ESMO Project

eIDAS-enabled Student Mobility for Identity Federation

Nikos Triantafyllou, UAegean
Katerina Ksystra, UAegean
Petros Kavassalis, UAegean

TNC 19
(Tallinn, June 19th 2019)

www.ESMO-project.eu
Contents

1. What is ESMO
2. eIDAS network
3. ESMO Gateway: Goals
4. ESMO Gateway: Design
5. ESMO Infrastructure: Achievements
6. Future Directions / Conclusions
ESMO Project

- CEF Project.
- 15 months. April 2018 – June 2019
- Partners
Objectives

• Promote **eIDAS adoption** through the CEF eID.
  - By minimising adoption costs for SPs.

• Facilitate **learning mobility**.
  - By enabling **eIDAS** cross-border electronic authentication.
  - By enabling cross-border exchange of **sector specific attributes**.
  - Promote **streamlined administrative procedures** (using trusted data transfer between institutions).

• **Ease** management of **trust** and data requirements.

• Promote **convergence** with **eduGAIN**, cooperation with other CEF and Erasmus+ projects based on common objectives.
• **European regulation** on eID and Signature

• Establishes **Mutual recognition** of eID schemes
  - Levels high and substantial: **mandatory**
  - Level low: **optional**

• **Member states** have sovereignty over:
  - Which **schemes are notified**
  - Organisation of the **federation at national level**.

• **Mandatory** for **public services**
  - Which accept at least substantial or high authentication mechanisms

• **CEF released building blocks** to support its enforcement
  - We use CEF eID infrastructure network
eIDAS Interoperability Architecture
<table>
<thead>
<tr>
<th>Country</th>
<th>Status</th>
<th>Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Croatia</td>
<td>High</td>
<td>NOTIFIED</td>
</tr>
<tr>
<td>Germany</td>
<td>High</td>
<td>NOTIFIED</td>
</tr>
<tr>
<td>Estonia</td>
<td>High</td>
<td>NOTIFIED</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>High</td>
<td>NOTIFIED</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Low - Sub</td>
<td>NOTIFIED</td>
</tr>
<tr>
<td>Portugal</td>
<td>High</td>
<td>NOTIFIED</td>
</tr>
<tr>
<td>Belgium</td>
<td>High</td>
<td>NOTIFIED</td>
</tr>
<tr>
<td>Spain</td>
<td>High</td>
<td>NOTIFIED</td>
</tr>
<tr>
<td>Italy</td>
<td>Low -High</td>
<td>NOTIFIED</td>
</tr>
</tbody>
</table>
ESMO Gateway: Goals

- **Goals:**
  - **Proxy** functionality to support eIDAS adoption
    - By minimising adoption costs
    - **Convergence with eduGAIN**
  - With **attribute aggregation capacity**
  - Which allows the SPs/APs&/IDPs **delegate** the management of trust
  - With **Multi-protocol support** both for SPs, IdPs and Aps
    - SAML2Int, SAML2-eIDAS, OIDC, OAUTH2
**Infrastructure: Architecture**

- **Personal Identification Attributes (PII):**
  - eIDAS

- **Academic Attributes:**
  - eduGAIN (Connection to Spanish and Greek EduGain Federations)
  - Academic APs
ESMO Gateway: Design Result

- **Result:**
  - **Microservices** architecture
    - With **protocol translation** capabilities
    - Cover features mismatch between protocols with additional metadata
  - **Security** model: Based on JWT/JWE and HttpSignatures
  - **Flexible** (allow multiple topologies)
  - **Scalable**
    - Adapt to demand and offer high availability
  - **Modularity** and extensibility
    - Facilitates hot-plugging of new modules or replicated instances
Infrastructure: Architecture
Gateway: Achievements

- Accepts requests for **eIDAS authentication** in: SAML2Int, SAML2eIDAS, OIDC
- Requests can include **additional academic attributes** to be retrieved from HEI APs.
- Acts as a proxy for the relying parties
- Acts as a proxy for the data sources, acting as a single point of entry
- Supported attribute set based on eduPerson, SCHAC to promote standards.
- Does not store user information, user centred application flow. Which facilitates **GDPR compliance**.
- Easy deployment (Docker images)
Project Sustainability: Challenges

• Identity reconciliation
  - Not matching or even targeted identifiers
  - Trusting the user claim, but risk of attr lending
  - SEAL Project

• Attribute sources scarce (except for eduGAIN)

• Offered attributes: reduced and simple set

• Technological gap for common users (both eIDAS and federations in general)
Beyond ESMO | Three models for attribute aggregation

1/ Centralized (ESMO)

- Round robin design
- SP agnostic of aggregation
- User experience

- Attributes transfer through an Attributes Aggregating Service (STORK 2.0 - ESMO ACM)
  - Linking Service on the fly
Beyond ESMO | Three models for attribute aggregation

2/ Edge (ESMO +)

- User initiated process
- SP handles aggregation
- Better user experience
- Not standardized aggregation process

• Attributes transfer through a locally deployed Linking Service (SP-side)
  - Mobility Identity and Access Management (UAegean Keycloak)
Beyond ESMO | Three models for attribute aggregation

3/ Decentralized (SEAL)

- User initiated process
- User handles aggregation
- No honey pots
- Standardized aggregation

- Attribute transfer through a Self-Sovereign Identity Service (SSI Service)
  - SEAL Project (2019-2021 - CEF funding)
Thank you for your attention

Nikos Triantafyllou
triantafyllou.ni@aegean.gr