Greek Research and Technology Network

Authentication and Authorisation Infrastructure

grnet

Διασυνδέοντας την Έρευνα και την Εκπαίδευση

Policy and procedures

Version 1.1.0

February 2012

Contents

d

d

1 Introduction

The *Authentication and Authorisation Infrastructure* (*AAI*) facilitates the cooperation of different organisations towards the goal of allowing users to access inter-organisation services. Through the infrastructure, users of the Federation can receive services in a secure and confidential manner, by using only their institutional account.

The Federation consists of the following three (3) categories of entities:

1. *Identity Providers* (*IdP*): are entities (e.g. academic foundations, research institutes etc.) that authenticate their users and certify the identity of them. Additionally, they may, in their discretion, send limited users' data to service providers.
2. *Service Providers* (*SP*): are entities that provide services to the users of academic, research and educational community. They may receive individual user data by Identity Providers, with their permission, for user authorisation and to provide personalised services.
3. *Federation Coordinator*: manages the processes of integration and withdrawal of the members from the Federation and coordinates the cooperation between them, monitors the compliance of the members with the Federation's policy, maintains the necessary infrastructure for the operation of the Federation (e.g. WAYF/DS, metadata) and promotes the development of services of institutional character.

   "Greek Research and Technology S.A." (GRNET) is defined as the coordinator of this Federation.

2 Conditions for participation

2.1 Formal requirements

Identity Providers and Service Providers are able to join or leave the Federation by applying to the Coordinator. Participation to the federation requires the agreement with this policy document and compliance with the terms and conditions that arise from it.

In the Federation **only** institutions of academic, research and education community of Greece can participate as Identity Providers and each institution may take part with a single Identity Provider in the infrastructure. The academic, research or educational nature of the organisation may be decided by the Coordinator at his discretion. In addition, the Coordinator may exceptionally add Identity Providers to the Infrastructure that do not meet the above criteria to serve specific purposes, such as virtual IdPs to serve guest users of the federations or to peer with other federations.

Any organisation can participate in the Infrastructure as a Provider of one or more services provided that these services promote the academic, research or educational work. There are no restrictions regarding the non-profit nature of the organisation, but in the case the organisation does not also participate as an Identity Provider, it is necessary for at least one Identity Provider to express interest in accessing the particular service; this interest should be formally expressed to the Coordinator.

2.2 Abuse

Each Identity Provider or Service Provider involved in the Federation must comply with the requirements of this document. In the case that the provider is found to violate one the requirements and if it is deemed that such a violation may result in a security breach and possibly in a personal data leakage, the Coordinator may temporarily suspend the provider's access to the federation.

The Coordinator shall not be held responsible if there are violations of this particular text or security breaches, that may lead to possible loss or damage, including personal data leak, where the loss is not related to his failure or neglect.

In case of abuse, the affected party may request compensation by the Service Provider or Identity Provider, which is responsible for the loss of personal data or any other possible damage. Responsible for resolving disputes are courts of the Hellenic Republic. The affected parties may notify the Coordinator for the dispute; however, his actions in relation to their participation in the infrastructure remain in his discretion.

3 Procedures

3.1 End-user support

End-user support is implemented at the first tier by the Identity Provider's service desk and not by the Service Providers or the Coordinator. For this purpose, Identity Providers must inform the Coordinator of the user support contact point (e-mail address and/or telephone number). This contact point may be publicly announced on the site of the infrastructure as well as to pages of the respective services.

In case that a problem resides in a Service Provider, the Identity Providers' administrators may contact the Service Provider directly, without the mediation or assistance of the Coordinator.

Both Identity Providers and Service Providers must keep the Coordinator informed for the technical/administrative contact points. These data are communicated to the Federation members but may not posted on the website of the infrastructure or the end-user web pages of the services.

3.2 Maintenance of metadata

The Coordinator assumes full maintenance of metadata[1] of the Infrastructure, including the members addition and removal from it, according to this policy document. The Coordinator can re-issue the metadata at any time. The metadata are signed by a predetermined digital certificate and with an expiry date in the site of the Infrastructure.

The members of the Federation have to update to the latest version of the metadata at least **once a day** and it is recommended to do that at least **every hour**.

[1] The data defining the infrastructure comprising of IdPs and SPs, according to the standard SAML V2.0[7]

3.3 Personal data

Members of the Federation are obliged to protect the personal data of the end users, in accordance with the requirements of current legislation (especially the laws on protection of personal data and the requirements of the respective Independent Authority) to the maximum extent possible.

The Identity Providers of the Infrastructure must ensure the legitimate and safe personal data transmission to the Service Providers while the Service Providers, in turn, must use and store the fewest personal data that are required for the proper functioning of their services in accordance with the currently existing legal framework.

The Coordinator assumes no responsibility for the maintenance of these obligations of its members and does not distribute or retain users data through the Infrastructure; the transmission of data is carried directly by the Identity Providers to the Service Providers.

3.4 Security and confidentiality requirements

Communication between Identity Providers and Service Providers of the infrastructure must be encrypted, based on technical specifications and standards that are referred in the respective section below.

In addition, the communication between Service Providers and users must be encrypted, if personal data are transmitted and it is recommended that the communication between Identity Providers and users should also be encrypted.

The members of the academic, research or educational community can, either as Identity Providers or Service Providers, receive digital certificates from the PKI service of GRNET. These certificates are internationally recognised and accepted by all modern browsers.

Moreover, to avoid a security vulnerability known as a ”replay attack”, the members of the infrastructure have to maintain time synchronised to a reliable source. The use of NTP protocol is recommended and the NTP source of the Coordinator may be used as a time source (*ntp.grnet.gr*).

Identity Providers have to keep log files related to the disclosure of personal data of the users. The data should be retained for a sufficient period of time in accordance with the policy of retention of each organisation and the legislation. It is recommended that Identity Providers should retain data for a period of time of at least 6 months.

Any incidents of security breach and/or possible loss of personal data at any point of communication and by any party, should be communicated directly to the CERT team of the Coordinator so that they can be handled in coordination.

4 Infrastructure

The Infrastructure is composed of both Identity Providers and Service Providers. The SAML standard (Security Assertion Markup Language) of the OASIS international standards organisation is employed for communication between parties; the standard is based on XML language and utilises transport encryption (SSL/TLS) as well as encrypted exchange messages (XML Signature/XML encryption). The standard has prevailed in the federations both in European academic communities as well as the U.S.A. one.

To be able to identify users with just their institutional accounts, it is essential that each Identity Provider that participates in the federation, is using a Directory Service that includes most, if not all, of its members. It is customary that this service is provided with software that uses the LDAP protocol (RFC 4510[8]).

Although the infrastructure was originally implemented using the SAML standard version V1.0[9] and V1.1[10] as well as extensions that were produced by the Shibboleth software, nowadays **only** the SAML V2.0[11] standard is used in the Infrastructure.

All members of the Infrastructure, both Identity Providers and Service Providers must implement at least this version of the standard; the implementation of other versions or other standards within the same Infrastructure is not prohibited but members are cautioned that this may affect potential troubleshooting efforts.

The SAML 2.0 standard allows great flexibility in its use, allowing customisations in each implementation and therefore hurting interoperability.

In this Infrastructure a subset of the standard and specifically *"Interoperable SAML 2.0 Profile"* is being used. Thus, the implementation of the most current version of the profile is mandatory; the current version may always be found in the website `http://saml2int.org/profile/current`.

5 Attributes

5.1 Communicating attributes

Each Identity Provider may set a, so called, “attribute release policy” for each Service Provider at its discretion, with the purpose of protecting the privacy of their users. However, transmitting false data for any purpose is prohibited.

Furthermore, it is suggested to Identity Providers to allow their users consent to the transmission of their data [2].

However, the transmission of the unique, targeted, identifier (see the dedicated section below) to every Service Provider is strongly recommended as it allows Service Providers to distinguish users while at the same time protecting the privacy of personal data.

Similarly, the acceptance and use, for any purpose, of data received is at the discretion of the Service Providers as long as there is no violation of this policy and effective legislation. It is recommended to Service Providers to notify the Coordinator for the data required for the proper operation of the Service, so that these requirements can be published at the metadata.

5.2 Relation to LDAP attributes

The method of implementation of the local Directory Service is within the organisation’s borders and hence out of the scope of this text. However, there are dependencies of the Infrastructure to Directory Service and in particular, in the attributes needed by it. Although the implementation of the Identity Provider infrastructure does not have to take place completely using the LDAP/X.500[3] standards, terminology and nomenclature of these standards are used in the Infrastructure[12].

[2] An example of a software method to implement that is the uApprove software package created by SWITCH, the Swiss NREN.

[3] It is common that some attributes are dynamically generated by Identity Providers based on other attribute values.

More specifically, in the Infrastructure, user attribute names are based on the following LDAP schemas:

- Base LDAP schemas, as defined in RFC 4519[14]
- `inetOrgPerson`, as defined in RFC 2798[15]
- `COSINE`, as defined in RFC 4524[16]
- `eduPerson`, version 200806[17]
- `SCHAC`, version v1.4.0 [18]
- `grEduPerson`, version v1.0[19]

5.3 Mandatory attributes

The existence of the following attributes is **mandatory** for all physical persons contained in the federation:

- `givenName`
- `sn`
- `cn` or `displayName`
- `eduPersonPrincipalName`
- `eduPersonAffiliation`
- `schacHomeOrganization`

In addition to the above, and especially for undergraduate students, the existence of the following attributes is mandatory:

- `schacPersonalUniqueCode`
- `grEduPersonUndergraduateBranch`

It should be noted, however, that the mandatory existence of attributes does not necessarily presupposes their availability to all services.

5.4 Targeted ID

Each user receives a unique, non-personalised, attribute for each combination of Identity Provider and Service Provider. This attribute must not include any personal data of the user, such as its username or its full name. It must not exceed 256 characters in length and may be in non human-readable format.

The attribute is unique per Service Provider as to protect the privacy of personal data, since in this way, two Service Providers can not correlate the information held on a user to create a more extensive user profile.

This attribute is commonly used to provide personalised services and to collect browsing statistics (e.g. unique visitor count). It can be used also for protecting Services from abuse or potential attacks; consequently, Identity Providers must be able to have the capability of reverse searching for a user, given the unique identifier, in a security incident situation, as to be able to identify the attacker's identity.

This identifier is sent by Identity Providers in the `Subject` of the SAML `Assertion` and specifically with the title `NameID`. Since this form was absent in the first versions of SAML standard, it was common to send this identifier in the value of the attribute `eduPersonTargetedId`; this notation should be avoided nowadays. For Identity Providers, the transmission of the attribute in the `Subject` is mandatory while the transmission as `eduPersonTargetedId` is optional; for Service Providers, accepting this attribute from any source is allowed as long as the value in `Subject` prevails over the others[4].

5.5 Personal characteristics

5.5.1 cn

OID	`2.5.4.3`
Shibboleth 1.x	`urn:mace:dir:attribute-def:cn`
SAML 2.0	`urn:oid:2.5.4.3`
Single-valued	no
Source	RFC 4519

The full name of the person. The use of the legal name of the person is recommended. The use of multiple values of the field is typically allowed, but it is recommended to be avoided.

[4] Detailed information on the subject are on page https://spaces.internet2.edu/display/SHIB2/NativeSPTargetedID.

Example: Maria-Anna Papadopoulou

5.5.2 displayName

OID	2.16.840.1.113730.3.1.241
Shibboleth 1.x	urn:mace:dir:attribute-def:displayName
SAML 2.0	urn:oid:2.16.840.1.113730.3.1.241
Single-valued	yes
Source	RFC 2798

The full name of the person, with the preferred format as selected by the person itself.

Example: Marianna Papadopoulou

5.5.3 givenName

OID	2.5.4.42
Shibboleth 1.x	urn:mace:dir:attribute-def:givenName
SAML 2.0	urn:oid:2.5.4.42
Single-valued	no
Source	RFC 4519

The given name of the person, also known as “first name”; may take multiple values.

Example: Mary, Anna

5.5.4 eduPersonNickname

OID	1.3.6.1.4.1.5923.1.1.1.2
Shibboleth 1.x	urn:mace:dir:attribute-def:eduPersonNickname
SAML 2.0	urn:oid:1.3.6.1.4.1.5923.1.1.1.2
Single-valued	no
Source	eduPerson

The name of the person, in a “friendly” form (nickname). Not recommended to use.

Example: `Miranna`

5.5.5 sn

OID	`2.5.4.4`
Shibboleth 1.x	`urn:mace:dir:attribute-def:sn`
SAML 2.0	`urn:oid:2.5.4.4`
Single-valued	no
Source	RFC 4519

The surname of the person; it may take multiple values, but it is recommended that this should be avoided. If a person has multiple surnames, it is suggested to store them in a single value, separating them with a hyphen or space.

Example: `Papadopoulou`, `Papadopoulou-Konstantatou`

5.5.6 schacSn1, schacSn2

OID	`1.3.6.1.4.1.25178.1.2.6`
Shibboleth 1.x	`urn:mace:terena.org:schac:attribute-def:schacSn1`
SAML 2.0	`urn:oid:1.3.6.1.4.1.25178.1.2.6`
Single-valued	no
Source	SCHAC

OID	`1.3.6.1.4.1.25178.1.2.7`
Shibboleth 1.x	`urn:mace:terena.org:schac:attribute-def:schacSn2`
SAML 2.0	`urn:oid:1.3.6.1.4.1.25178.1.2.7`
Single-valued	no
Source	SCHAC

The first name and second surname of the person, respectively. The separation of the first and the second surname should be done manually and not in an automated fashion. The use of these attributes is not recommended.

5.5.7 uid

OID	`0.9.2342.19200300.100.1.1`
Shibboleth 1.x	`urn:mace:dir:attribute-def:uid`
SAML 2.0	`urn:oid:0.9.2342.19200300.100.1.1`
Single-valued	no
Source	RFC 4519

It is the person's login name for services. It can take many values, although it is common and suggested to take only one. It is recommended that the values are unique within the own organisation but since it is not possible to be unique across the Federation its use should be avoided by the Service Providers; the eduPersonPrincipalName alternative should be used instead.

5.5.8 eduPersonPrincipalName

OID	`1.3.6.1.4.1.5923.1.1.1.6`
Shibboleth 1.x	`urn:mace:dir:attribute-def:eduPersonPrincipalName`
SAML 2.0	`urn:oid:1.3.6.1.4.1.5923.1.1.1.6`
Single-valued	yes
Source	eduPerson

An attribute *unique* across the whole *Federation*; usually, this is an inter-institutional username. It takes the values of the `user@domain` form, and although it has a similar form with an e-mail address (and hence the `mail` attribute), their values are not necessarily the same.

Two different persons should **never** be assigned to have the same value, either simultaneously or at different time periods; in other words, each value given forever only once.

A user, however, can acquire a different attribute value, in the Identity Provider's discretion. However, since the value has usually been exposed to Service Providers, this should be done with special attention and sparingly as it is likely to have been used e.g. as a primary key in a service database.

5.5.9 userPassword

OID	`2.5.4.35`
Shibboleth 1.x	`urn:mace:dir:attribute-def:userPassword`
SAML 2.0	`urn:oid:2.5.4.35`
Single-valued	no
Source	RFC 4519

The personal password of the user, accompanied by the encoding method. This should **never** be sent to Service Providers.

5.5.10 preferredLanguage

OID	`2.16.840.1.113730.3.1.39`
Shibboleth 1.x	`urn:mace:dir:attribute-def:preferredLanguage`
SAML 2.0	`urn:oid:2.16.840.1.113730.3.1.39`
Single-valued	yes
Source	RFC 2798

The preferred language of written or verbal communication of the person. The possible values are defined in ISO 639[21] and RFC 2616[22]. Caution is required for the code distinction of the Greek language (`el`) and Greece (`gr`).

5.5.11 schacMotherTongue

OID	`1.3.6.1.4.1.25178.1.2.1`
Shibboleth 1.x	`urn:mace:terena.org:schac:attribute-def:schacMotherTongue`
SAML 2.0	`urn:oid:1.3.6.1.4.1.25178.1.2.1`
Single-valued	yes
Source	SCHAC

The mother language of the person, the language who is learnt first. The possible values are defined in RFC 5646[23]. Caution is required for the code distinction of the Greek language (`el`) and Greece (`gr`).

Examples: `el`, `el-GR`, `en-GB`.

5.5.12 schacGender

OID	1.3.6.1.4.1.25178.1.2.2
Shibboleth 1.x	urn:mace:terena.org:schac:attribute-def:schacGender
SAML 2.0	urn:oid:1.3.6.1.4.1.25178.1.2.2
Single-valued	yes
Source	SCHAC

The gender of the person. The possible values are 0 (unknown), 1 (male), 2 (female), 9 (unspecified).

5.5.13 schacDateOfBirth

OID	1.3.6.1.4.1.25178.1.2.3
Shibboleth 1.x	urn:mace:terena.org:schac:attribute-def:schacDateOfBirth
SAML 2.0	urn:oid:1.3.6.1.4.1.25178.1.2.3
Single-valued	yes
Source	SCHAC

The birth date of the person. These values take the form YYYYMMDD, where YYYY is the year using four digits, MM the month using two digits and DD the day using two digits. See also RFC 3339[24], §5.6 and ISO 8601[25].

5.5.14 schacYearOfBirth

OID	1.3.6.1.4.1.25178.1.0.2.3
Shibboleth 1.x	urn:mace:terena.org:schac:attribute-def:schacYearOfBirth
SAML 2.0	urn:oid:1.3.6.1.4.1.25178.1.0.2.3
Single-valued	yes
Source	SCHAC

The date of birth of person, using four digits. see also the RFC 3339[24], §5.6 and ISO 8601[25].

5.5.15 schacPlaceOfBirth

OID	1.3.6.1.4.1.25178.1.2.4
Shibboleth 1.x	urn:mace:terena.org:schac:attribute-def:schacPlaceOfBirth
SAML 2.0	urn:oid:1.3.6.1.4.1.25178.1.2.4
Single-valued	yes
Source	SCHAC

The birthplace of the person.

Example: Athens, Greece

5.5.16 schacCountryOfCitizenship

OID	1.3.6.1.4.1.25178.1.2.5
Shibboleth 1.x	urn:mace:terena.org:schac:attribute-def:schacCountryOfCitizenship
SAML 2.0	urn:oid:1.3.6.1.4.1.25178.1.2.5
Single-valued	no
Source	SCHAC

The countries whose nationality the person has. The countries are expressed with their two-digit code in accordance with ISO 3166 standard[26]. Caution is required for the code distinction of the Greek language (el) and Greece (gr).

Example: gr

5.5.17 schacPersonalTitle

OID	1.3.6.1.4.1.25178.1.2.8
Shibboleth 1.x	urn:mace:terena.org:schac:attribute-def:schacPersonalTitle
SAML 2.0	urn:oid:1.3.6.1.4.1.25178.1.2.8
Single-valued	yes
Source	SCHAC

The title or address of the person. These values follow the definition of the `personalTitle` attribute of the RFC 4524[16] standard.

Examples: `Dr`, `Mrs`

5.6 Contact and location information

5.6.1 mail

OID	`0.9.2342.19200300.100.1.3`
Shibboleth 1.x	`urn:mace:dir:attribute-def:mail`
SAML 2.0	`urn:oid:0.9.2342.19200300.100.1.3`
Single-valued	no
Source	RFC 4519

The e-mail address or addresses of the person. These values follow the format of e-mail addresses, as defined by the RFC 5321[27] standard. It is not necessary for the address of the user to be provided by his/her respective organisation but may be any valid e-mail address.

5.6.2 telephoneNumber

OID	`2.5.4.20`
Shibboleth 1.x	`urn:mace:dir:attribute-def:telephoneNumber`
SAML 2.0	`urn:oid:2.5.4.20`
Single-valued	no
Source	RFC 4519

The telephone number of the person *at his/her organisation*. These values should follow the format of telephone numbers as defined by the ITU-T E.123[28] standard.

5.6.3 facsimileTelephoneNumber

OID	`2.5.4.23`
Shibboleth 1.x	`urn:mace:dir:attribute-def:facsimileTelephoneNumber`
SAML 2.0	`urn:oid:2.5.4.23`
Single-valued	no
Source	RFC 4519

The person's facsimile (fax) telephone number *at his/her organisation*. These values should follow the format of telephone numbers as defined by the ITU-T E.123[28] standard.

5.6.4 homePhone

OID	`0.9.2342.19200300.100.1.20`
Shibboleth 1.x	`urn:mace:dir:attribute-def:homePhone`
SAML 2.0	`urn:oid:0.9.2342.19200300.100.1.20`
Single-valued	no
Source	RFC 4524

The telephone number of the person *at his/her residence*. These values should follow the format of telephone numbers as defined by the ITU-T E.123[28] standard.

5.6.5 mobile

OID	`0.9.2342.19200300.100.1.41`
Shibboleth 1.x	`urn:mace:dir:attribute-def:mobile`
SAML 2.0	`urn:oid:0.9.2342.19200300.100.1.41`
Single-valued	no
Source	RFC 4524

The mobile telephone number of the person. These values should follow the format of telephone numbers as defined by the ITU-T E.123[28] standard.

5.6.6 postalAddress

OID	`2.5.4.16`
Shibboleth 1.x	`urn:mace:dir:attribute-def:postalAddress`
SAML 2.0	`urn:oid:2.5.4.16`
Single-valued	no
Source	RFC 4519

The address of the person *at his/her organisation*. The value may be up to 6 lines of 30 characters each; the `$` character is used as a line break character.

5.6.7 postalCode

OID	`2.5.4.17`
Shibboleth 1.x	`urn:mace:dir:attribute-def:postalCode`
SAML 2.0	`urn:oid:2.5.4.17`
Single-valued	no
Source	RFC 4519

The postal code of the address of the person concerned *at his/her organisation*.

5.6.8 homePostalAddress

OID	`0.9.2342.19200300.100.1.39`
Shibboleth 1.x	`urn:mace:dir:attribute-def:homePostalAddress`
SAML 2.0	`urn:oid:0.9.2342.19200300.100.1.39`
Single-valued	no
Source	RFC 4524

The home address of the person *at his/her home*. The value may be up to 6 lines of 30 characters each; the `$` character is used as a line break character.

5.6.9 o

OID	`2.5.4.10`
Shibboleth 1.x	`urn:mace:dir:attribute-def:o`
SAML 2.0	`urn:oid:2.5.4.10`
Single-valued	no
Source	RFC 4519

The name of the organisation(s) with which the person is associated.

Example: `University of Athens`

5.6.10 ou

OID	`2.5.4.11`
Shibboleth 1.x	`urn:mace:dir:attribute-def:ou`
SAML 2.0	`urn:oid:2.5.4.11`
Single-valued	no
Source	RFC 4519

The name of organisational unit or units with which the person is related; each organisational unit should be a unit of an organisation that is necessarily defined in attribute `o`.

Examples: `Department of Informatics`, `Network Operations Centre`

5.6.11 eduPersonOrgDN

OID	`1.3.6.1.4.1.5923.1.1.1.3`
Shibboleth 1.x	`urn:mace:dir:attribute-def:eduPersonOrgDN`
SAML 2.0	`urn:oid:1.3.6.1.4.1.5923.1.1.1.3`
Single-valued	yes
Source	eduPerson

It is the distinguished name of the organisation with which the person is related.

Example: the *student* student of the organisation *university* will receive the value `dc=university,dc=gr`.

5.6.12 schacHomeOrganization

OID	`1.3.6.1.4.1.25178.1.2.9`
Shibboleth 1.x	`urn:mace:terena.org:schac:attribute-def:schacHomeOrganization`
SAML 2.0	`urn:oid:1.3.6.1.4.1.25178.1.2.9`
Single-valued	yes
Source	SCHAC

The so called "home organisation" of the person. It takes the value of the primary domain name (see RFC 1035[29]) used by the organisation. All persons of the same organisation—and thus Identity Provider—should have the same value in this attribute.

Example: for the student above, `university.gr`

5.6.13 schacHomeOrganizationType

OID	`1.3.6.1.4.1.25178.1.2.10`
Shibboleth 1.x	`urn:mace:terena.org:schac:attribute-def:schacHomeOrganizationType`
SAML 2.0	`urn:oid:1.3.6.1.4.1.25178.1.2.10`
Single-valued	yes
Source	SCHAC

The type of the home organisation. It takes URN values of the hierarchical form:
`urn:mace:terena.org:schac:homeOrganizationType:`*`<country-code>`*` :`
`<string>`, where:

- `<country-code>`, the country code (and thus Federation) according to ISO 3166[26] or the word "int".

- <string>, the type of the organisation, as defined by a clear and predefined vocabulary by each Federation.

The vocabulary for this attribute is issued at the TERENA URN Registry: http://www.terena.org/registry/terena.org/schac/homeOrganizationType/

For this Federation (i.e. for the <country-code> gr), no values are defined at present. Identity Providers may, however, use the values of the int or eu hierarchies.

5.6.14 l

OID	2.5.4.7
Shibboleth 1.x	urn:mace:dir:attribute-def:l
SAML 2.0	urn:oid:2.5.4.7
Single-valued	no
Source	RFC 4519

The location of the person. It takes free text values defined by the home organisation, such as city name, country or geographic area. Each name must be a separate attribute value.

Example: Athens

5.6.15 schacCountryOfResidence

OID	1.3.6.1.4.1.25178.1.2.11
Shibboleth 1.x	urn:mace:terena.org:schac:attribute-def:schacCountryOfResidence
SAML 2.0	urn:oid:1.3.6.1.4.1.25178.1.2.11
Single-valued	no
Source	SCHAC

The country or countries in which the person resides. The countries are expressed by their two-digit code in accordance with ISO 3166[26] standard. Caution is required for the code distinction of the Greek language (el) and Greece (gr).

Example: gr

5.6.16 schacUserPresenceID

OID	`1.3.6.1.4.1.25178.1.2.12`
Shibboleth 1.x	`urn:mace:terena.org:schac:attribute-def:schacUserPresenceID`
SAML 2.0	`urn:oid:1.3.6.1.4.1.25178.1.2.12`
Single-valued	no
Source	SCHAC

It consists of URI values (see RFC 3986[30]) that describe points of network presence of the user, such as XMPP, SIP, H.323, etc. protocol addresses.

Examples: `xmpp: pepe@im.univx.es`, `sip: pepe@myweb.com`

5.7 Person—organisation relationship

5.7.1 employeeNumber

OID	`2.16.840.1.113730.3.1.3`
Shibboleth 1.x	`urn:mace:dir:attribute-def:employeeNumber`
SAML 2.0	`urn:oid:2.16.840.1.113730.3.1.3`
Single-valued	yes
Source	RFC 2798

The numeric or alphanumeric employee number of the person within by his/her home organisation. These values must be unique within the organisation but not necessarily unique across the federation.

5.7.2 title

OID	`2.5.4.12`
Shibboleth 1.x	`urn:mace:dir:attribute-def:title`
SAML 2.0	`urn:oid:2.5.4.12`
Single-valued	no
Source	RFC 4519

The position or positions of the person in his/her *home organisation*. It takes free-text values as defined by the home organisation and are not necessarily unambiguous within the federation.

Example: `professor`, `programmer`

5.7.3 schacPersonalPosition

OID	`1.3.6.1.4.1.25178.1.2.13`
Shibboleth 1.x	`urn:mace:terena.org:schac:attribute-def:schacPersonalPosition`
SAML 2.0	`urn:oid:1.3.6.1.4.1.25178.1.2.13`
Single-valued	no
Source	SCHAC

The position or positions of the person in his/her *home organisation*. It takes values of URN format that are globally unique, while the organisations can create new at will, taking advantage of their hierarchical form. These values are of the form:

`urn:mace:terena.org:schac:personalPosition:`*`<country-code>`*`:`*`<domain>`*`:`*`<iNSS>`*, where:

- `<country-code>`, the country code (and thus federation) according to ISO 3166[26] or the word "int".
- `<domain>`, the primary domain name (see RFC 1035[29]) of the home organisation).
- `<iNSS>`, a *Namespace Specific String*, case insensitive, in the form specified in RFC 2141[31].

The vocabulary for this attribute is issued at the TERENA URN Registry:

`http://www.terena.org/registry/terena.org/schac/personalPosition/`

Any organisation of this federation may create values for the attribute if **it has requested and received** its own hierarchy by the Coordinator, i.e. the prefix with `gr` as the `<country-code>` and `<domain>` for the primary domain name of the organisation.

Example:
`urn:mace:terena.org:schac:personalPosition:pl:umk.pl:programmer`

5.7.4 eduPersonOrgUnitDN

OID	`1.3.6.1.4.1.5923.1.1.1.4`
Shibboleth 1.x	`urn:mace:dir:attribute-def:eduPersonOrgUnitDN`
SAML 2.0	`urn:oid:1.3.6.1.4.1.5923.1.1.1.4`
Single-valued	no
Source	eduPerson

Contains the distinguished names of the organisational units in which the person belongs to. Each person can belong to more than one organisational unit.

Example: the student *student* is studying in the department *department* of the organisation *university* and is related with the laboratories *lab1* and *lab2* of the department (e.g. participating in research activities). The attribute, then, will take the values:

1. `ou=department,dc=university,dc=gr`
2. `ou=lab1,ou=department,dc=university,dc=gr`
3. `ou=lab2,ou=department,dc=university,dc=gr`

5.7.5 eduPersonPrimaryOrgUnitDN

OID	`1.3.6.1.4.1.5923.1.1.1.8`
Shibboleth 1.x	`urn:mace:dir:attribute-def:eduPersonPrimaryOrgUnitDN`
SAML 2.0	`urn:oid:1.3.6.1.4.1.5923.1.1.1.8`
Single-valued	yes
Source	eduPerson

Contains the distinguished name of the primary organisational unit in which the person belongs to.

Example: for the student in the previous example, the attribute receive the value `ou=department,dc=university,dc=gr`.

5.7.6 eduPersonAffiliation

OID	`1.3.6.1.4.1.5923.1.1.1.1`
Shibboleth 1.x	`urn:mace:dir:attribute-def:eduPersonAffiliation`
SAML 2.0	`urn:oid:1.3.6.1.4.1.5923.1.1.1.1`
Single-valued	no
Source	eduPerson

Contains the person's affiliation to the organisation. The only permitted values are:

- faculty
- student
- staff
- alum
- member
- affiliate
- employee

5.7.7 eduPersonPrimaryAffiliation

OID	`1.3.6.1.4.1.5923.1.1.1.5`
Shibboleth 1.x	`urn:mace:dir:attribute-def:eduPersonPrimaryAffiliation`
SAML 2.0	`urn:oid:1.3.6.1.4.1.5923.1.1.1.5`
Single-valued	yes
Source	eduPerson

Contains the person's primary affiliation to the organisation. If there is a value in this attribute, it should also be stored as one of the values of the `eduPersonAffiliation` attribute.

5.7.8 eduPersonScopedAffiliation

OID	`1.3.6.1.4.1.5923.1.1.1.9`
Shibboleth 1.x	`urn:mace:dir:attribute-def:eduPersonScopedAffiliation`
SAML 2.0	`urn:oid:1.3.6.1.4.1.5923.1.1.1.9`
Single-valued	yes
Source	eduPerson

Contains the person's affiliation to the organisation, within the particular security domain. It is composed of two parts: (i) the person's affiliation, (ii) the domain or subdomain of the organisation; the value is of the form `affiliation@domain`. The allowed values for the *affiliation* part are the same as for the `eduPersonAffiliation` attribute.

Example: for a student studying in the department *department* of the *university* university, the attribute can hold the value `student@department.university.gr`. If the same student also collaborates with the *lab1* laboratory of the department *department*, the attribute could also hold a value of `student@lab1.department.university.gr`.

5.7.9 grEduPersonUndergraduateBranch

OID	`1.3.6.1.4.1.16515.2.3.2.1`
Shibboleth 1.x	`urn:mace:grnet.gr:grEduPerson:attribute-def:grEduPersonUndergraduateBranch`
SAML 2.0	`urn:oid:1.3.6.1.4.1.16515.2.3.2.1`
Single-valued	yes
Source	grEduPerson

The school or the department of a student. Defined only if the `eduPersonAffiliation` attribute holds the `student` as one of its values.

The value that this attribute holds are **strictly** the values defined by the federation which typically map to the codes assigned to university departments by the Greek Ministry of Education.

The set of possible values are listed at the website:
`http://aai.grnet.gr/registry/grEduPerson/undergraduateBranch/`

Example: `243` for the "National Kapodistrian University of Athens, Department of Mathematics "

5.8 Linkage identifiers

5.8.1 schacPersonalUniqueCode

OID	`1.3.6.1.4.1.25178.1.2.14`
Shibboleth 1.x	`urn:mace:terena.org:schac:attribute-def:schacPersonalUniqueCode`
SAML 2.0	`urn:oid:1.3.6.1.4.1.25178.1.2.14`
Single-valued	no
Source	SCHAC

Specifies a "unique code" for the person. Its value does not necessarily correspond to any identifier outside the organisation, although the values should be unique both within the organisation and at the federation level.

The values should also be human-readable and in part recognisable by administration services of the organisation.

For example, the attribute can hold values such as the student or employee number.

It takes URN values of the hierarchical form:
`urn:mace:terena.org:schac:personalUniqueCode:`
`<country-code>``:`*`<iNSS>`*, where:

- `<country-code>`, the country code (and thus federation) according to ISO 3166[26] or the word "int".
- `<iNSS>`, a *Namespace Specific String*, case insensitive, in the form specified in RFC 2141[31].

The vocabulary for this attribute is issued at the TERENA URN Registry:
`http://www.terena.org/registry/terena.org/schac/personalUniqueCode/`

- `<country-code>`, the country code (and thus federation) according to ISO 3166[26] or the word “int”.

Especially for Greek student numbers, the following hierarchy is defined: `urn:mace:terena.org:schac:personalUniqueCode:gr:`*`<domain>`*`:`*`<iNSS>`*, where:

- `<domain>`, the primary domain name (see RFC 1035[29]) of the home organisation).
- `<iNSS>`, a *Namespace Specific String*, case insensitive, in the form specified in RFC 2141[31].

The `<iNSS>` should describe the person within the organisation in a unique way; in case of a unique institution-wide student number, it should be used as-is. Should, however, a separate student number per school or department is employed, the use of the form *<branch>*:*<id>*, where `<branch>` the code of the school or department and `<id>` the student number within the department, is recommended.

Examples:
`urn:mace:terena.org:schac:personalUniqueCode:gr:uoa.gr:654:05123`,
`urn:mace:terena.org:schac:personalUniqueCode:gr:auth.gr:12345678`

5.8.2 schacPersonalUniqueID

OID	`1.3.6.1.4.1.25178.1.2.15`
Shibboleth 1.x	`urn:mace:terena.org:schac:attribute-def:schacPersonalUniqueID`
SAML 2.0	`urn:oid:1.3.6.1.4.1.25178.1.2.15`
Single-valued	no
Source	SCHAC

Specifies a “legal unique identifier” for the person, e.g. national identity card number, social security number etc.

It takes URN values of the hierarchical form:
`urn:mace:terena.org:schac:personalUniqueID:`*`<country-code>`*`:`*`<idType>`*`:`*`<idValue>`*, where:

- <country-code>, the country code (and thus Federation) according to ISO 3166[26] or the word "int".
- <idType>, identifier type, defined per country.
- <idValue>, identifier

The vocabulary for this attribute is issued at the TERENA URN Registry:
http://www.terena.org/registry/terena.org/schac/personalUniqueID/

For <country-code> gr, there are no identifier types (<idType>) defined at present.

Example:
urn:mace:terena.org:schac:personalUniquelD:se:NIN:12345678

5.9 Authorisation & entitlements

5.9.1 eduPersonEntitlement

OID	1.3.6.1.4.1.5923.1.1.1.7
Shibboleth 1.x	urn:mace:dir:attribute-def:eduPersonEntitlement
SAML 2.0	urn:oid:1.3.6.1.4.1.5923.1.1.1.7
Single-valued	no
Source	eduPerson

It contains a URI (URL or URN) that describes access rights to specific resources (services) of the federation; it is thus used for authorisation. This attribute is used to describe groups of persons that are not otherwise specified in organisations' directories, but that should have access to specific resources.

The values are defined by Service Providers and can be service-specific and not federation-wide. It is advised to Service Providers to define new values with care, since work is needed on the Identity Providers for supporting each additional value.

It is recommended for the Service Providers to communicate new values to the Coordinator. The Coordinator maintains a page at the federation's website with such values and their use at:
http://aai.grnet.gr/registry/eduPersonEntitlement/

Example: access to academic libraries is given based on the existence of the value `urn:mace:dir:entitlement:common-lib-terms`.

5.9.2 schacUserStatus

OID	`1.3.6.1.4.1.25178.1.2.19`
Shibboleth 1.x	`urn:mace:terena.org:schac:attribute-def:schacUserStatus`
SAML 2.0	`urn:oid:1.3.6.1.4.1.25178.1.2.19`
Single-valued	no
Source	SCHAC

The condition of a person as a user of a service (active, in expiration, etc.). It takes URN values of the hierarchical form:
`urn:mace:terena.org:schac:userStatus:`*`<country-code>`*`:`*`<domain>`*`:`*`<iNSS>`*, where:

- `<country-code>`, the country code (and thus federation) according to ISO 3166[26] or the word "int".
- `<domain>`, the primary domain name (see RFC 1035[29]) of the home organisation).
- `<iNSS>`, a *Namespace Specific String*, case insensitive, in the form specified in RFC 2141[31].

The vocabulary for this attribute is issued at the TERENA URN Registry:
`http://www.terena.org/registry/terena.org/schac/userStatus/`

Any organisation of this federation may create values for the attribute **if it has requested and received** its own hierarchy by the Coordinator, i.e. a prefix with `gr` as `<country-code>` and `<domain>` as its name space.

Example:
`urn:mace:terena.org:schac:userStatus:si:ujl.si:webmail:active`

A History

- Version 1.1.0, February 2012 (*Faidon Liambotis*)
  - Simplify joining conditions
  - First version in the English language
- Version 1.0.0, June 2010 (*Faidon Liambotis*)
  Based on previous recommendation texts[2] and policy drafts of Angelos Varvitsiotis and George Thanos, written within the GRNET VNOC project.

References

[1] Υποδομή Ταυτοποίησης και Εξουσιοδότησης. Εθνικό Δίκτυο Έρευνας και Τεχνολογίας. [Online]. Available: http://aai.grnet.gr/

[2] Α. Βαρβιτσιώτης και Γ. Θάνος, "Κείμενο συστάσεων προς διαχειριστές υπηρεσιών καταλόγου, Idp και sp σχετικά με τις διαδικασίες που πρέπει να τηρούνται όταν παρέχονται υπηρεσίες με χρήση του shibboleth," Εθνικό Δίκτυο Έρευνας και Τεχνολογίας, Jun. 2007.

[3] "Rules of Membership," UK Access Management Federation for Education and Research, Nov. 2007. [Online]. Available: http://www.ukfederation.org.uk/library/uploads/Documents/rules-of-membership.pdf

[4] I. A. Young, "Technical Recommendations for Participants," UK Access Management Federation for Education and Research, Nov. 2008. [Online]. Available: http://www.ukfederation.org.uk/library/uploads/Documents/recommendations-for-use-of-personal-data.pdf

[5] N. B. Zanon, C. Graf, D. Isch, and A. Redard, "AAI Policy," 1.12, SWITCH, Jul. 2004. [Online]. Available: http://www.switch.ch/aai/docs/AAI_Policy.pdf

[6] "AAI Attribute Specification," 1.2, SWITCH, Sep. 2007. [Online]. Available: http://www.switch.ch/aai/docs/AAI_Attr_Specs.pdf

[7] "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS Standard, OASIS, Mar. 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf

[8] K. Zeilenga, "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," RFC 4510 (Proposed Standard), Internet Engineering Task Force, Jun. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4510.txt

[9] "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML)," OASIS Standard, OASIS, Nov. 2002. [Online]. Available: http://www.oasis-open.org/committees/download.php/2290/oasis-sstc-saml-1.0.zip

[10] "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V1.1," OASIS Standard, OASIS, Sep. 2003. [Online]. Available: http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf

[11] "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0," OASIS Standard, OASIS, Mar. 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[12] "SAML V2.0 X.500/LDAP Attribute Profile," Commitee Draft 01, OASIS, Dec. 2006. [Online]. Available: http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-attribute-x500-cd-01.pdf

[13] M. Mealling, "A URN Namespace of Object Identifiers," RFC 3061 (Informational), Internet Engineering Task Force, Feb. 2001. [Online]. Available: http://www.ietf.org/rfc/rfc3061.txt

[14] A. Sciberras, "Lightweight Directory Access Protocol (LDAP): Schema for User Applications," RFC 4519 (Proposed Standard), Internet Engineering Task Force, Jun. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4519.txt

[15] M. Smith, "Definition of the inetOrgPerson LDAP Object Class," RFC 2798 (Informational), Internet Engineering Task Force, Apr. 2000, updated by RFCs 3698, 4519, 4524. [Online]. Available: http://www.ietf.org/rfc/rfc2798.txt

[16] K. Zeilenga, "COSINE LDAP/X.500 Schema," RFC 4524 (Proposed Standard), Internet Engineering Task Force, Jun. 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4524.txt

[17] "eduPerson & eduOrg Object Classes," Internet2, Jun. 2008. [Online]. Available: http://middleware.internet2.edu/eduperson/

[18] "SCHAC, SCHema for ACademia," TERENA. [Online]. Available: http://www.terena.org/activities/tf-emc2/schac.html

[19] "grEduPerson," Εθνικό Δίκτυο Έρευνας και Τεχνολογίας, 2010. [Online]. Available: http://aai.grnet.gr/schemas/grEduPerson/

[20] "funetEduPerson," Haka federation. [Online]. Available: http://www.csc.fi/hallinto/haka/tekniikka/funeteduperson-skeema/fep_2.1.pdf

[21] ISO, *ISO 639-1:2002 Codes for the representation of names of languages — Part 1: Alpha-2 code*. Geneva, Switzerland: International Organization for Standardization, 2002. [Online]. Available: http://www.iso.ch/cate/d22109.html

[22] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, "Hypertext Transfer Protocol – HTTP/1.1," RFC 2616 (Draft Standard), Internet Engineering Task Force, Jun. 1999, updated by RFCs 2817, 5785. [Online]. Available: http://www.ietf.org/rfc/rfc2616.txt

[23] A. Phillips and M. Davis, "Tags for Identifying Languages," RFC 5646 (Best Current Practice), Internet Engineering Task Force, Sep. 2009. [Online]. Available: http://www.ietf.org/rfc/rfc5646.txt

[24] G. Klyne and C. Newman, "Date and Time on the Internet: Timestamps," RFC 3339 (Proposed Standard), Internet Engineering Task Force, Jul. 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3339.txt

[25] ISO, *ISO 8601:2000. Data elements and interchange formats — Information interchange — Representation of dates and times*. Geneva, Switzerland: International Organization for Standardization, 2000. [Online]. Available: http://www.iso.ch/cate/d26780.html

[26] ISO, *ISO 3166-2:1998 Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code*. Geneva, Switzerland: International Organization for Standardization, 1998. [Online]. Available: http://www.iso.ch/cate/d8349.html

[27] J. Klensin, "Simple Mail Transfer Protocol," RFC 5321 (Draft Standard), Internet Engineering Task Force, Oct. 2008. [Online]. Available: http://www.ietf.org/rfc/rfc5321.txt

[28] "Notation for national and international telephone numbers, e-mail addresses and Web addresses," Recommendation E.123, ITU-T, Feb. 2001. [Online]. Available: http://www.itu.int/rec/T-REC-E.123/en

[29] P. Mockapetris, "Domain names - implementation and specification," RFC 1035 (Standard), Internet Engineering Task Force, Nov. 1987, updated by RFCs 1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2845, 3425, 3658, 4033, 4034, 4035, 4343. [Online]. Available: http://www.ietf.org/rfc/rfc1035.txt

[30] T. Berners-Lee, R. Fielding, and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," RFC 3986 (Standard), Internet Engineering Task Force, Jan. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc3986.txt

[31] R. Moats, "URN Syntax," RFC 2141 (Proposed Standard), Internet Engineering Task Force, May 1997. [Online]. Available: http://www.ietf.org/rfc/rfc2141.txt