Authentication and Authorisation
for Research and Collaboration

eGov-IDs and research communities in Europe: STORK2.0 and eduGAIN integration experiences

Christos Kanellopoulos

Architecture WP Leader, GRNET

WORKSHOP GARR 2016

TERABIT GENERATION - UNA COMUNITA' AD ALTE PRESTAZIONI

The AARC Project

Authentication and Authorisation for Research and Collaboration

- Two-year EC-funded project
- 20 partners
  - NRENs, e-Infrastructure providers and Libraries as equal partners
- About 3M euro budget
- Starting date 1st May, 2015
- https://aarc-project.eu/

The AARC Project

Development of pan-European identity federation services for researchers, educators and students

- Two-year EC-funded project
- 20 partners
  - NRENs, e-Infrastructure providers and Libraries as equal partners
- About 3M euro budget
- Starting date 1st May, 2015
- https://aarc-project.eu/

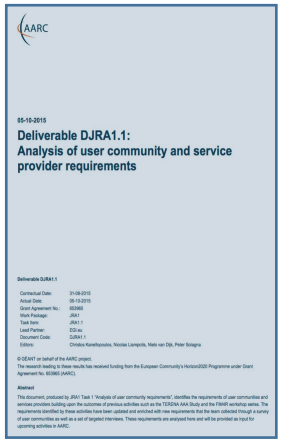
The AARC Project

Stimulate AAI services by supporting communities involved in the emerging data-rich science era

- Two-year EC-funded project
- 20 partners
  - NRENs, e-Infrastructure providers and Libraries as equal partners
- About 3M euro budget
- Starting date 1st May, 2015
- https://aarc-project.eu/

Requirements

Analysis of User Communities



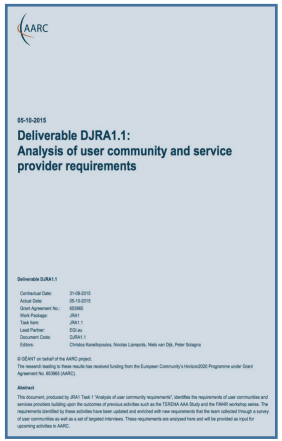
And Infrastructure Providers

Attribute Release	Attribute Aggregation	User friendliness	SP friendliness
Credential translation	Persistent Unique Identifiers	User Managed Information	Credential Delegation
Levels of Assurance	Homeless users	Step up Authentication	Best Practices and Policies
Community based AuthZ	Non web-browser	Social & e-Gov IDs	Incident Response

aarc-project.eu

Requirements

Analysis of User Communities



And Infrastructure Providers

Attribute Release .	Attribute Aggregation	User friendliness	SP friendliness
Credential translation	Persistent Unique Identifiers	User Managed Information	Credential Delegation
Levels of Assurance	Homeless users	Step up Authentication	Best Practices and Policies
Community based AuthZ	Non web-browser	Social & e-Gov IDs	Incident Response

aarc-project.eu

eGOV IDs & eIDAS

What is eIDAS?

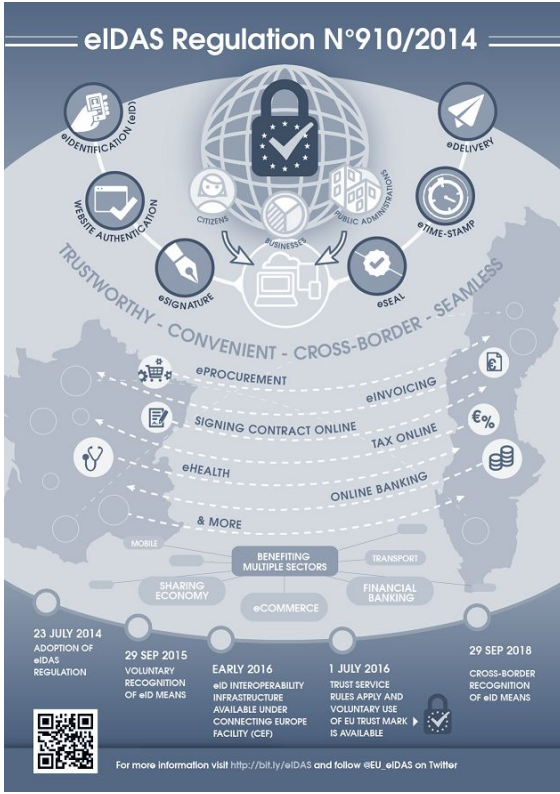
- The Regulation (EU) N°910/2014 on **electronic identification and trust services for electronic transactions** in the internal market (eIDAS Regulation) adopted by the co-legislators on 23 July 2014

What does it do?

- ensures that **people and businesses can use** their own national electronic identification schemes (**eIDs) to access public services** in other EU countries where eIDs are available.
- creates an European internal market for eTS, namely electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication
- Ensures that they will **work across borders and have the same legal status as traditional paper based processes**.

eIDAS Timeplan

- **23 JUL 2014**
  Adoption of eIDAS regulation
- **29 SEP 2015**
  Voluntary recognition of eID means
- **EARLY 2016**
  eID Interoperability Infrastructure available under Connecting Europe Facility (CEF)
- **1 JULY 2016**
  Trust Service rules apply and voluntary use of EU Trust Mark is available
- **29 SEP 2018**
  Cross-border recognition of eID means



STORK

AARC

What ~~is~~ was STORK?

- **CEF "Large Scale Pilot" project** series aiming to address the issues of cross-border interoperability of eID.
- **interconnects national eID infrastructures** and allows national electronic identities to identify users towards any services that uses STORK.
- allows people to use their national electronic ID to establish new e-relations with foreign electronic services, which may be operated by public or private service providers.
- a framework that does not change existing national eID infrastructure, but defines **an interoperability layer on top of national systems that supports cross-border eID federations**

STORK

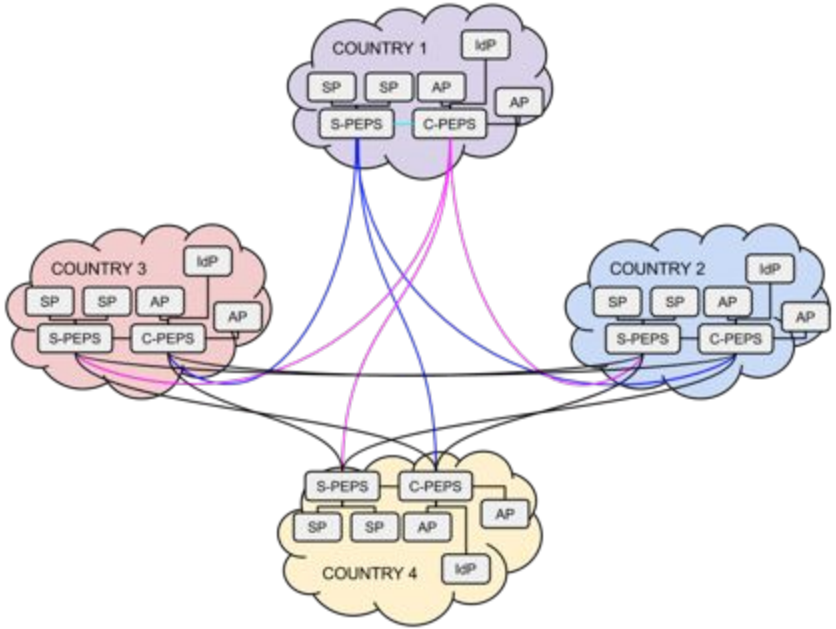
STORK-2 was a pilot project. No production rollout

- 17 countries “PEPS/VIDP-Enabled”
- More than 30 services running
- More than 40 different credentials supported

3 year project 2012 to 2015

19 countries involved

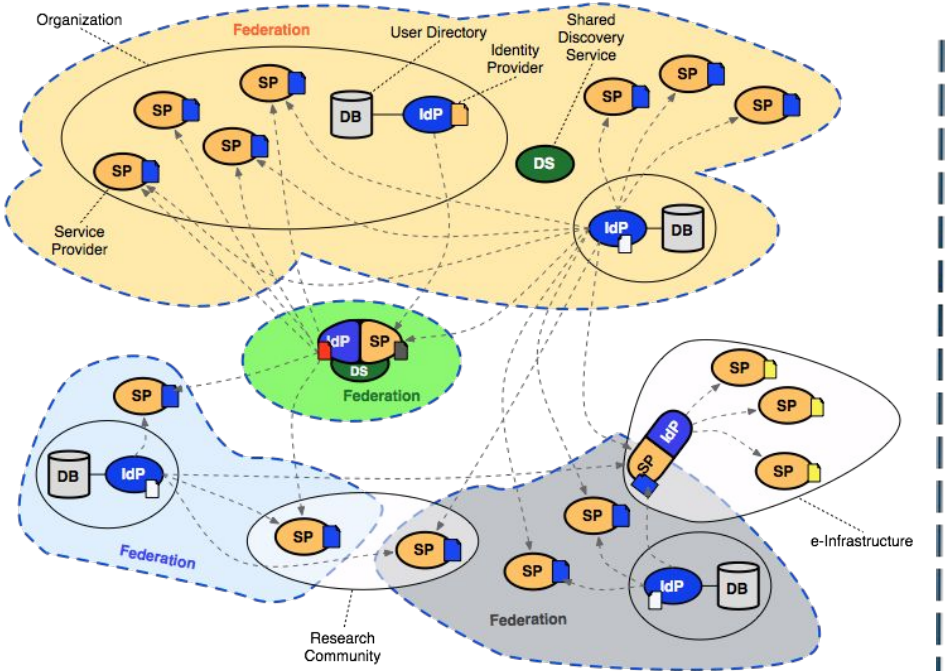
58 partners

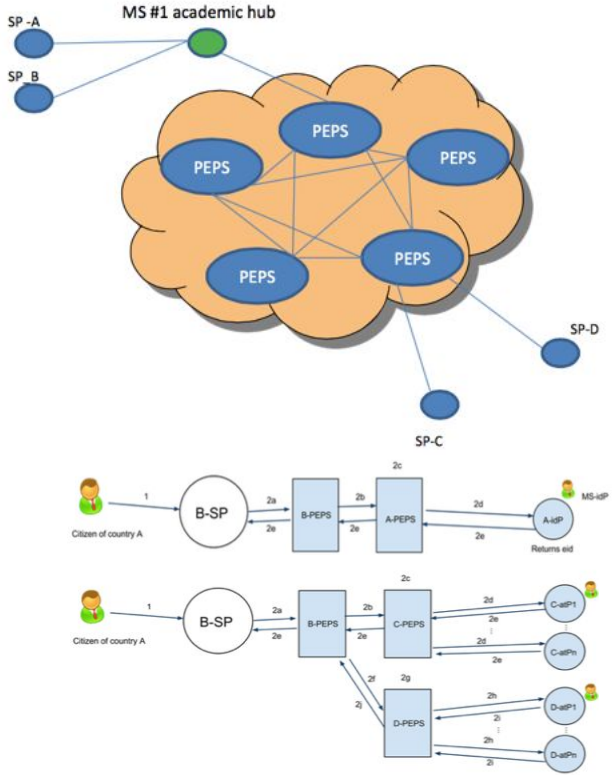


eduGAIN - STORK Interoperation Pilot

- Started in 2014 as a joint activity between GN3Plus/GN4P1 and STORK-2
- Goals:
  - Investigation of the compatibility between “eduGAIN” and “STORK-2” in terms of architecture and implementation
  - Investigate possible alternatives for utilizing eGOV IDs in services available in the academic federations

eduGAIN and STORK High Level Architectures

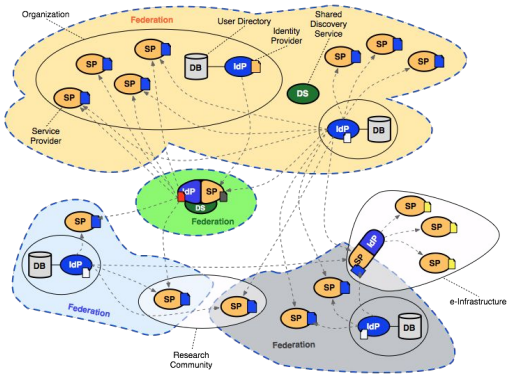


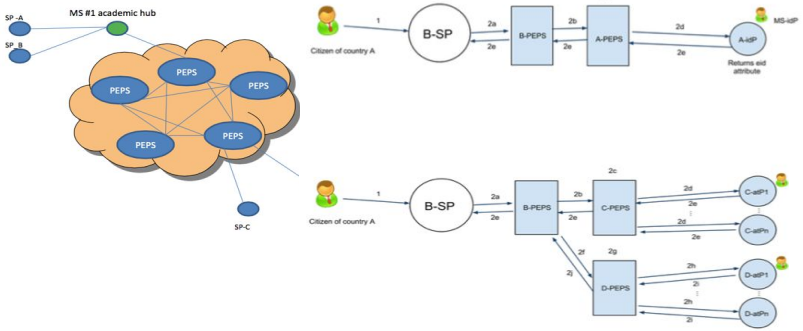


Similarities and differences

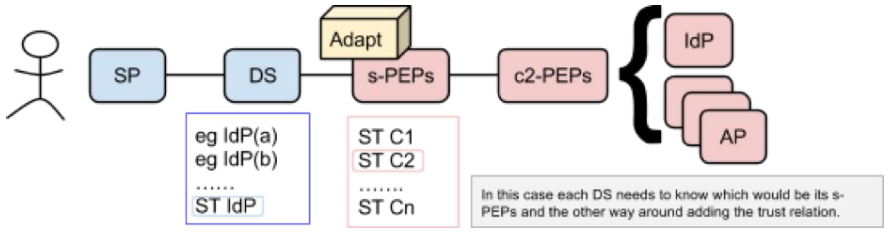
- SAML2 Interoperability Profile
- Full Mesh Federations and Hub and Spoke
- “Central” Metadata Service
- Dynamic Trust
- Attributes based on eduPerson
- Production infrastructure

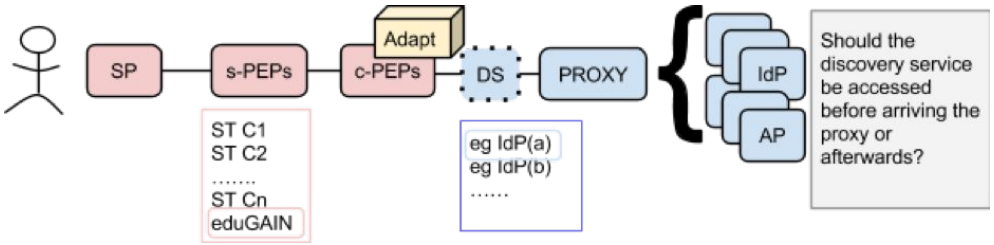
- $SAML_{STORK}$ Profile
- Proxied architecture
- Static Trust between Proxies (PEPS)
- Attribute Authorities & Attribute Aggregation
- Levels of Assurance
- STORK defined Attributes
- Pilot infrastructure

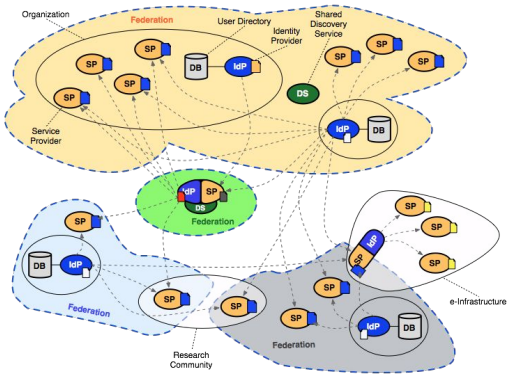


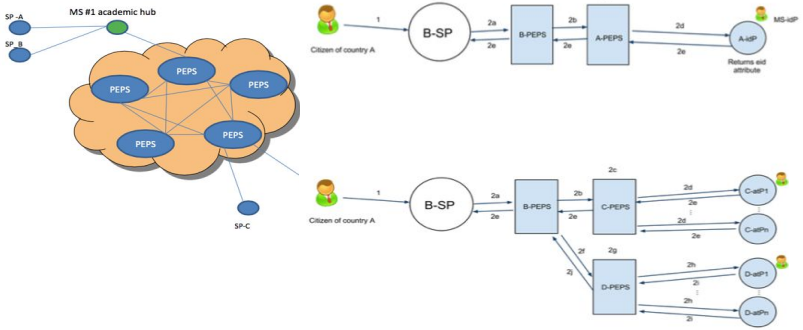


Proposal A: Middleware adaptors on C/S-PEPS

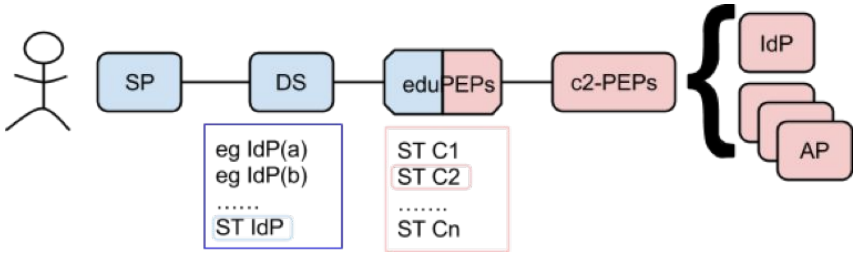


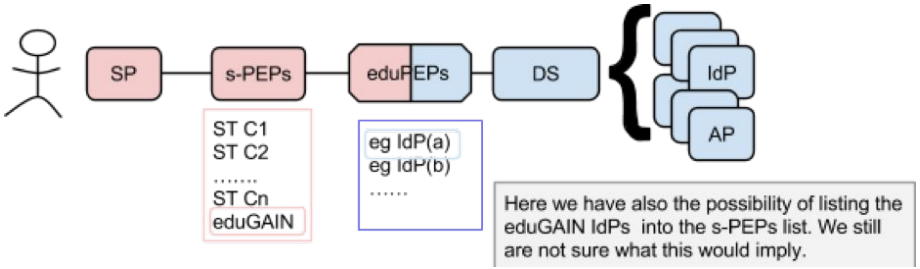


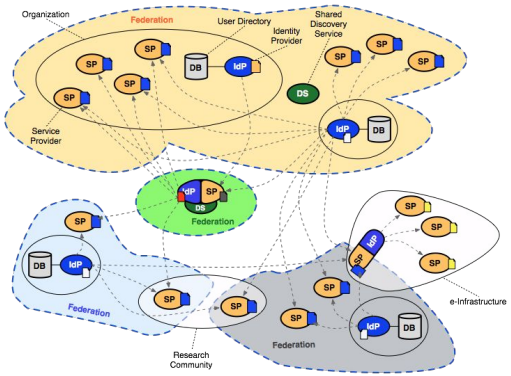


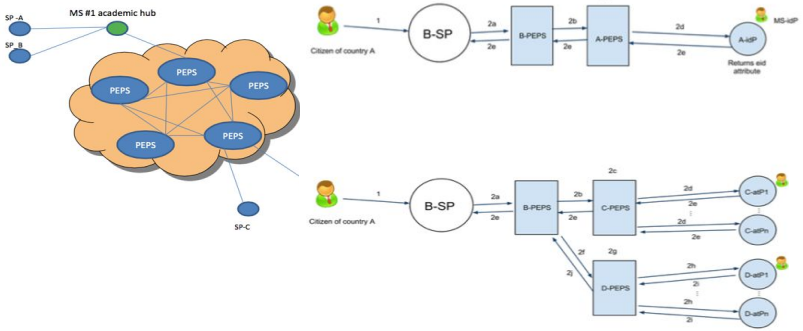


Proposal B: eduPEPS Proxying entity

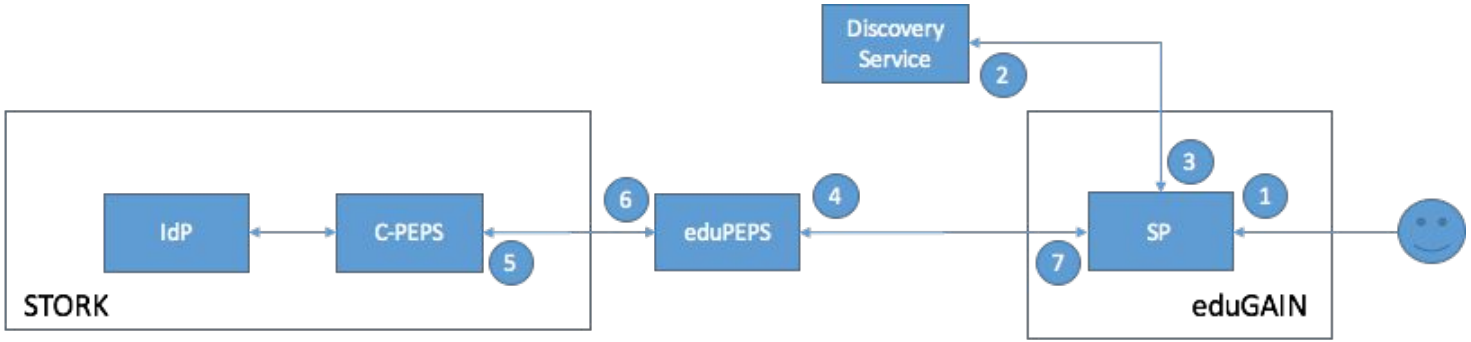






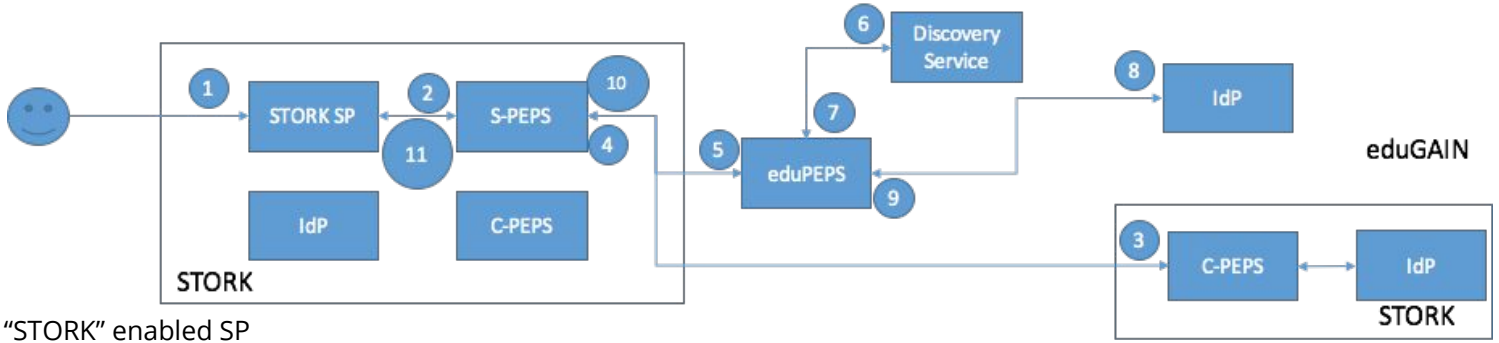


A user visits an “eduGAIN” enabled SP. Authentication and Attribute Retrieval on/from STORK



1.User visits an eduGAIN enabled SP
2.The SP redirects the user to the Discovery Service. The user selects that she wants to be authenticate using her eGov ID
3.The DS redirects the user back to the SP with the information about the eduPEPS
4.The SP redirects the user to the eduPEPS along with an attribute request. The user has to choose her home country
5.The user is redirected to the C-PEPS proxy service of her country and there she authenticates using her eID
6.The C-PEPS redirects the user back to the eduPEPS along with a SAML response that include the SAML authentication assertion and the requested attributes
7.The eduPEPS validates the SAML response, translates it to SAML2Int and redirects the user to the SP along with the SAML assertion

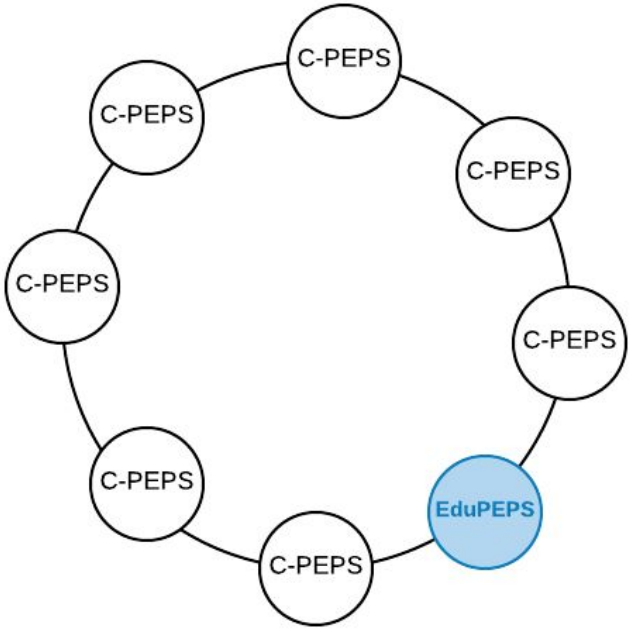
A user visits a STORK enabled SP. Authentication using eID and Attribute Retrieval from an “eduGAIN” IdP



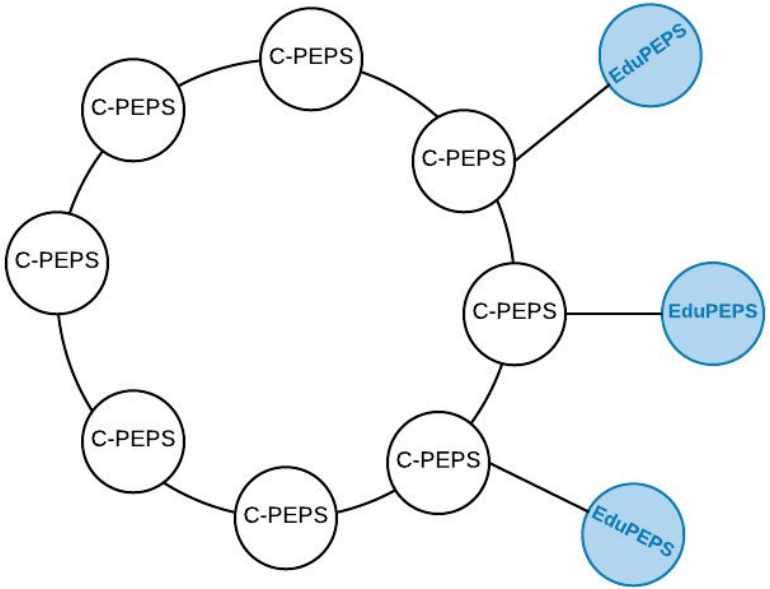
1. User visits a “STORK” enabled SP
2. The “STORK” SP redirects the user to the S-PEPS. The user selects that she wants to be authenticate via “eduGAIN”
3. The S-PEPS redirects the user to the C-PEPS, where the user authenticates
4. The C-PEPS redirects the user back to the S-PEPS with the authentication assertion and a basic set of attributes
5. The S-PEPS verifies the response from the C-PEPS and redirects the user to eduPEPS. The eduPEPS translates the STORK SAML Attribute Request into a SAML2Int SAML Attribute Request
6. The eduPEPS redirects the user to a Discovery Service in eduGAIN (The Discovery Service could be integrated in the eduPEPS and skip this extra step.)
7. In the Discovery Service the user selects her home institution and is redirected back to the eduPEPS
8. The eduPEPS redirects the user to the IdP of the home institution that the user selects along with the SAML2Int Attribute Request.
9. Upon successful authentication and the IdP redirects the user back to the eduPEPS along with a SAML assertion that includes the released attributes
10. The eduPEPS translates the SAML assertion(s) and the retrieved attributes and generates a STORK SAML assertion. The user is redirected back to the S-PEPS with the STORK SAML assertion generated by the eduPEPS
11. The S-PEPS verifies the response from the eduPEPS and redirects the user back to the STORK SP along with aggregated set of the requested attributes.

Deployment/Trust Models

eduPEPS as a C-PEPS



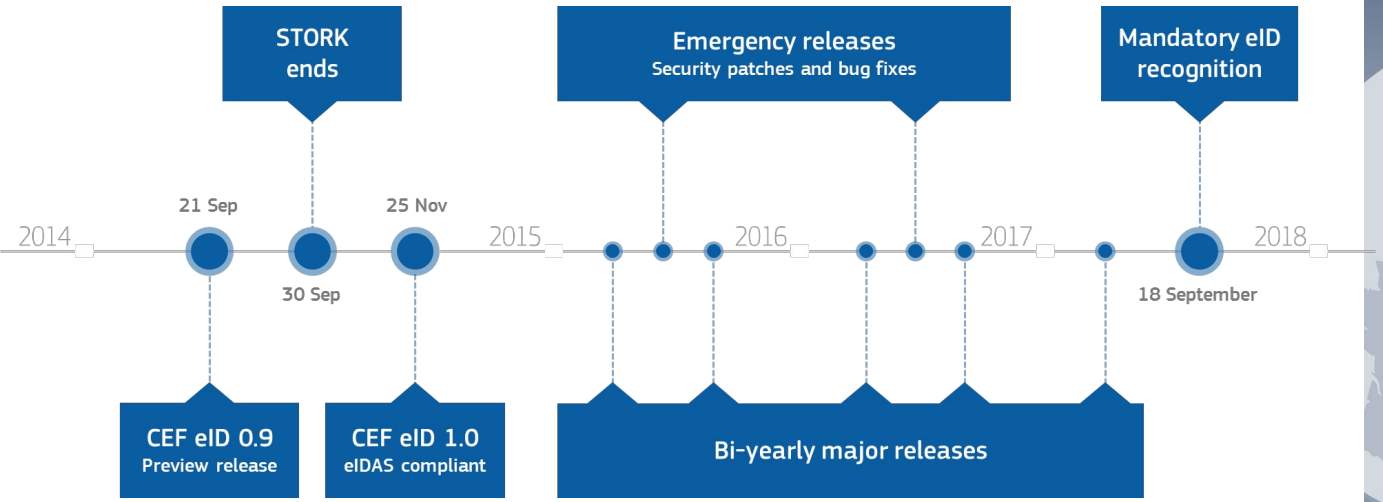
eduPEPS as bridge behind the C-PEPS

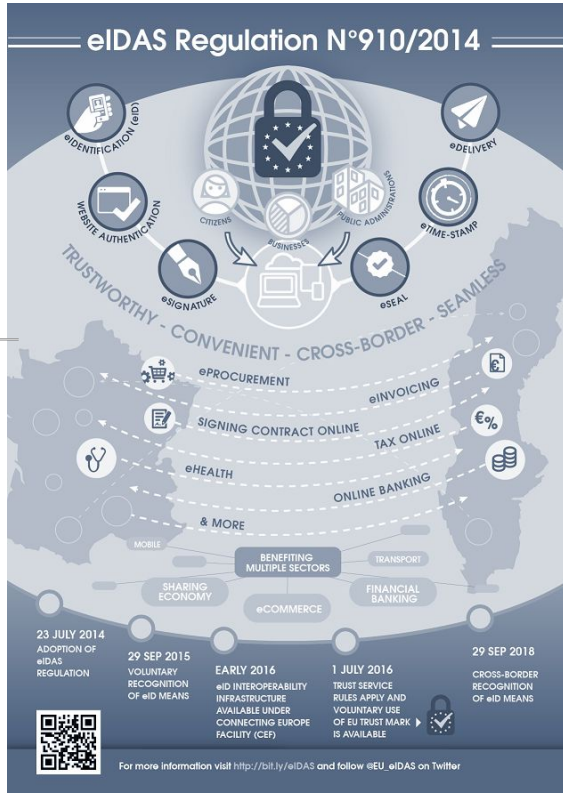


eduPEPS Proof-of-Concept

- A SAML Proxy (SAML2Int $\Leftrightarrow$ $SAML_{STORK}$)
  - Based on OpenSAML and STORM SAML libraries
- Attribute translation library
- Built-in Discovery and User Consent
- Supports both deployment models
- Successfully tested with Spanish and Greek Pre-production PEPS
- https://github.com/edugain-stork/edupeps

eIDAS Timeplan

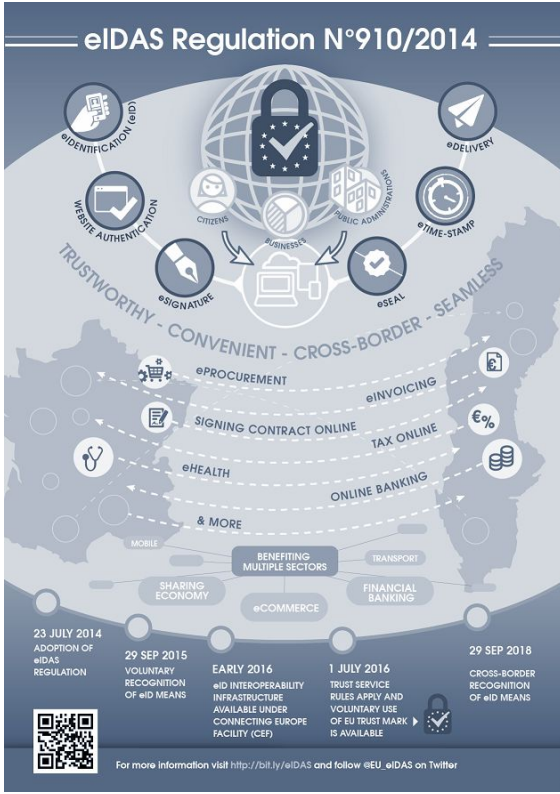




The EU invests €5.5 million to boost secure and efficient online services across Europe

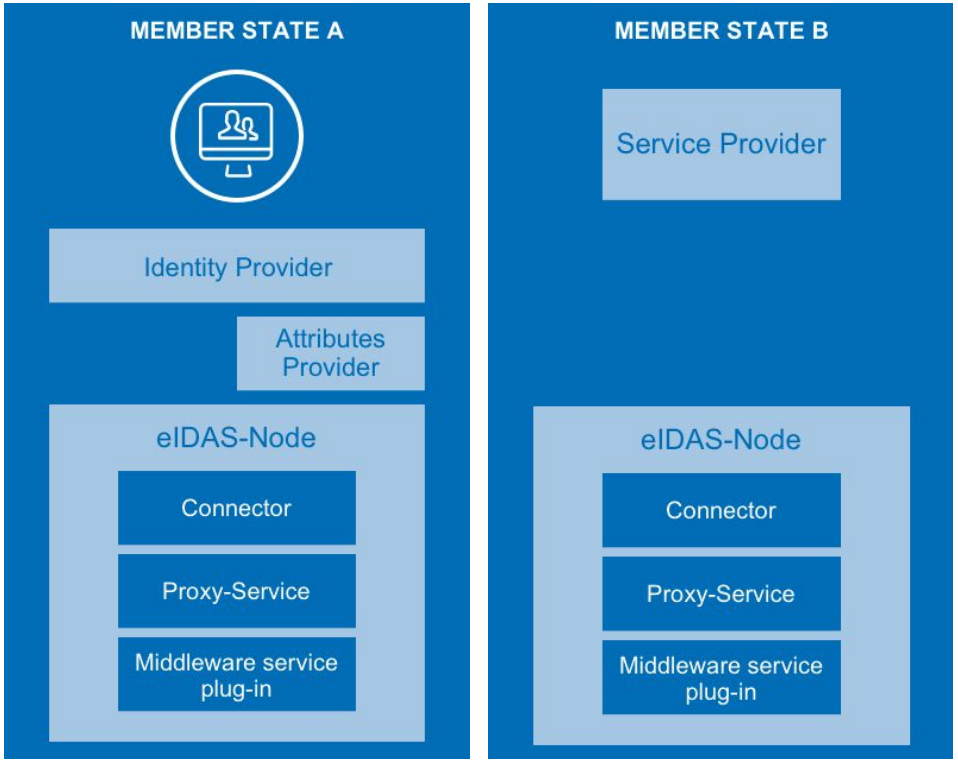
http://ec.europa.eu/inea/en/eu-invests-%E2%82%AC55-million-to-boost-secure-efficient-online-eID-services

- The European Union will co-finance 20 projects addressing the cross-border interconnection of electronic identification (eID) services in Europe.
- Budget from the Connecting Europe Facility (CEF) programme in the sector of telecommunications
- Goal: help EU Member States with the roll-out of technical infrastructure to create interoperable, pan-European eID services under the recently completed eIDAS legal framework.
- 1st call August 2015 & 2nd call March 2016



From Stork to the eIDAS node

- STABILITY (!!!!)
- Documentation
- C-PEPS ➜ Proxy Service
- S-PEPS ➜ Connector
- VIDP ➜ MS Middleware service plugin



eIDAS Natural Person Mandatory Attributes

- Uniqueness Identifier
  - SAML Attribute Name: http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier
  - SAML Attribute FriendlyName: PersonIdentifier
- Current Family Name(s)
  - SAML Attribute Name: http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName
  - SAML Attribute FriendlyName: FamilyName
- Current First Name(s)
  - SAML Attribute Name: http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName
  - SAML Attribute FriendlyName: FirstName
- Date of Birth
  - SAML Attribute Name: http://eidas.europa.eu/attributes/naturalperson/DateOfBirth
  - SAML Attribute FriendlyName: DateOfBirth

eIDAS Levels of Assurance

- http://eidas.europa.eu/LoA/low
- http://eidas.europa.eu/LoA/substantial
- http://eidas.europa.eu/LoA/high

- More details:

  http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R1502&from=EN

Thank you

Any Questions?

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).