Update on eIDAS

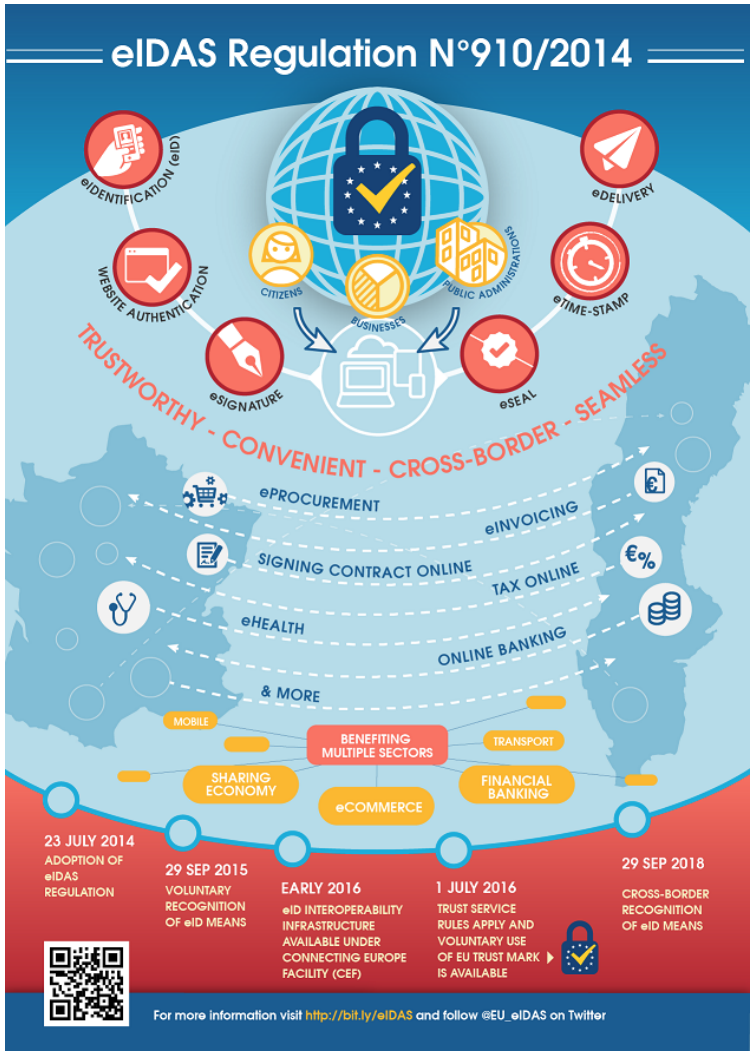
Christos Kanellopoulos

eduGAIN TownHall, Vienna

February 21st, 2017

Background information

- **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



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.

Cross-sector interoperation with eIDAS

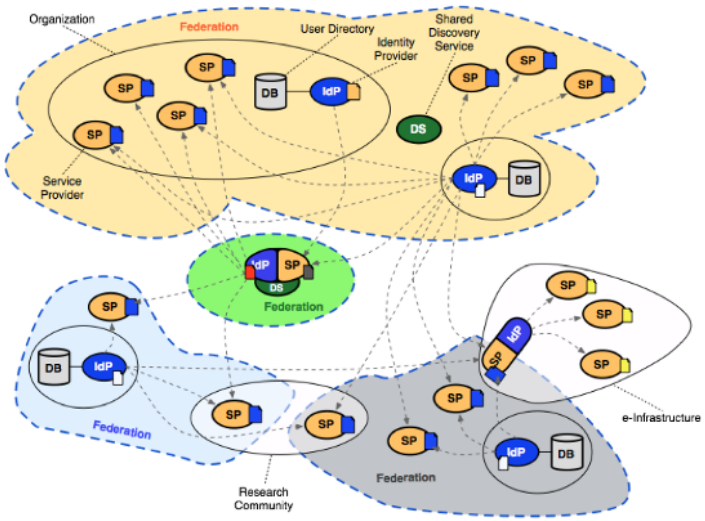
- **2016-07 – 1st meeting in Brussels between AARC, GN4 and eIDAS Reps**
  - Investigate the possibility of an interoperation pilot between eduGAIN and eIDAS
- **2016-09 – 2nd meeting in London (AARC, GN4, Internet2, eIDAS Reps)**
  - Draft proposal for an interoperability pilot between
  - 3 Use cases:
    - 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]
- **2016-10 – eduGAIN Steering Group**
  - Internal analysis and recommendation 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?

eduGAIN – eIDAS Comparison - https://goo.gl/tLbXE4

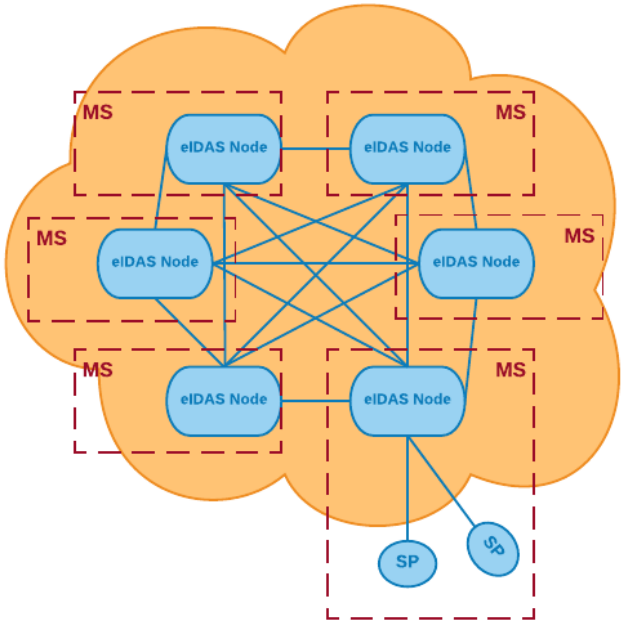
C. Kanellopoulos/AARC - GN4, **Licia Florio**/GÉANT – AARC, **Maarten Kremers**/SURFNET – GN4,

Wolfgang Pempe/DFN, **Davide Vaghetti**/GAAR, **Ioannis Kakavas**/GRNET, **Nicolas Liampotis**/GRNET

National Federations in eduGAIN



eIDAS Nodes



eduGAIN – eIDAS Comparison - https://goo.gl/tLbXE4

eduGAIN

- **Architecture**
  - Dynamic topology (proxied and full mesh federations
  - IdPs and SPs published in eduGAIN MDS
- **Service Providers**
  - Requested attributes in the metadata
- **Attributes**
  - eduPerson

eIDAS

- **Architecture**
  - “Static” topology (proxies)
  - Static trust relationship between eIDAS Nodes
- **Service Providers**
  - Requested attributes in AuthN request
  - SPType: Private or Public
- **Attributes**
  - **Surname, Name, Date of Birth, Unique Identifier,** First name at birth, Family name at birth, Place of birth, Current address, Gender

eduGAIN – eIDAS Comparison - https://goo.gl/tLbXE4

eduGAIN

- **SAML AuthN Request**
  - Dynamic topology (proxied and full mesh federations
  - RequestAuthnContext MAY be set and comparison attribute SHOULD NOT me provided or be set to “exact"
- **SAML AuthN Response**
  - MUST be signed
  - Unsolicited responses MUST be accepted

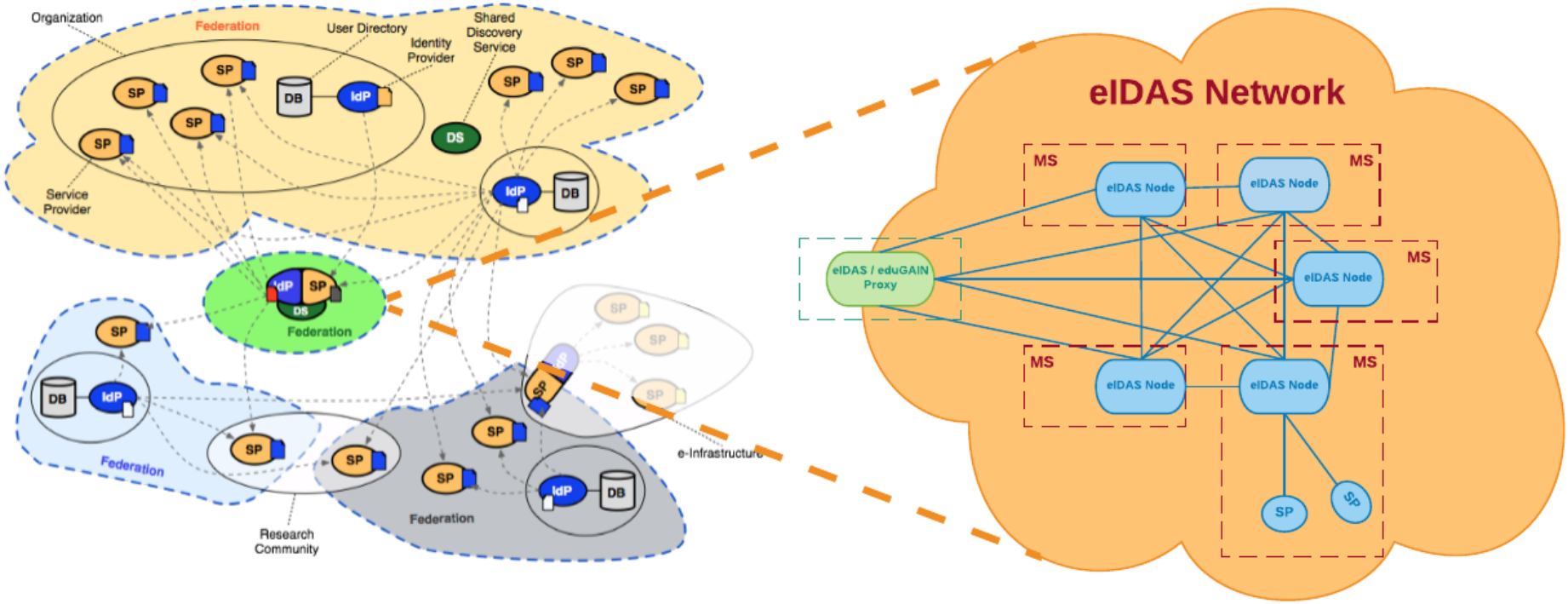
eIDAS

- **SAML AuthN Request**
  - Force auth must be set to True
  - SPType must be set to Public or Private <eidas:SPType>
  - Requested attributes <eidas:RequestedAttributes>
  - RequestAuthnContext MUST be set and comparison attribute MAY be provided
- **SAML AuthN Response**
  - MAY be signed
  - Unsolicited responses MUST NOT be accepted

Interoperability Scenarios

- **Scenario 1:** A service with global scope that would function as a gateway between any entity in the eduGAIN inter-federation and the eIDAS Network
- **Scenario 2:** An implementation with national scope that would function as a “gateway” between the national academic federation and the eIDAS-Node in the specific country.

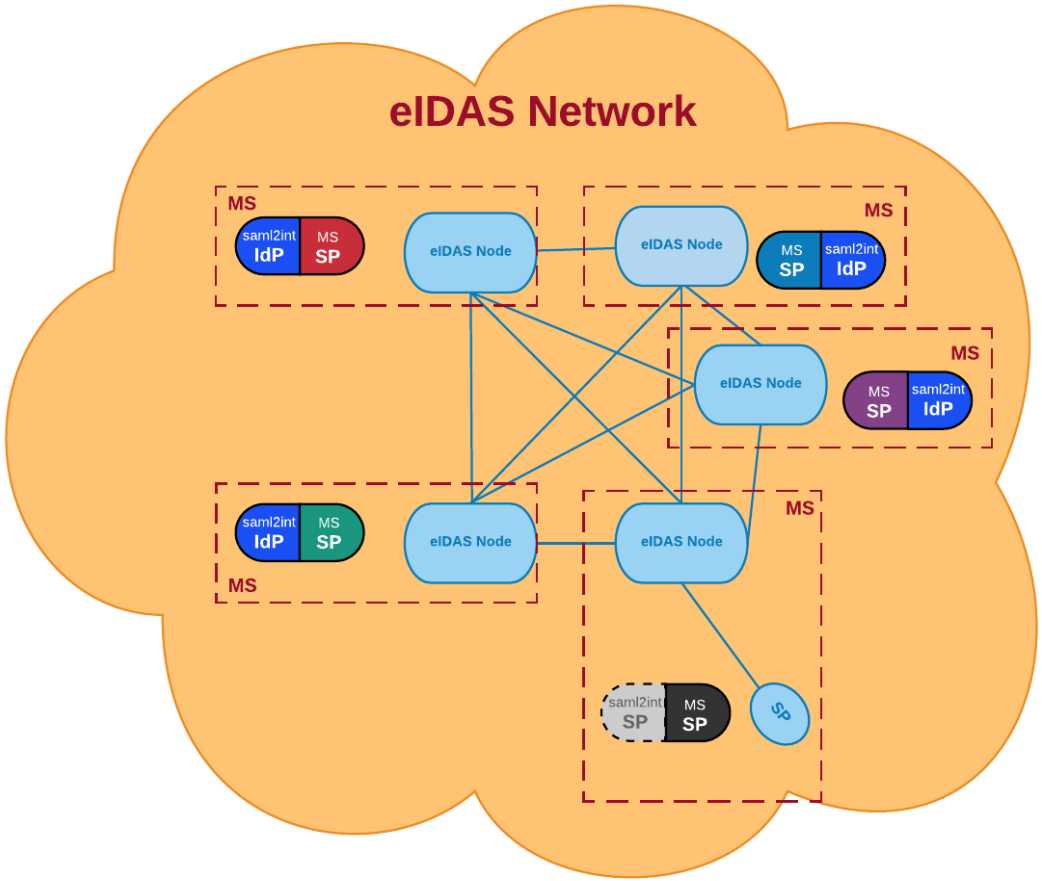
Interoperability Scenarios | Scenario 1



Interoperability Scenarios | Scenario 1

- Taps directly to eIDAS Interoperability Framework, which is the only common standardized interface across all the national eID schemes
- Just one service for all the federations participating in eduGAIN
- No extra burden to the federation operators
- SPs can treat the service as a proxy IdP
- Flexibility on how eIDAS becomes visible to the federations
- Avoid creating islands in which some federation will be able to use the local eGOV ID scheme, while there is no support in others
- SPs worldwide could potentially benefit from such a bridge
- Not under the direct control of each Federation
- Has to be operated as an eduGAIN service
- Increased burden (and possible liability) for the organization(s) operating the service
- eIDAS is a European specific service, why should federations outside of Europe care about this?

Interoperability Scenarios | Scenario 2



Interoperability Scenarios | Scenario 2

- Tailored to the needs of each federation
- Fully controlled by the federation
- The burden and liability of the implementation is distributed to the federations
- The implementation could be more lightweight for some cases
- Each implementation would be specific to each country
- Dependency on the willingness or the reluctancy of each country's eGOV ID governance to accomplish the integration with the local R&E identity federation
- Extra burden (and possibly costs) on the operators of the federation

skanct@gmail.com

Thank you and any questions

GÉANT

Networks · Services · People

www.geant.org