EGI-Engage: The AAI Strategy for the EGI Infrastructure

Christos Kanellopoulos - GRNET
AAI in EGI Today

- EGI Trust Fabric is based on IGTF
- Services require X.509v3 certificates and proxies for user authentication
- Identity vetting and user traceability provided by the IGTF providers
- Authorization is based on VO groups and roles
- VO registration process is fairly lightweight
Adeps in EGI Today

- EGI Trust Fabric is based on IGTF
- Services require X.509v3 certificates and proxies for user authentication
- Identity vetting and user traceability provided by the IGTF providers
- Authorization is based on VO groups and roles
- VO registration process is fairly lightweight
- Provides solution for web and non-web access, with delegation built-in, clear separation of authn and authz and has been working/evolving for the last 15 years
- But a fairly low number of users understand X.509 certificates

David Groep, NIKHEF
Peter Solagna, EGI.eu
Why move to FedAuth

Cross-national federated access progressed tremendously

- eduGAIN: more federations, with technical interop across countries
- Increased awareness of research & scholarship use cases
- ‘the will to make it happen’: demonstrated by SirTFi, AARC, VOPaaS, …

A great promise for easier collaboration

- Move to authenticators ‘closer’ to the user understanding – mainly home organization credentials
- Ability to ‘hide’ end-user PKIX technology – and offer simpler authentication for web-based services through ‘OpenID Connect’ and ‘SAML’

And there are bridges – since for non-Web, command-line and brokerage ‘SAML2Int WebSSO’ does not work

- STS, CiLogon, TCS, SSH-to-MyProxy tokens, Moonshot, …

Source: “Developments in the Trust Fabric” - David Groep, NIKHEF
Although many production federations are pretty good, and quite a few IdPs have good processes …

● public documentation, self-assessment and peer-review are missing
● it’s not consistent across IdPs

and processes are not designed for collaboration use cases

● re-use of identifiers occurs (also an issue for social IdPs)
● the identity providers provide no identity … or it’s non-consistent
● identifiers generated are specific to each SP (defeating brokering)

and may not provide traceability needed for valuable resources

● some allow users to change their own data (including e.g. their email address and all contact data), or do not collaborate in case of issues

Source: “Developments in the Trust Fabric” - David Groep, NIKHEF
EGI FedAuth Activities

Proof-of-concepts started in the predecessor of EGI-Engage:

- Cloud AAI Pilot
  https://wiki.egi.eu/wiki/AAI_pilot

- EGI User Platform LTOS
  https://wiki.egi.eu/wiki/Long-tail_of_science_pilot
● **Goal 1**: Connect cloud services to the SURFnet OpenConext service to retrieve SAML assertions containing user identities and attributes that describe the user capabilities

● **Goal 2**: Provision account and groups/projects on the cloud service providers

● Cloud stacks to be integrated: OpenNebula, OpenStack (Juno/Icehouse), Synnefo

● Identity Providers: SURFnet IdP, GRNET, EGI, OpenConext Proxy IdP, Hexxa, EduGAIN

● Attribute Providers: OpenConext, Perun
● **Zero-barrier access:** any user who carries out relevant research can get a start-up resource allocation

● **100% coverage:** anyone with internet access can become a user

● **User-centric:** User support for platform users is available through the NGIs

● **Realistic:** Reuse existing technology building blocks as much as possible, require minimal new development

● **Secure:** Provide acceptable level of tracking of users and user activities (Not necessarily f2f vetting)

● **Scalable:** Can scale up to support large number resource providers, technology providers, use cases and users

● **Valuable:** Produce tangible outcomes

**Source:** A new platform from EGI for the LTOS - https://goo.gl/IT99tx
EGI-Engage Targets

- Explore approaches to **easier safe management of user credentials**
- Identify possibilities and requirements for user authentication against both **web and non web-based applications**.
- Identify **user registration and management requirements** from a VO perspective. *Engage with the CCs*, capture workflows and develop solution prototypes.
- **Explore current technical possibilities** and the usability of existing infrastructures covering identity management
- Develop **authentication solutions for use cases**
- Investigate **alternative identity-vetting approaches** to current practices
- **Liaise with other projects** focusing on AAI to share know-how and best practices.


Links to other activities

JRA2.1: Federated data  
JRA2.2: Federated cloud  
JRA2.3: e-Infra Interoperation

JRA1.2: Registry and marketplace  
JRA1.3: Accounting  
**JRA1.4: Ops Tools**  
JRA1.5: Resource Allocation

**Bold text:** Collaborators of JRA1.1  
**Normal text:** Customers of JRA1.1  
**Red text:** Target for PY1

SA1.1: Security Ops  
SA1.3: Platform Ops

SA2.1: Training (AAI)  
SA2.2: User Support (AAI)  
SA2.3: Elixir-ESFRI  
SA2.4: BBMRI  
SA2.5: MoBRAIN-ESFRI  
SA2.6: DARIAH-ERIC-ESFRI  
SA2.7: LifeWatch-ESFRI  
SA2.8: EISCAT_3D-ESFRI  
SA2.9: EPOS-ESFRI
# EGI-Engage Roadmap

<table>
<thead>
<tr>
<th>#</th>
<th>Task name</th>
<th>Start date</th>
<th>Release date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td><strong>Identification of and liaison with stakeholders</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• WP3 F2F and EGI Conference ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Liaise with AARC ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Connections with GN4, EUDAT2020 and PRACE ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Identification of initial set of tools ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>05/2015 (PM3)</td>
<td>06/2015 (PM4)</td>
</tr>
<tr>
<td>1.2</td>
<td><strong>Requirements capturing</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Use FIM4R as the starting point and align with AARC DJRA1.1 ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Identify the most important use cases (CC) ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Technical guidelines for enabling federated access in the initial set of tools ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>05/2015 (PM3)</td>
<td>08/2015 (PM6)</td>
</tr>
<tr>
<td>1.3</td>
<td><strong>Technical architecture and pilot implementation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Phase 1:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Which AA services are needed ✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Collaboration with the AAI pilot and the user portal activity for the LTOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Pilot: Connection of the first set of EGI tools to the EGI IdP proxy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Phase 2:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Expansion to EGI Tools and selected CCs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Interaction with SA2 (Training &amp; User support)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Phase 3:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Technology reassessment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Pilot services and best practices to enable federated AAI solutions released</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Phase 4:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Architecture and solution for the production EGI AAI services</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Identity Management for Distributed User Communities report</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>09/2015 (PM7)</td>
<td>12/2015 (PM10)</td>
</tr>
</tbody>
</table>
• Users should be able to use any (web and non-web) EGI Service using federated access.
  • Leverage National Federations via eduGAIN
  • Support for external IdPs like the EGI SSO
• Federated access should be the enabler and not the barrier
  • Users that do not have account on one of the IdPs in the eduGAIN Federations, should still be able to access the EGI services as it is the case now.
  • Support for multiple technologies (SAML, OpenID Connect, X509)
• Users should be identified uniquely and persistently
  • EGI should require from the IdPs at least an identifier that uniquely identifies the user in the scope of that organization.
  • Within the EGI environment, a user should have one **persistent non-reassignable unique identifier**.
  • Work with AARC on the problem of globally unique identifiers.
• **Flexible support for Attribute Retrieval**
  - Define the minimum set of required attributes
  - Attribute sources: Home organizations, VOs/Scientific Communities, the users themselves

• **Multiple Levels of Assurance**
  - e.g. there should be a distinction in the LoA between self-asserted attributes and the attributes provided by the Home Organization/VO
  - Work in collaboration with AARC Policy Task

• **Support for “differentiated assurance”**
  - Retrieve just an opaque ID from the IdP
  - Questions about real names or pseudonyms, enrolling users to communities, auditability and tracing, inident response must be taken up by somebody else (Infrastructure, VO, Peer collaborators etc)
• **User authentication does not imply access rights**
  • Access to the various services should be granted based on the VO/EGI roles the user have

• **Service Provider onboarding should be easy and secure**
  • Service providers should not have to deal with the complexity of connecting to multiple AAIs. Connect once with the infrastructure and leverage multiple AAIs seamlessly
  • Service providers should be free to choose one of the available technologies that best meet their needs (e.g. SAML, OpenID Connect, X509 etc)
  • Service providers should not have the burden to implement services that can be provided centrally (e.g. Discovery Services, Token Translation services)
  • Work in collaboration with the AARC Architecture and Pilot tasks

• **Ensure support of and compliance to existing policies**
  • Work in collaboration with the AARC Policy Task
EGI AAI Architecture with the AARC Token Translation Pilot
EGI AAI Architecture
supporting both SAML and OpenID/OAuth2
New AAI Services

From X.509 certificates to a multiple identity tokens

- Users will access EGI services with their Home Organisation credentials, which will be mapped to one persistent EGI unique identifier
- Different levels of Assurance
- Token Translation Services to convert users’ credentials:
  - Online CA, PUSPs, etc.
- Pilot implementation ready by QR2 2016
Thank you for your attention.

Questions?