

EGI AAI Platform

Christos Kanellopoulos - GRNET



www.egi.eu

EGI-Engage is co-funded by the Horizon 2020 Framework Programme of the European Union under grant number 654142



Authentication and Authorisation Infrastructure

Task	JRA1.1
Start	M3 (May)
End	M27

Partners	EGI.eu	CESNET	GRNET	NIKHEF	STFC
-----------------	--------	--------	-------	--------	------

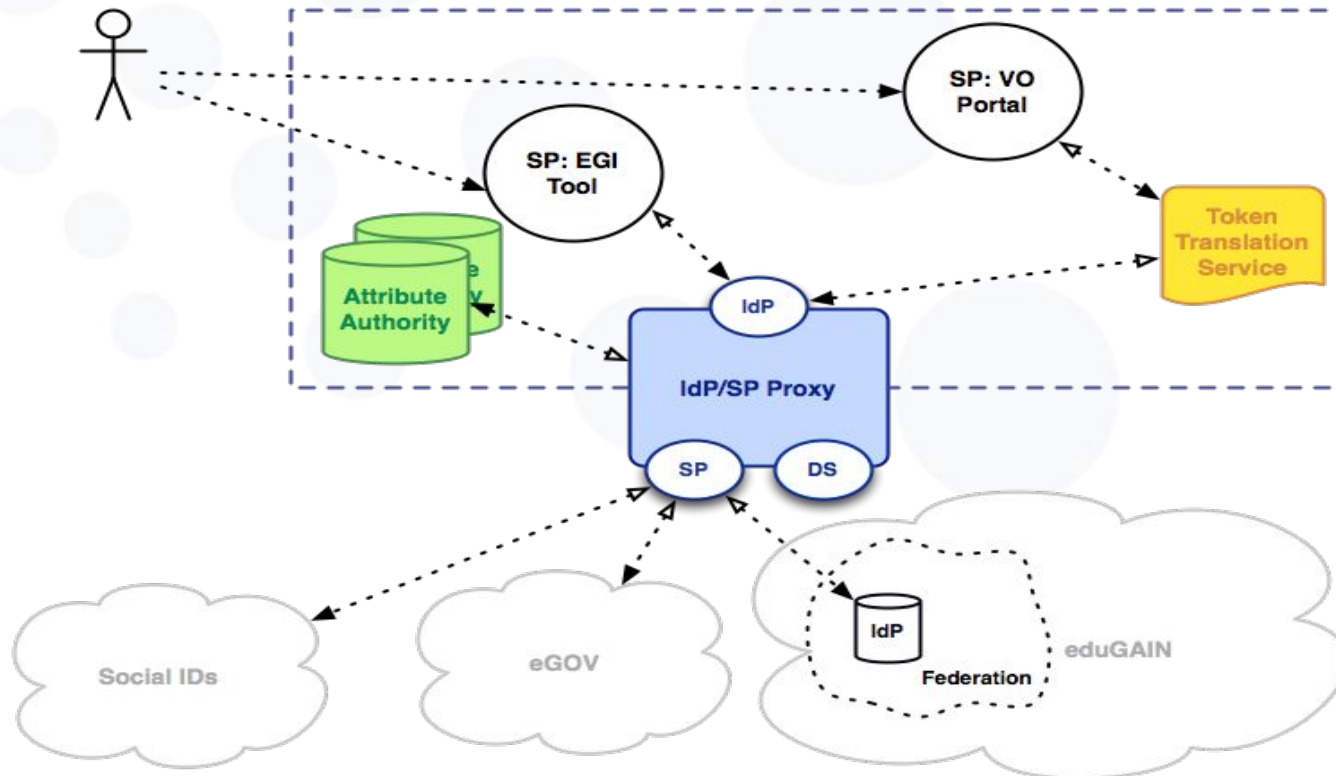
Month	Milestone - Deliverable	Title
M16 Aug-2016	M3.4	Pilot services and best practices to enable federated AAI solutions released
M24 Feb-2017	D3.9	Identity Management for Distributed User Communities report

EGI AAI Requirements

1. Users should be able to access the EGI Services using the credentials they have from their Home Organizations using eduGAIN when possible
 - a. Users should be able to access the EGI services using credential from an IdP not part of the eduGAIN. As long as the IdP fulfills a certain set of requirements.
 - b. 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.
2. EGI should expect to receive from the user's Home Organization at least an identifier that uniquely identifies the user coming from within the scope of that organization.
3. Within the EGI environment, a user should have one persistent non-reassignable non-targeted unique identifier.
4. EGI should define a set of minimum mandatory attributes, without which a user cannot exist within the EGI environment.
5. EGI should attempt to retrieve these attributes from the user's Home Organization. If this is not possible, then an alternate process should exist in order to acquire and verify the missing user attributes.
6. There should be a distinction (LoA) between self-asserted attributes and the attributes provided by the Home Organization/VO
7. Access to the various services should be granted based on the VO/EGI roles the user have.
8. EGI Services should not have to deal with the complexity of multiple IdPs/Federations/Attribute Authorities/technologies. This complexity should be handled centrally and should be hidden to the EGI Services.

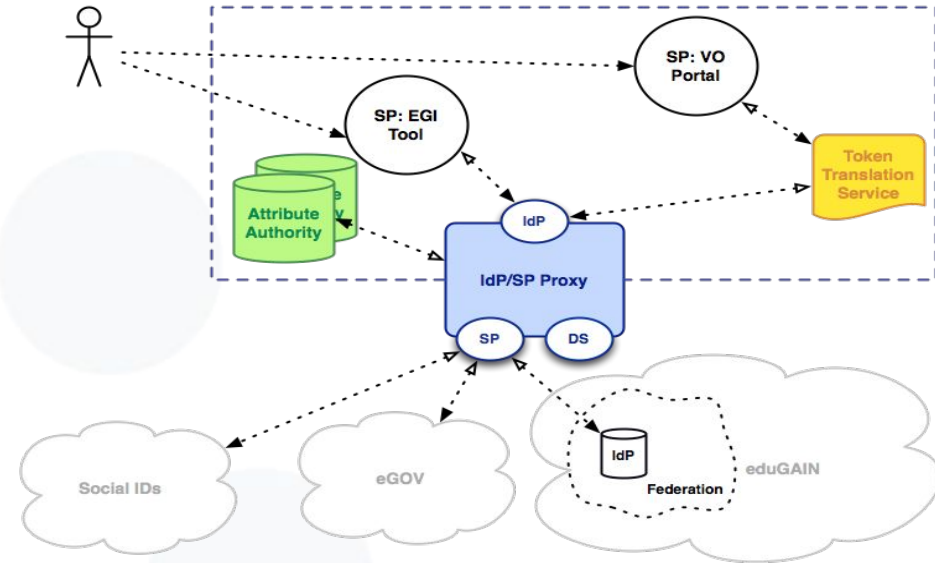
AAI Pilot & Architecture

- **May 2015:** Introduction of the EGI AAI Roadmap and Architecture



AAI Pilot & Architecture

- **Use case 0 - IdP/SP proxy**
- **Use case 1 - Attribute Authorities (Internal)**
 - Use case 1.1 - Perun
 - Use case 1.2 - GOCDB
- **Use case 2 - Token Translation**
 - Use case 2.1 - Token Translation with CILogon
 - Use case 2.2 - Token Translation with PUSP
- **Use case 3 - Hybrid stack SAML / OpenID Connect**

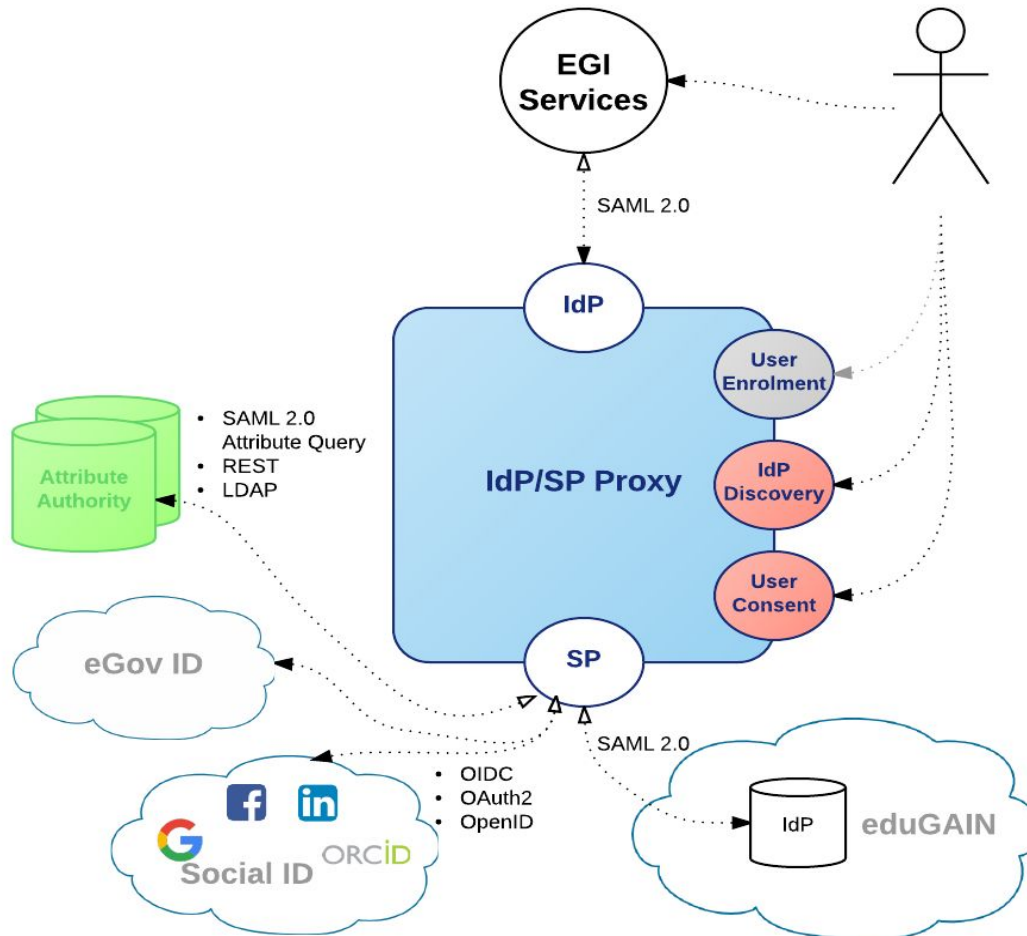


Why Proxy?

- All EGI SPs can have one statically configured IdP
- No need to run an IdP Discovery Service on each EGI SP
- Connected SPs get consistent/harmonised user identifiers and accompanying attribute sets from one or more AAs that can be interpreted in a uniform way for authZ purposes
- External IdPs only deal with a single EGI SP proxy

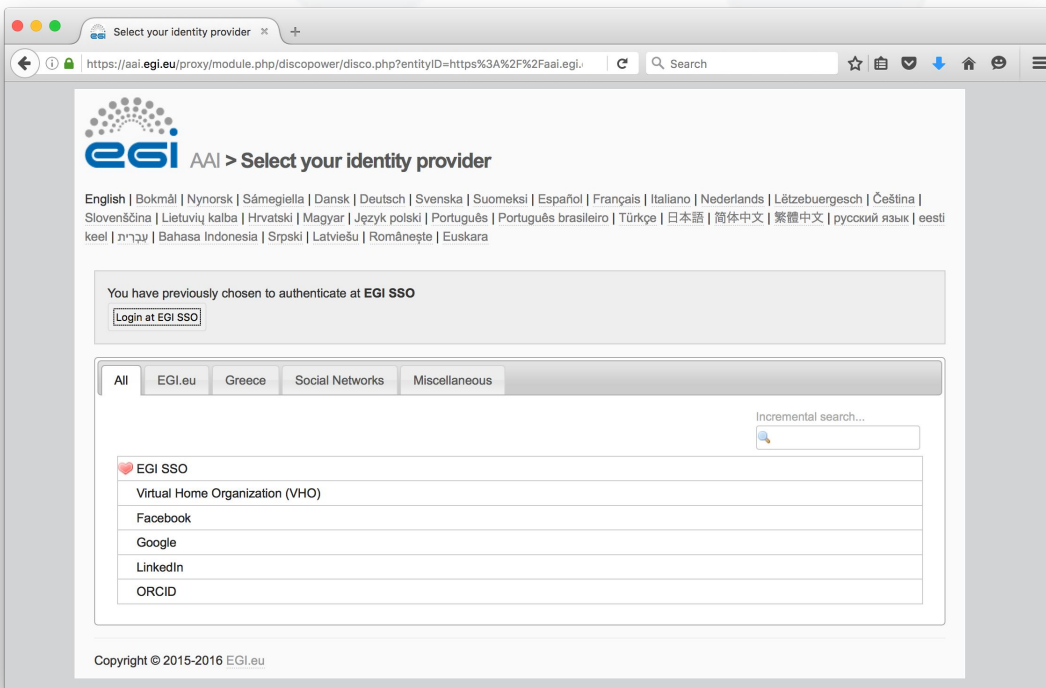
In a nutshell: EGI services will not have to deal with the complexity of multiple IdPs/Federations/Attribute Authorities/technologies. This complexity will be handled centrally by the proxy.

Use case 0: IdP/SP Proxy



- Based on OpenConnex Core Engine (simpleSamlPhp)
- IdP Discovery
- User Enrolment
- User Consent
- Support for LoA
- Attribute Queries
 - SAML2.0 Attribute Query, REST, LDAP
- Support for OIDC/OAuth2
 - Google, Facebook, LinkedIn, ORCID
- Support for SAML STORK
 - eGOV IDs (Experimental)

Use case 0: IdP/SP Proxy



- Based on OpenConnex Core Engine (simpleSamlPHP)
- IdP Discovery
- User Enrolment
- User Consent
- Support for LoA
- Attribute Queries
 - SAML2.0 Attribute Query, REST, LDAP
- Support for OIDC/OAuth2
 - Google, Facebook, LinkedIn, ORCID
- Support for SAML STORK
 - eGOV IDs (Experimental)

Use case 0: IdP/SP Proxy

Levels of Assurance

- EGI AAI proposal for 3 levels of assurance. Each level is represented by a URI:
 - Low: Authentication through a social identity provider → <https://aai.egi.eu/LoA#Low>
 - Substantial: Password authentication at the user's home IdP → <https://aai.egi.eu/LoA#Substantial>
 - High: Substantial + multi-factor authn (not yet supported, TBD) → <https://aai.egi.eu/LoA#High>
- TODO: Create an appropriate document for each LoA (this may be, but does not have to be, referenced by the URI above).

Use case 0: IdP/SP Proxy

Levels of Assurance

- **3 Use Cases:**
 - allow an IdP to advertise those LoAs for which it is able to meet the associated requirements
 - allow an IdP to indicate the actual LoA in its responses
 - allow a SP to express its expectations for the LoA at which a user should be authenticated

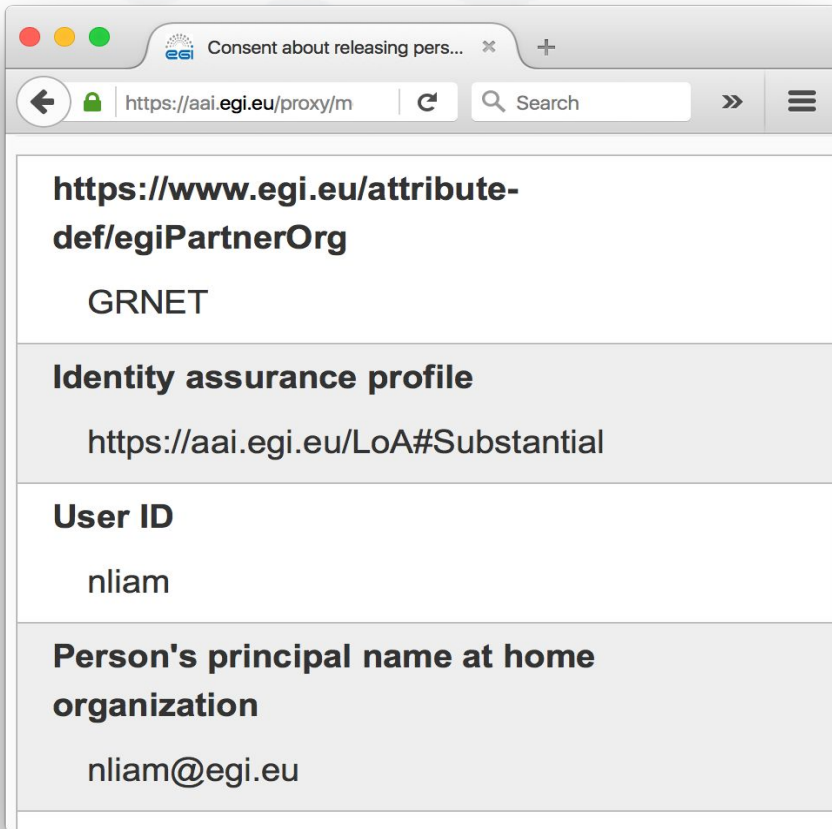
Use case 0: IdP/SP Proxy

Levels of Assurance: IdP SAML2 Metadata

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" [...] entityID="https://aai.egi.eu/proxy/saml2/idp/metadata.php">
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oasis:names:tc:SAML:attribute:assurance-certification" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" xsi:type="xs:string">https://aai.egi.eu/LoA#Low</saml:AttributeValue>
        <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" xsi:type="xs:string">https://aai.egi.eu/LoA#Substantial</saml:AttributeValue>
        <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" xsi:type="xs:string">https://aai.egi.eu/LoA#High</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
```

Use case 0: IdP/SP Proxy

Levels of Assurance: User Attribute Assertions



Consent about releasing pers... x +

https://aai.egi.eu/proxy/m

<https://www.egi.eu/attribute-def/egiPartnerOrg>

GRNET

Identity assurance profile

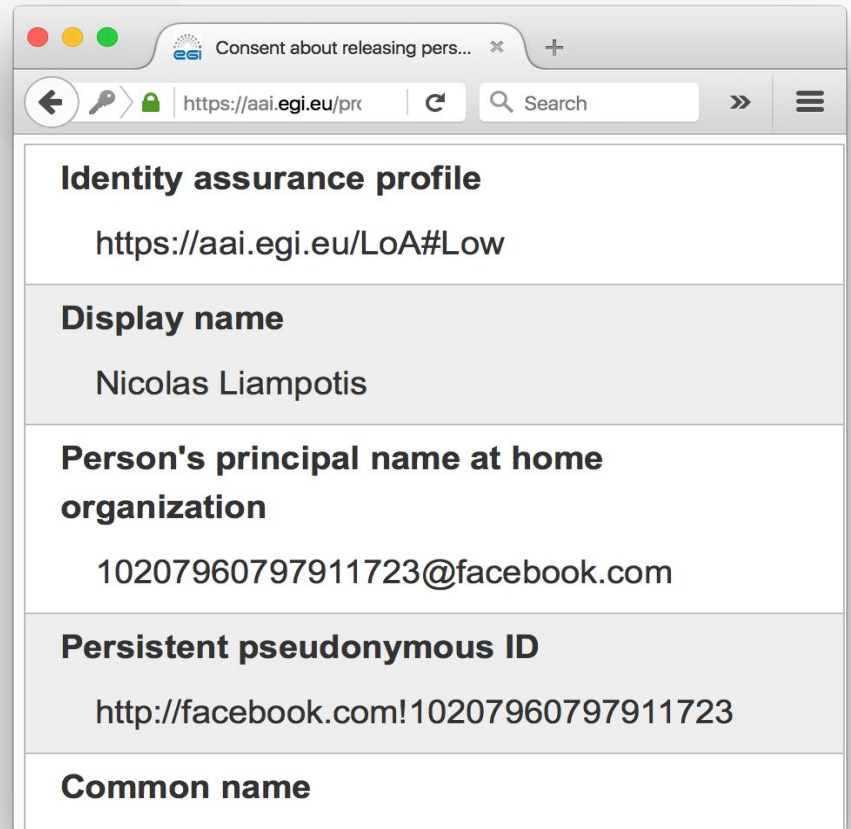
<https://aai.egi.eu/LoA#Substantial>

User ID

nliam

Person's principal name at home organization

nliam@egi.eu



Consent about releasing pers... x +

https://aai.egi.eu/prc

Identity assurance profile

<https://aai.egi.eu/LoA#Low>

Display name

Nicolas Liampotis

Person's principal name at home organization

10207960797911723@facebook.com

Persistent pseudonymous ID

<http://facebook.com!10207960797911723>

Common name

Use case 0: IdP/SP Proxy

Levels of Assurance: AuthnContextClassRef

```
<saml:AuthnStatement AuthnInstant="2016-03-02T16:11:05Z"  
SessionNotOnOrAfter="2016-03-03T00:11:05Z" SessionIndex="  
_a7f1c5f62cc2df3c99ba5bbc4c2dc1aad2adcc8b8a">  
  <saml:AuthnContext>  
    <saml:AuthnContextClassRef>  
      https://aai.egi.eu/LoA#Substantial  
    </saml:AuthnContextClassRef> <saml:AuthenticatingAuthority>https://www.  
egi.eu/idp/shibboleth</saml:AuthenticatingAuthority>  
  </saml:AuthnContext>  
</saml:AuthnStatement>  
<saml:AttributeStatement>
```

Use case 0: IdP/SP Proxy

EGI User Identifier

The EGI User ID should be:

- **personal** - used by a single person (as opposed to shared user accounts)
- **persistent** - used for an extended period of time across multiple sessions
- **non-reassignable** - assigned exclusively to a specific person, and never reassigned to another individual
- **non-targeted** - not intended for a specific relying party (or parties), i.e. should be shared
- **globally unique** - unique beyond the namespace of the IdP and the namespace of the SP(s) with which the ID is shared
- **opaque** - should (by itself) provide no information about the user, i.e. should be privacy-preserving

Use case 0: IdP/SP Proxy

Available identifiers

- **eduPersonPrincipalName (ePPN)** - A name-based identifier for a person in the form "user@scope" where the "scope" portion is the administrative domain of the identity system where the identifier was created and assigned.
- **eduPersonTargetedID (ePTID)** - A persistent, non-reassigned, opaque identifier for a principal.
- **eduPersonUniqueId (ePUID)** - A long-lived, non re-assignable, omnidirectional identifier suitable for use as a principal identifier by authentication providers or as a unique external key by applications.

	ePPN	ePTID	ePUID
personal	✓	✓	✓
persistent	✓	✓	✓
non-reassignable	✗	✓	✓
non-targeted	✓	✗	✓
globally unique	✓	✓	✓
opaque	✗	✓	✓

Use case 0: IdP/SP Proxy

EGI Unique User Id Generation

The IdP/SP Proxy adds (or replaces) the eduPersonUniqueId (urn:oid:1.3.6.1.4.1.5923.1.1.1.13) attribute, based on the first non-empty value from this attribute list:

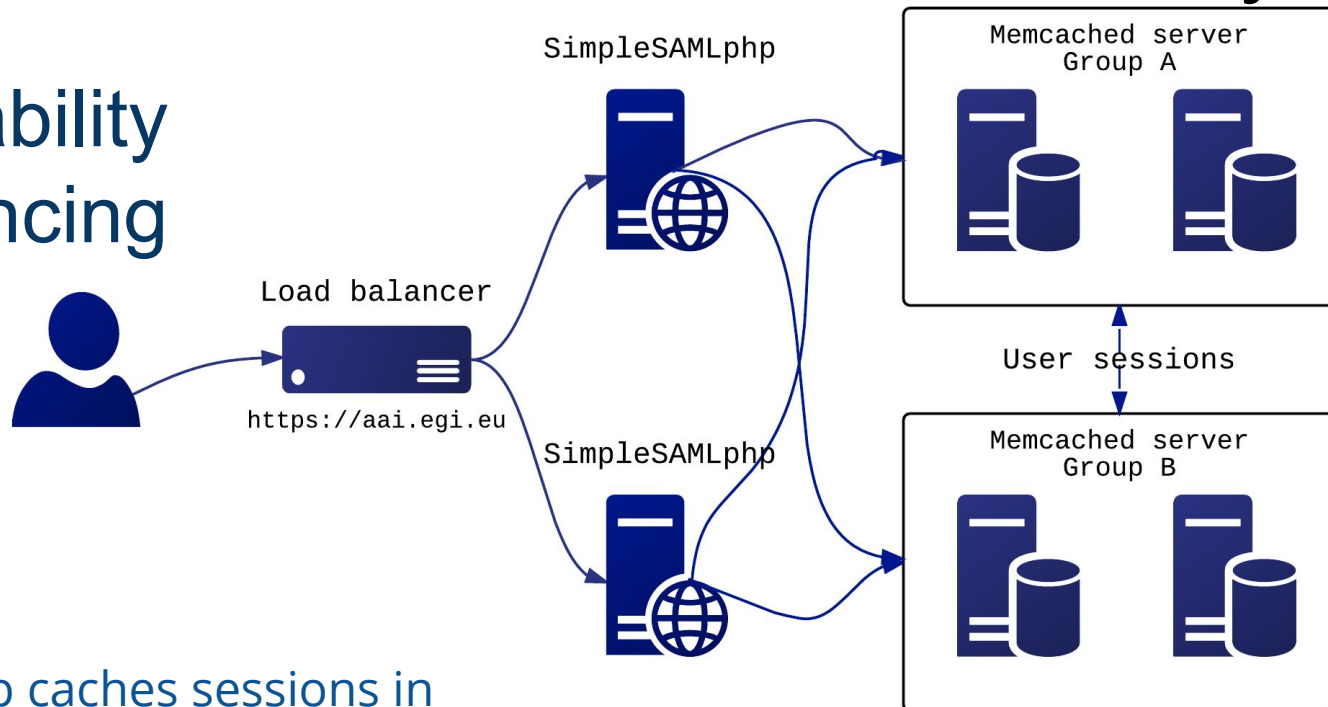
- ePUID
- ePPN
- ePTID

The selected attribute value is hashed and the “egi.eu” scope portion is added to the generated ePUID, e.g.:

```
ef72285491ffe53c39b75bdcef46689f5d26ddfa00312365cc4fb5ce97e9ca87@egi.eu
```

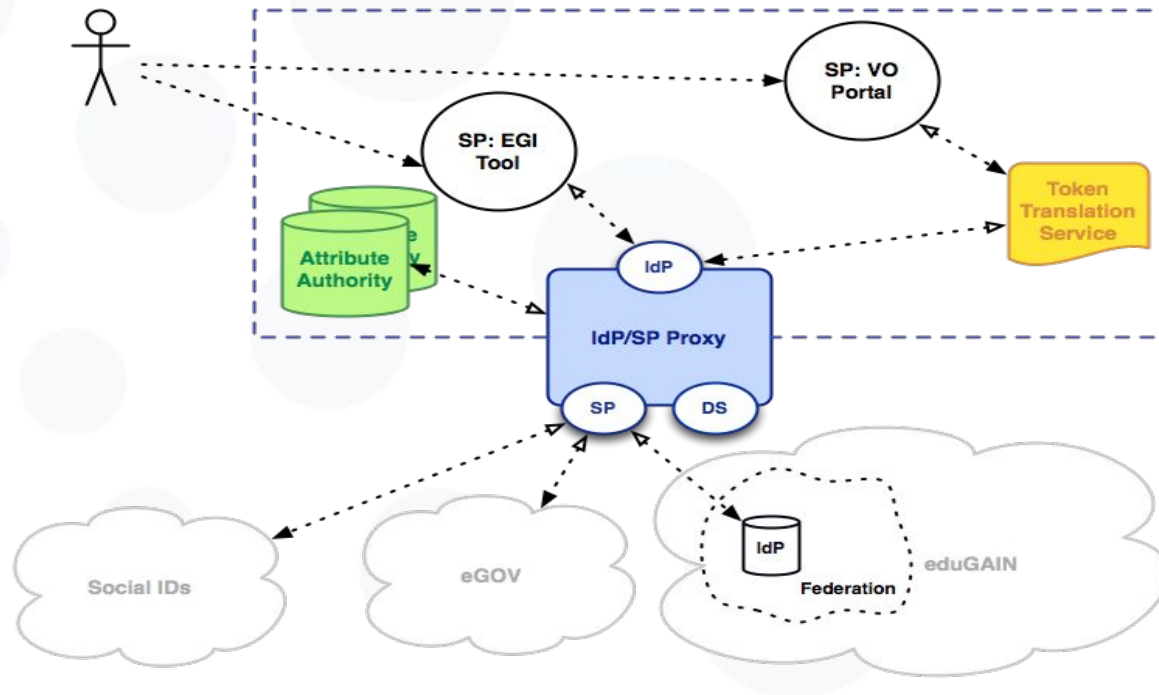

Use case 0: IdP/SP Proxy

High Availability & Load Balancing



- SimpleSAMLphp caches sessions in Memcached, an in-memory key-value store for small chunks of arbitrary data
- Sessions are distributed and replicated among different Memcached servers, enabling load-balancing and fail-over
- User requests are load balanced among multiple SimpleSAMLphp web front-ends that use the back-end matrix of Memcached servers

Use case 1: Attribute Authorities



- Use case 1.1 - Connection with Perun - **DONE**
- Use case 1.2 - Connection with GOCDB - **In progress**
- Use case 1.3 - Connection with COmanage - **DONE**
- Use case 1.4 - Connection with the new OpenConnex Attribute Aggregator - **In progress**

Use case 1: Attribute Authorities

The EGI SP proxy supports attribute aggregation through:

- **LDAP Attribute Aggregator**
 - SimpleSAMLphp module
 - Allows SSP to issue LDAP queries for retrieving attributes
- **AQ Attribute Aggregator**
 - SimpleSAMLphp module
 - Enables SSP to issue SAML 2.0 attribute queries to Attribute Authorities that support SAML 2.0 SOAP binding
- **OpenConext attribute aggregation**
 - Java application
 - Handles attribute aggregation and provides REST API for accessing attribute information

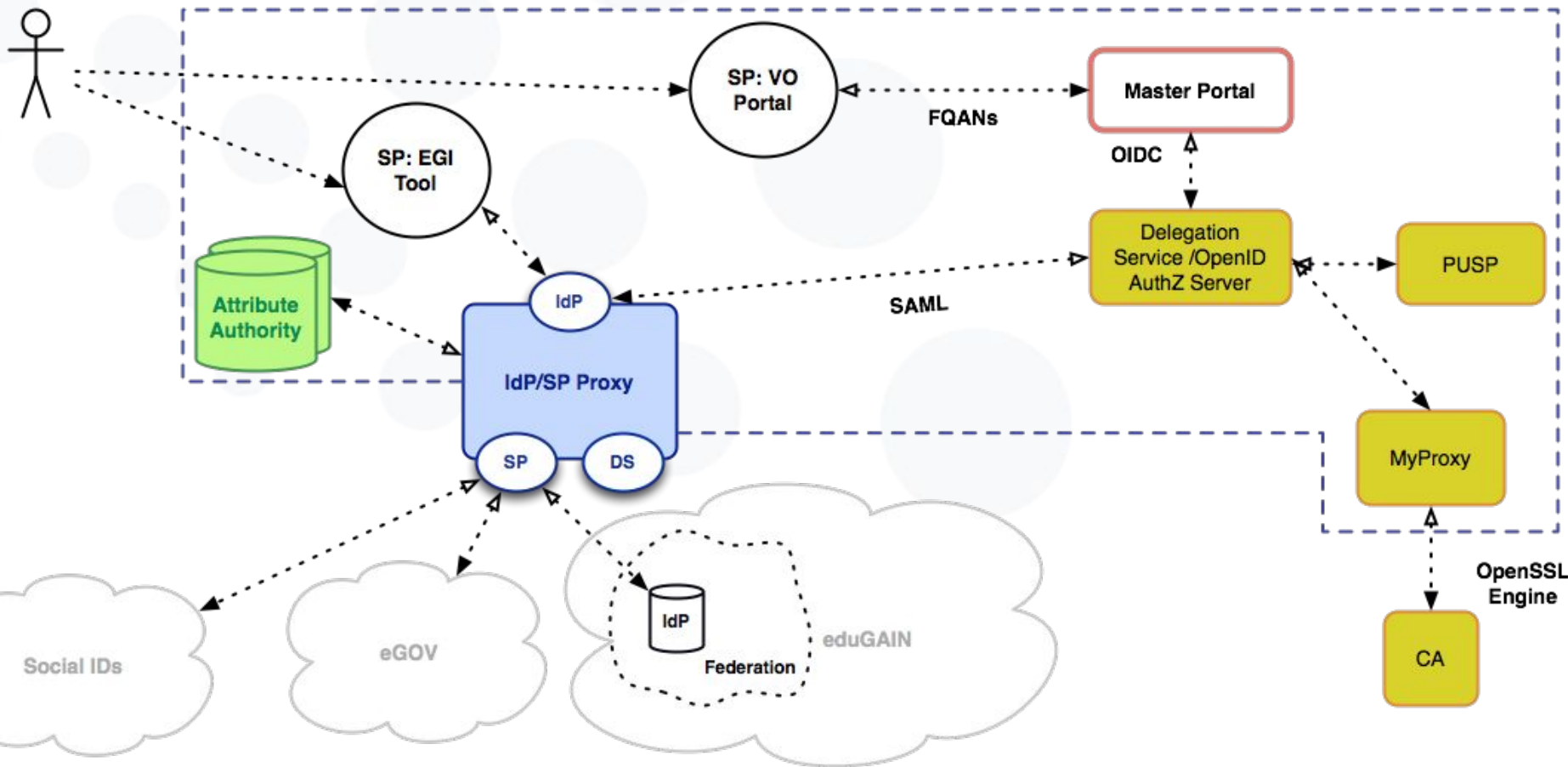
Use case 1: Attribute Authorities

eduPersonUniqueId	urn:oid:1.3.6.1.4.1.5923.1.1.1.13	✓
eduPersonPrincipalName	urn:oid:1.3.6.1.4.1.5923.1.1.1.6	✓
eduPersonTargetedID	urn:oid:1.3.6.1.4.1.5923.1.1.1.10	✓
displayName	oid:2.16.840.1.113730.3.1.241	✓
sn	urn:oid:2.5.4.4	✓
givenName	urn:oid:2.5.4.42	✓
mail	urn:oid:0.9.2342.19200300.100.1.3	✓
eduPersonAssurance	urn:oid:1.3.6.1.4.1.5923.1.1.1.11	✓
eduPersonEntitlement	urn:oid:1.3.6.1.4.1.5923.1.1.1.7	✓
eduPersonScopedAffiliation	urn:oid:1.3.6.1.4.1.5923.1.1.1.9	?

CoCo & R&S compliance

```
<md:EntityDescriptor entityID="https://aai.egi.eu/proxy/module.php/saml/sp/metadata.php/sso">
  <md:Extensions>
    <mdattr:EntityAttributes xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <saml:Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="http://macedir.org/entity-category" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" xsi:type="xs:string">http://www.geant.net/uri/dataprotection-code-of-conduct/v1</saml:AttributeValue>
        <saml:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" xsi:type="xs:string">http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
      </saml:Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
</md:EntityDescriptor>
```

Use case 2: Token Translation: CILogon + PUSP



Timeline	Expected Result	Required Technical Components	Status
2015-Q4	EGI IdP/SP deployed	SimpleSamI PHP / OpenConnex	Done
2015-Q4	Interconnect the EGI IdP/SP with a SAML 2.0 IdP	SAML 2.0	Done
2015-Q4	Interconnect the EGI IdP/SP with a SAML 2.0 SP	SAML 2.0	Done
2015-Q4	Interconnect the EGI IdP/SP with Perun as attribute provider	PERUN, SimpleSAMLphp LDAP Connector	Done

Timeline	Expected Result	Required Technical Components	Status
2016-Q1	EGI IdP/SP OIDC input interface (OIDC → SAML)	OIDC Connector	DONE
2016-Q1	Interconnect the EGI IdP/SP with GOCDB as attribute provider	GOCDB, GOCDB connector	DONE
2016-Q1	Interconnect the EGI IdP/SP with CILogon based Token Translation Services	CILogon, MyProxy	DONE
2016-Q1	Interconnect the EGI IdP/SP with PUSPs based Token Translation Services	eToken Server and/or MyProxy	DONE
2016-Q1	First pilot with EGI operational tools (AppDB, GOCDB)	N.A.	DONE

Timeline	Expected Result	Required Technical Components	Status
2016–Q2	EGI AAI published in eduGAIN		In progress
2016–Q2	EGI AAI Enrollment Service	COmanage	In progress
2016–Q2	EGI IdP/SP Proxy Attribute Aggregation	OpenConext	In Progress
2016–Q2	Pilot with selected use cases from the EGI-Engage Competence Centers (ELIXIR, DARIAH)		Planning
2016–Q3	EGI AAI OpenID Connect Provider		Planning
2016–Q3	Interconnect the EGI IdP/SP proxy with an OIDC service (OneData?)		Planning
2016–Q3	Second pilot with selected use cases from the EGI-Engage Competence Centers		
2016–Q3	Technology reassessment and definition of the roadmap until the end of the EGI-Engage project		

Thank you for your attention.

Questions?



www.egi.eu

This work by Parties of the EGI-Engage Consortium is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

