Technological Profile

Document	Technological Profile
Identifier (OID)	1.3.6.1.4.1.19974.12.3.1.3
Version	1.3
Last modified	05.09.2012

1. Used technology

Authentication and authorisation data are exchanged in the Federation using the SAML 2.0 (or equivalent) protocol.

1.1. SimpleSAMLphp

The central service of TAAT uses SimpleSAMLphp for data exchange and considers this when guidelines are prepared. SimpleSAMLphp is the recommended software solution for Identity and Service Providers.

SimpleSAMLphp is freeware available on the page http://simplesamlphp.org/.

1.2. Other solutions

Using other software solutions (e.g. Shibboleth) is also permitted if they are compatible with TAAT. The modification of attributes in such a case is a duty of the Identity or Service Provider who uses the different solution.

1.3. JANUS Administration Tool

The Identity or Service Provider administers their metadata in JANUS themselves and they are obliged to keep the metadata up to date.

The Identity Provider may prohibit an End User associated with the Identity Provider to use certain service(s) with the assistance of JANUS.

The Identity Provider may choose the services in the case of which a data communications confirmation form is displayed to the End Users associated with the Identity Provider.

The Service Provider may prohibit the End Users of certain Identity Provider(s) to use their service with the assistance of JANUS.

2. Connection statuses

The connections of Identity and Service Providers with TAAT divide into three statuses: test, quality assurance and production.

- Test status is open to everyone who wants to join the Federation. Connections and systems are set up (incl. updated) always in this status.
- EENet checks the general and technical readiness of the Service or Identity Provider for joining the Federation and the functioning of the connection for quality assurance purposes.
- Only contractual users of the TAAT service are in production. Making changes in the systems is not permitted.

Every status has a hub and the connections in the relevant status cannot see those who are connected to other hubs.

2.1. Procedures

The Service or Identity Provider that wants to join the Federation connects to the test hub and the status of the connection is ‘test’. Once the connection is set up and functional, the entity that wants to join defines its status in JANUS as ‘pending quality assurance’.

If the entity that wants to join meets the joining conditions determined in the Federation Policy, EENet changes the connection status to ‘quality assurance’. If the connection functions and all attributes are sent correctly, the contract is signed and the status is defined as ‘pending production’.

The moment of going to production is determined by the Identity or Service Provider themselves by changing their status in JANUS to ‘production’.

All further testing is done in the test status, whilst the production level system remains functional at the same time. A changed connection must go through all steps (except entry into contract) to get to production.

3. Attributes sent via TAAT

For each authentication, the Identity Provider issues the person’s data as values of the attributes agreed in the Federation. TAAT only accepts attributes described in clauses 3.1 and 3.2.

All attributes must comply with this document both in terms of format and semantics. Attributes are sent as a text string in UTF-8 encoding.

The NameFormat of attributes is `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

3.1. Compulsory attributes

Every Identity Provider must issue compulsory attributes. The Service Provider may presume that these attributes always exist for every End User.

- sn – surname according to identity document;
- cn – full name according to identity document;
- eduPersonPrincipalName – unique username through history or other identifier in the home institution in the format of identifier@domain. TAAT generates the identifier eduPersonTargetedID on the basis of the setting;
- mail – e-mail address, may be more than one;
- displayName – the preferred name of the user. First name must be issued if unknown;
- eduPersonAffiliation – role in home institution, may be more than one. Permitted roles are described in clause 3.4.

3.2. Optional attributes

Optional attributes are the attributes that the Identity Provider may send out. The Service Provider must keep in mind that there may be no optional attributes.

- eduPersonScopedAffiliation – role in group, may be more than one. Permitted presentation formats are described in clause 3.5;
- preferredLanguage – may be more than one. Language codes consist of two letters as set out in the ISO 3166 standard;

- schacPersonUniqueID – Estonian personal identification code. The attribute is not sent if the person does not have a personal identification code. The personal identification code is sent as an eleven-digit number according to the standard *Personal Identification Code. EV ST 585-90*, and the identifier of the state and ID type will be added in front of the code and separated with colons. For Estonia, the identifier is 'ee:EID:'.

3.3. TAAT attributes

Attributes that are prepared by TAAT and sent to the Service Provider regarding every query.

- schacHomeOrganization – home institution's ID, in the format of domain name;
- eduPersonTargetedID – an ID that cannot be personalised and is used across the Federation, different for each End User and service pair. The attribute is always presented as a string of 75 characters.

3.4. Roles

Permitted roles that can be sent with the duPersonAffiliation or eduPersonScopedAffiliation attribute:

- **student** – undergraduate or postgraduate student
- **faculty** – academic or research staff
- **staff** – technical or administrative staff
- **affiliate** – person associated with the institution (also temporarily) who has no specific rights
- **library-walk-in** – person who uses a computer in the institution's network
- **alum** – alumnus/alumna (graduate)

In addition to the above, the Identity Provider must also add the following roles if they correspond to affiliation conditions:

- **employee** – combination of the roles **staff** and **faculty** members
- **member** – combination of the roles **student, staff** and **faculty** members

3.5. Groups

The attribute eduPersonScopedAffiliation is used in the format <roll>@<grupp>.<nimeruumitähis>, where:

- the role is defined in clause 3.4.;
- the group has a single meaning in its namespace;
- the namespace identifier determines the semantics and is either specific to the Identity or Service Provider, or valid across throughout the Federation. The namespace identifier is in the format of a domain name.

The Identity Provider must prepare and publish the list of groups it uses.

Groups with TAAT namespace identifiers that are valid throughout the Federation:

- role@<studeylevel>.studylevel.taat.edu.ee, where the permitted study levels and their meaning is described in clause 3.6. Used only with the student role. Only one study level may be associated with one student place.
- role@<unit.---.unit>.ou.taat.edu.ee, where ‘unit’ is a subunit of the institutions; there may be several units if a hierarchic order is guaranteed so that each mentioned unit is the subunit of the one to its right or the biggest possible. The unit of minimal size is the identifier of the curriculum or specialty. The attribute must contain at least one unit.
  Unit identifiers must be in minimal format and always the same in institutions.

3.6. Study levels

Use of the following study level indicators is permitted:

- **dok** – doctoral studies
- **mag** – master’s studies
- **bac** – bachelor’s studies
- **int** – study based on the integrated curricula of bachelor’s and master’s studies, including medical training, veterinary training, pharmacist training, dentistry training, architectural studies, civil engineering studies and class teacher training
- **rak** – acquisition of professional higher education
- **kursus** – participation in courses or in-service training not for the purpose of acquiring a specific degree or level, and which is not related to a student place
- **gymn** – acquisition of general secondary education
- **kutse** – acquisition of vocational secondary education
- **keskeri** – acquisition of secondary specialised education

The definitions of study levels comply with the Education Act of the Republic of Estonia.

4. Metadata

TAAT is the source of remote metadata for all Identity and Service Providers. The Identity and Service Provider must add the metadata of all three TAAT hubs to its list of remote metadata.

Every Identity and Service Provider must register its hosted metadata in JANUS.

Metadata are presented in XML or SimpleSAMLphp format, and the following attributes must be defined:

- entityID – unique URI of the service or authentication system. Used to identify the specific Identity or Service Provider in all systems, highly sensitive to changes
- certData – Base64 encoded certificate
- OrganizationName – unique name of the Service or Identity Provider. Must be presented in Estonian (et) and English (en), but may also contain more languages.

- OrganizationDisplayName – unique name of the Service or Identity Provider that is displayed to the End User. Must be presented in Estonian (et) and English (en), but may also contain more languages.
- OrganizationURL – information page of the Service or Identity Provider.
  Please note: The domain part must be unique for each Identity Provider (schacHomeOrganization is generated from this).
- name – name displayed in JANUS, in domain format.
- SingleSignOnService – URL with login location (SAML endpoint). Not used for Service Providers.
- SingleLogoutService – URL with user’s logout location (SAML endpoint).