eduGAIN service with eIDAS eID
    - Use case 2: authentication to an eduGAIN service where a higher LoA is required
    - Use case 3: registering at a university online with cross-border attribute provision
      [** This use case is only going to be a study and not an actual implementation]

Proposed time plan

- Preparatory phase [Nov 2016 - Dec 2016]
  - + Confirm pilot participants and use cases
- Alpha phase 1 [Jan 2017 - Mar 2017]
  - Develop testing process for each use case
  - Define interoperability architecture and standards
  - Analysis of potential security and fraud risks + Analysis of privacy and consent requirements
  - Analysis of potential legal issues
- Alpha phase 2 [Apr 2017 - Oct 2017]
  - Technical connectivity between eIDAS and eduGAIN
  - Use case 1: authenticate to eduGAIN service with eIDAS eID
  - Use case 2: authentication to an eduGAIN service where a higher LoA is required
  - Use case 3: registering at a university online with cross-border attribute provision [** This use case is only going to be a study and not an actual implementation]
- Alpha evaluation [Nov 2017 - Dec 2017]

Use cases

1. **The use of eIDAS eIDs in the context of academic research services.**

   The use case scenario is a researcher participating in an international collaboration, who will be accessing services available in eduGAIN using eIDAS eID assertions as a means of identifying herself. There is an important benefit here for eduGAIN as there are cases in which researchers do not have eIDs from an academic institution but may have access to national eID through eIDAS

2. **The use of eIDAS as a mean to access services that require higher LoA**

   The use case scenario is a researcher participating in an international collaboration (e.g. a Bio-bank), who will be accessing services available in eduGAIN using eIDAS eID assertions as a mean to elevate the LoA of the identity assertion. This is an existing problem for eduGAIN as there are no higher levels of assurance currently.

3. **The combination of eIDAS eID assertions and user attributes coming from a university**

   The use case scenario will mimic the user journey of an individual registering at a university in country B (eIDAS eID assertion- from IDPs) and asserting proof of their academic attributes from an institution in country A (attribute enrichment). The user will register to enrol at a university in country A by asserting an identity and additional attributes established in country B. It is noted that the US does not currently have a national eID service meaning that

   this element of the alpha will focus on user research rather than technical implementation aspects.

Next steps

- **Confirmation of pilot participants and use cases**
  - Confirmed participants: GRNET & SURFNET
  - Any other federation interested in participating?
- **Internal analysis and decision on the interoperation scenarios:**
  - Establish bridge/proxy at the national level?
  - A distributed bridge/proxy at the GÉANT/eduGAIN level?
  - eIDAS as an Identity Federation in eduGAIN?

skanct@grnet.gr

Thank you and any questions

GÉANT

Networks · Services · People

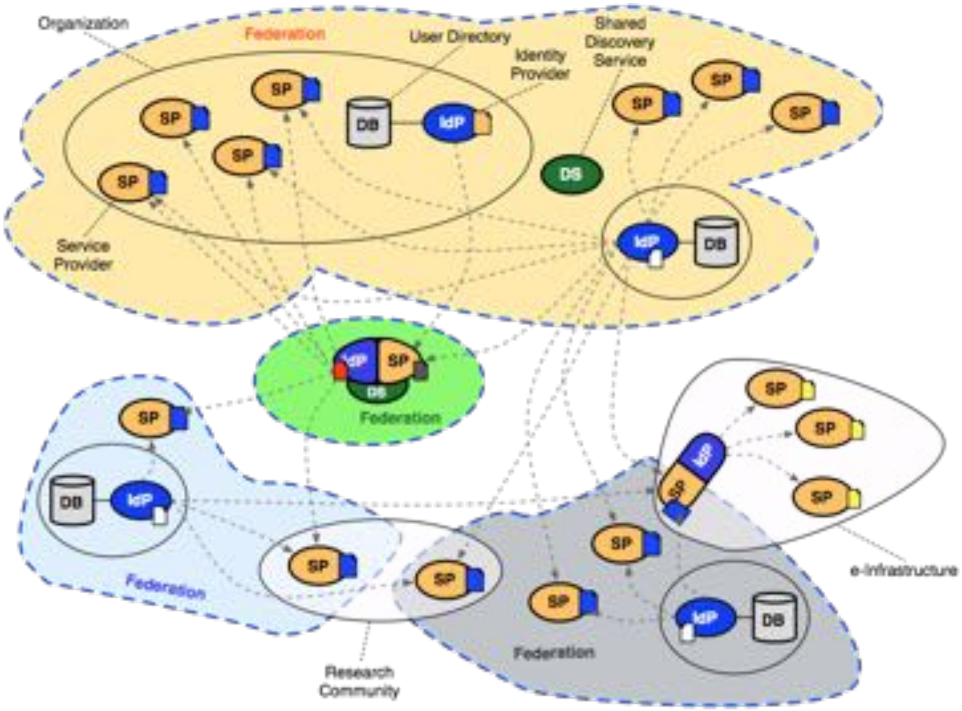
www.geant.org

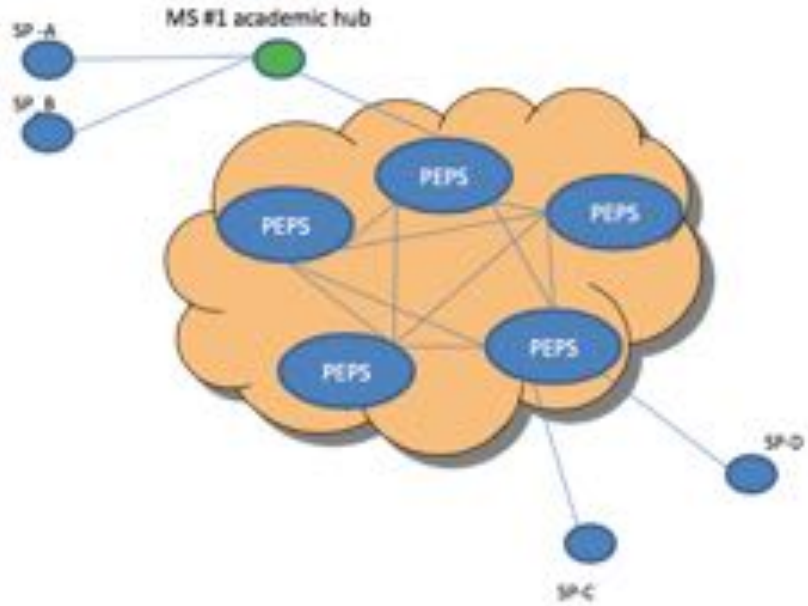
Background Material
eduGAIN – STORK2 Interoperability Pilot

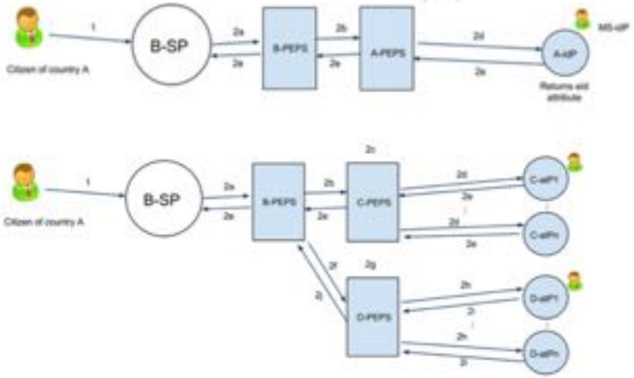
eduGAIN – STORK2 Interoperability Pilot

- Some similarities, but enough differences to hinder direct interoperability:
  - **SAML**
    - eduGAIN Federations are using the SAML2Int SAML profile
    - STORK is using STORKsaml, which has custom SAML extensions
  - **Attributes**
    - eduGAIN Federations use the eduPerson schema
    - STORK2 has defined attribute schemas for various verticals (including academia)
  - **Trust relationship**
    - In the eduGAIN Federations, Service Providers typically interact directly with the Identity & Attribute Providers.
    - In the STORK architecture cross-border authentication and attribute exchange goes through proxies that are operated at the member state level
  - **Levels of Assurance**
    - In eduGAIN Federations LoA is not used at the moment, but will be introduced soon
    - STORK introduces custom SAML2 extensions to communicate per attribute LoA
  - **Attribute Release Policies**
    - In eduGAIN Federations IdPs have very strict Attribute Release policies. FAM is considered as a privacy enhancing tool. Considerations about forced vs freely given consent
    - In the STORK pilot: Liberal attribute release policies based on user consent

eduGAIN – STORK2 High Level Architecture



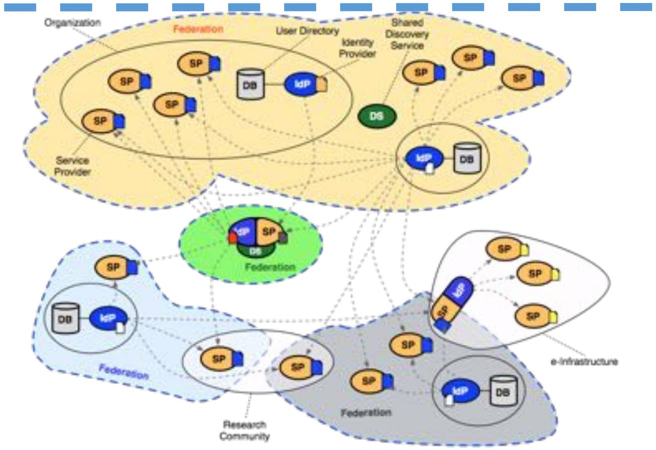


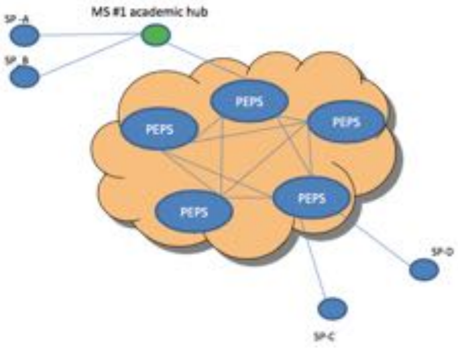


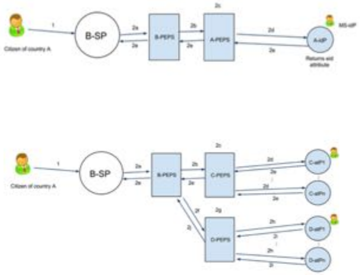
eduGAIN – STORK2 High Level Architecture

- SAML2 Interoperability Profile
- Full Mesh Federations and Hub and Spoke
- “Central” Metadata Service
- Dynamic Trust
- Attributes based on eduPerson
- Production infrastructure

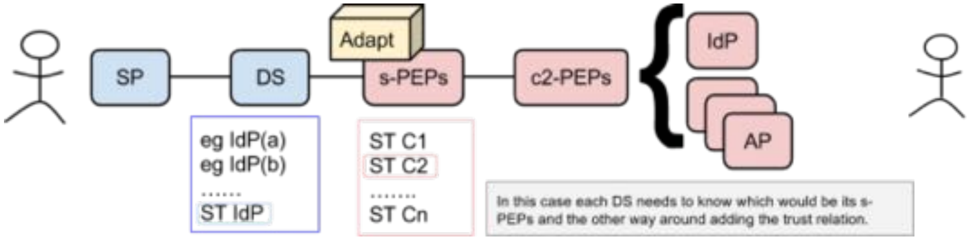
- SAML$_{\mathbf{STORK}}$ Profile
- Proxied architecture
- Static Trust between Proxies (PEPS)
- Attribute Authorities & Attribute Aggregation
- Levels of Assurance
- STORK defined Attributes (?)



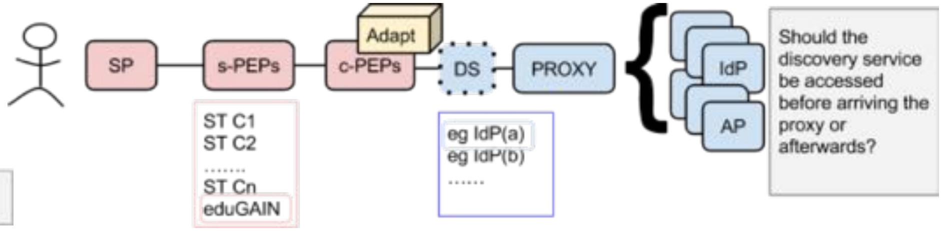




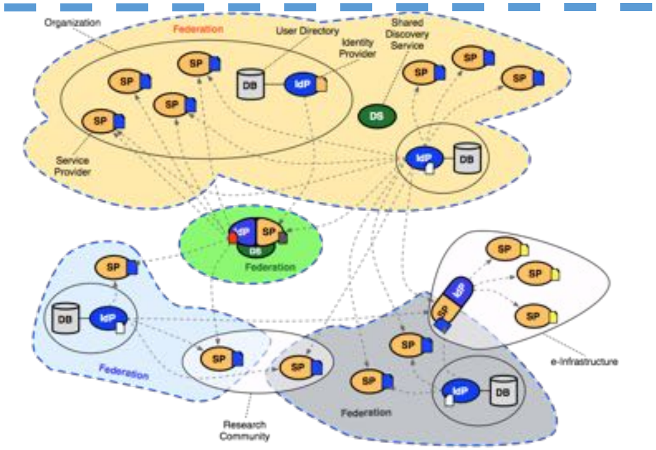
Scenario A: Middleware adaptors for C/S-PEPS

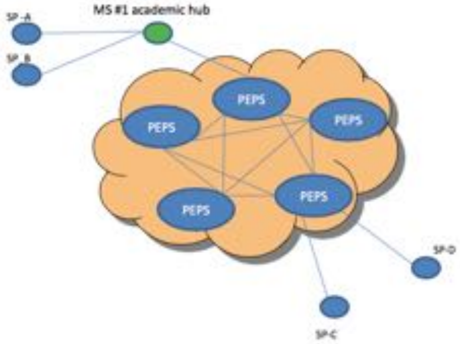


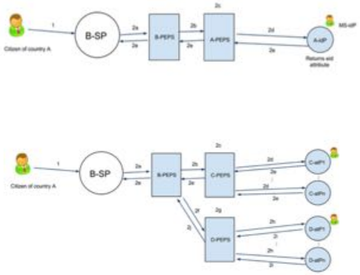
In this case each DS needs to know which would be its s-PEPs and the other way around adding the trust relation.



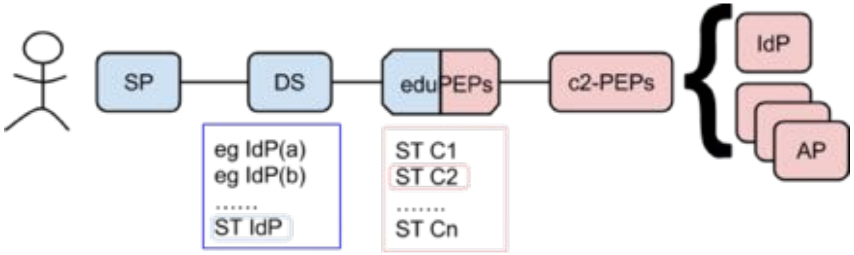
Should the discovery service be accessed before arriving the proxy or afterwards?

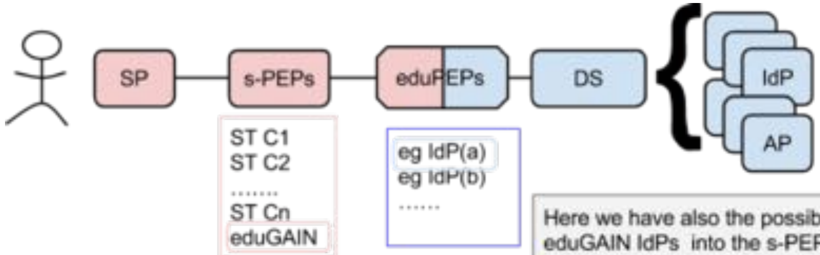




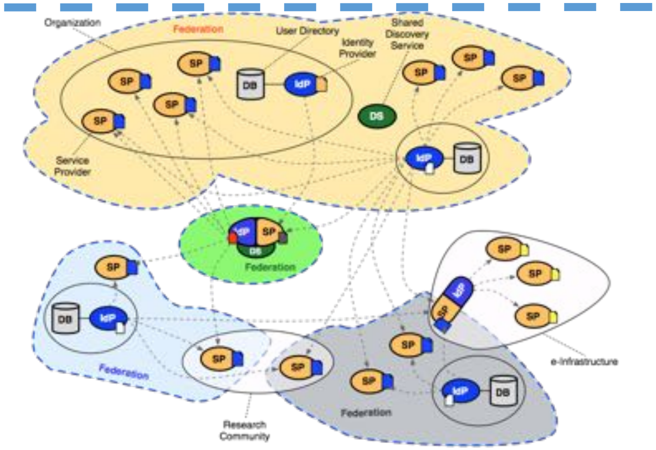


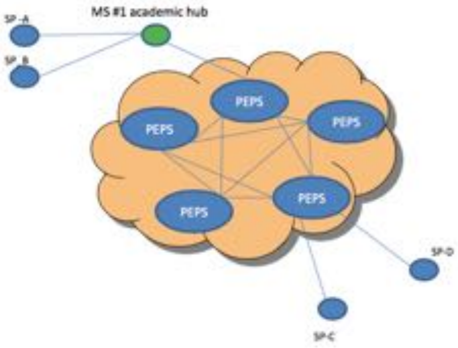
Scenario B: eduPEPS Proxying Entity

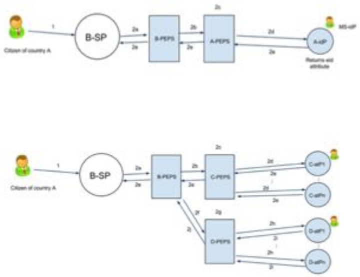




Here we have also the possibility of listing the eduGAIN IdPs into the s-PEPs list. We still are not sure what this would imply.


Organization
Federation
User Directory
Identity Provider
Shared Discovery Service
SP
DB
IdP
DS
Service Provider
Federation
Federation
e-Infrastructure
Research Community
Federation


SP-A
SP-B
MS #1 academic hub
PEPS
PEPS
PEPS
PEPS
PEPS
SP-D
SP-C


Citizen of country A
1
B-SP
2a
2e
B-PEPS
2b
A-PEPS
2c
2d
2e
A-IdP
MS-IdP
Returns eid attribute
Citizen of country A
1
B-SP
2a
2e
B-PEPS
2b
C-PEPS
2c
2d
2e
C-IdP1
C-IdPn
2f
2g
2i
D-PEPS
2h
D-IdP1
D-IdPn