On integration of academic attributes in the eIDAS infrastructure to support cross-border services

Diana Berbecaru, Antonio Lioy
Politecnico di Torino, Dip. di Automatica e Informatica
Corso Duca degli Abruzzi 24, 10129, Torino (ITALY)

***Abstract*—The EU Regulation 910/2014 on electronic identification and trusted services for electronic transactions in the internal market, known also as eIDAS Regulation, will become effective on 29 September 2018. By that date, each EU Member State is required to recognize the electronic identities of other EU Member States that have notified their electronic identification (eID) schemes. From the technical point of view, intensive efforts are being spent to effectively connect the various national eID schemes in a unified interoperability architecture, the eIDAS infrastructure.**

This paper describes our proposal to integrate academic attributes into the eIDAS infrastructure, as part of the "eID for University" project (in short eID4U). This project aims to support the practical implementation of the eIDAS Regulation in a selected set of academic services at the universities participating in the project. The objective is to enhance the eIDAS infrastructure with support for academic attributes and to design and implement a set of eIDAS-enabled academic e-services, like the Registration in some study programmes (e.g. Erasmus student exchange programme) or the Login facility (with national eIDs) on a foreign university's web portal.

***Index Terms*—electronic identity, eIDAS infrastructure, attribute management, academic services**

I. Introduction

The federated identity model (FIM) is the most widely used nowadays to authenticate persons when accessing on-line services. In this model, the identity data about a person and his authentication credentials are managed by an entity named Identity Provider (IdP), which exchanges identity attributes with those entities that consume them to provide access to services, named Service Provider (SP), provided the SP and the IdP have established a trust relationship. Additionally, often other entities are defined to manage other information associated to the users and they are named Attribute Providers (APs). Many countries in Europe have already deployed or are updating their national eID systems to allow citizens to get access to public services by exploiting the FIM model and the eIDs issued by specialized authorities, like governmental bodies or agencies. For example, Italy is currently deploying SPID, the Italian digital identity system, which has been pre-notified on December 2017 [1] to the European Commission (EC), putting thus the grounds to allow Italian citizens and businesses to access with their SPID credentials all the digital services of Public Administrations (and possibly also private companies) of EU Member States.

Historically speaking, since the late 90's, many EU governments developed and deployed eID systems, such as the Belgian BelPIC, the Estonian ID KAART Card, the Finnish FinneiD, or the "neuer Personalausweis" in Germany. Some countries followed with mass card roll-outs such as Portugal and Spain, while other countries provided eID via authentication portals by using usernames and passwords such as the UK Government Gateway or DigiD in The Netherlands. Nowadays, we encounter various solutions for authenticating citizens in public services: some countries continue to use cards on wide scale, other countries exploit both cards and username and passwords, while mobile solutions (exploiting personal mobile smart devices) have started to be increasingly used in several countries, like in Austria or Estonia.

The increasing mobility of the citizens and consequently the increase of cross-border public administration procedures generated the necessity to achieve cross-border interoperability of national eID systems within EU. One of the latest step performed by the EC to foster the recognition and the exploitation of eIDs in cross-border services was the release (on July 23, 2014) of the eIDAS Regulation [2], which will become effective in 2018. Moreover, the EC has also financed the eID large scale pilot projects STORK [3] and the follower STORK-2.0 [4], which connected different national eID solutions for identification and authentication in an unified eID interoperability framework.

The success and the outcome of the STORK projects was used as baseline in the definition of the eIDAS Regulation and its technical specification [5]. Nowadays, many European countries have already set up eIDAS nodes typically running the eIDAS sample implementation [6] and most of them have performed conformance testing with the EC [7].

The eIDAS infrastructure is composed of eIDAS nodes (one per country), which need to be connected to the national IdPs/APs, in order to be able to authenticate persons and to provide attributes for them. Additionally, the eIDAS nodes have to be connected to the national SPs to allow foreign citizens to authenticate in their home country through the eIDAS infrastructure when accessing SP' services. The eIDAS nodes are connected to the IdPs (which are part of a notified eID scheme in that country) by using Member State-specific solutions, while the connection of APs and SPs to the national eIDAS nodes and the development of new eIDAS services are still in their infancy. This is due in part to the fact that

978-1-5386-4444-7/18/$31.00 ©2018 IEEE

sector-specific attributes (in domains like academia, business, eHealth, e-Justice, e-Procurement) are not yet supported and thus they cannot be transferred through the eIDAS nodes. Moreover the connection of the eIDAS nodes to the national APs is still subject to further work, but several research projects have started to work on these aspects. For example, the eID4U project [8] is aimed mainly to enable the definition and transport of (new) academic attributes through the eIDAS nodes in order to implement eIDAS-enabled academic services exploiting such attributes.

In this paper, we describe our proposal to enhance the eIDAS infrastructure with support for the academic attributes in the eID4U project. In practice, we will detail: a) the proposed eIDAS-enabled services, that is the use cases exploiting the attributes retrieved through the eIDAS framework, and b) the retrieval of the academic attributes from the APs and their transfer through the eIDAS node, with the help of a so-called *AP Connector* module.

The paper is organized as follows: Section II gives an overview of the related work, Section III describes the proposed eIDAS-enabled services, Section IV describes our approach to enhance the eIDAS infrastructure with support for academic attributes, Section V details some solutions we have designed and implemented so far to provide and transport additional attributes through the eIDAS infrastructure, in addition to the eIDAS minimum data set for a natural person specified in [5]. Finally, Section VI concludes the paper and indicates future work.

II. Related Works

Several research projects have dealt with or are dealing with the definition of reliable infrastructures to transfer academic data between institutions in Europe. The EMREX project [9] for example allows mobile students to transfer their achievement records from abroad. EMREX is a decentralized system, which is composed of National Contact Points (NCPs) which the students contact to fetch their academic results [10]. To allow students to retrieve their results (e.g. achievement records) from another high education institution, either in the same country or from abroad, the project developed a dedicated application, named EMREX client. Moreover, EMREX defines also an XML-based format, named ELMO, for the academic results obtained by a student, which is digitally signed with the private key of the NCP that issued it. EMREX does not define any authentication method but delegates this task to the university. In brief, when the student visits an university abroad he will first register at the foreign university and he will obtain authentication credentials valid at the university abroad. When he wants to transfer the academic records he will be authenticated by means of that credentials. With respect to eIDAS, which aims to allow students to use their nationally issued credentials to perform academic services, EMREX has limitations in terms of authentication because however the students will have to obtain new credentials at the visiting university, which might become invalid after some period of time or might have an level of assurance considered “low” (as it’s typically the case for usernames and passwords).

The European Student Card (ESC) project [11] defines a centralized platform to allow students to exchange academic information between universities that adhered to the project. Basically, the students are provided with smart-cards that can be used for authenticating them, which contains a unique student European ID [12]. Even though the idea to have a unique student European ID is good as it could solve many problems to obtain data for a specific student uniquely identified, the main limitation in this solution is that it allows students to benefit from new services based upon the information on the card (reductions at the libraries or at university restaurant) only at the universities that adhered (and thus recognize) the card.

III. Proposed eIDAS-enabled services

In the eID4U project, we consider the design, implementation, and test of three eIDAS-enabled academic e-services, based on existing services and exploiting the (new) attributes defined in the project: eRegistration, eLogin, and eAccess.

A. eRegistration

The registration service is one of the most widely used at universities. The registration service that may benefit from the integration with the eIDAS infrastructure is the eRegistration for (incoming) Erasmus students.

At present, incoming Erasmus students perform registration procedures directly at the visiting university site, where they provide personal data, which has to be inserted manually and has to be verified by the operators. In the proposed “eIDAS-enabled eRegistration for Erasmus students” service, some data (attributes) regarding the academic career of the student that are currently inserted manually by the student will be automatically retrieved in a trustworthy way through the eIDAS infrastructure. Note that in such service, the eIDAS attributes for natural persons (e.g. name, surname, date of birth) will be complemented with additional (academic) attributes required by such service, such as the current university of the student, the course name the student is enrolled at his home university and the field and level of study. The added value of this proposed service consists in reducing the burden at the Erasmus offices that would have the possibility to obtain trustworthy data required for registration or preregistration of incoming students through the eIDAS network, avoiding thus the processing of paper documents and the manual insertion/verification of such data.

Universities also have to manage an increasing number of foreign students/academic staff that attend the university for a short or long time. Such persons typically have to register to get access to the university’s portal containing course materials, lab exercises, news, or reserved areas where they can upload and maintain their homeworks. During the registration at a course, some pre-requisities have to be typically checked, for example whether the person is a student or a teacher, whether he attended in the past other mandatory courses, and so on. So, also in this case the student service offices have to manually check some pre-requisites. Thus, another service that could exploit eIDAS is the so-called "eIDAS-enabled eRegistration for courses" that would allow foreign students/academic staff (e.g. professors, researchers) with valid eIDAS credentials to register at course/university's portal by exploiting the eIDAS infrastructure. In this service, additional attributes besides the ones that are part of the eIDAS minimum data set are typically required, e.g. information of previous student's academic career might be requested to allow him to register to a particular course.

B. eLogin

Universities have already in place a Single Sign-On system that allows their users to authenticate once and then transparently get access to several services. However, the Login with university credentials is typically offered after the student has registered at that university. The proposed eIDAS-enabled eLogin would allow foreign students with valid eIDAS credentials to get access, through single-sign-on mechanisms, to different academic services offered by the universities involved, e.g. to distance learning courses which are quite appealing for foreign students. Moreover, some existing services could be enhanced by incorporating the strong authentication that can be performed through eIDAS infrastructure. For example, there are some low-sensitivity services that can be accessed through a simple username and password. In this case, one problem often encountered is that the users forget their university credentials (username and/or password) and they have to contact a Help Desk for recovery.

In the eID4U project, we proposed "eIDAS-enabled eLogin", that could be used in various cases. For example, in case of password loss, the person will be asked to perform strong authentication through the eIDAS infrastructure (with his/her national eID) and afterwards will be able to automatically recover her credentials, reducing (or even avoiding) the contact with the university's helpdesk. In case the user feels comfortable with its eID, this system could completely replace the standard login procedure in use at the university.

C. eAccess

WiFi access requires reliable authentication mechanism. Nowadays, foreign students/academic staff typically authenticate to obtain WLAN access with their own university credentials through the eduROAM network, when visiting other universities abroad. However, one problem that it is still uncovered is the possibility to provide WLAN access to other persons that are not part of the academic system (such as industrial companies delegations, public administration persons) that visit universities for various events (e.g. project meetings, open conferences, seminars). Currently, the most adopted solution is to set up temporarily a valid credential (username/password) which is shared between the persons attending the event or assigned to each individual. This is of course a management burden as well a security risk. In the eID4U project, we proposed eIDAS-enabled eAccess service, which will allow WLAN access based on eIDAS credentials.

IV. Proposed support for academic attributes in eIDAS infrastructure

First of all, a short description of the eIDAS infrastructure is given further below.

Arhitecture. The eIDAS interoperability framework comprises two different authentication models. In the "*proxy model*", each country adhering to this model has to run a single gateway called "*eIDAS node*". This component is actually logically called "eIDAS-Proxy-Service" (in short, eIDAS Proxy) when we refer to the eIDAS node in which the citizen will be authenticated and is called "eIDAS-Connector" (in short, Connector) when we refer to the eIDAS node in the SP country. In the "*middleware model*" (adopted mainly by Germany) the SPs and the Connector integrate the foreign eIDs by using a country specific middleware (MW). Cross-border authentication is delegated from an SP to its national Connector, which acts as a gateway and subsequently forwards the authentication request to the responsible foreign country's eIDAS Proxy (or to the MW). The authentication request is handled by the eIDAS Proxy according to Member-State (MS) specific approach. Most countries follow the traditional approach in which a new authentication request is constructed by the eIDAS Proxy and is sent (through the user's browser) to the national IdP where the citizen is asked to authenticate with a national eID. Upon successful authentication, the authentication response containing also the attributes that have been requested are returned through the eIDAS infrastructure back to the requesting SP.

Each eIDAS node has two interfaces implementing two types of protocols: the one used for communicating with the national SPs and IdPs is MS specific (sometimes it is referred as the *Specific* part of the eIDAS node), whereas the one communicating with the other proxies exploits the eIDAS communication protocol [13] (sometimes it is referred as the *Generic* part of the eIDAS node). Such protocol is based on SAML 2.0 WebSSO Profile [14] to transfer identification and authentication data cross border between the eIDAS nodes.

Attributes. Currently, the eIDAS infrastructure supports only a limited number of person attributes to be exchanged through the eIDAS nodes, e.g. family name, first name, date of birth, unique identifier, current address and gender of a person. These attributes are part of a so-called eIDAS minimum data set for natural persons. eIDAS defines also attributes for legal persons (which are not covered in this paper), e.g. the legal name, legal address, VAT registration number, the tax registration number or the legal entity identifier. The attributes are either mandatory or optional, the mandatory ones have to be valued and returned to the requesting SP while the optional ones would not cause an error in case they are not valued by the IDP/AP.

A. Defining academic attributes and an attribute schema

To support the academic attributes, the eIDAS node needs to be updated with support for new attributes. Thus, in the first phase we have started the definition of the attributes to be used in the proposed academic services. As result of our preliminary analysis, some academic attributes that are typically required to register a foreign student as an Erasmus student are the current student's university name (and Erasmus code), and the course at which a student is currently enrolled in his university. Other additional attributes are the ones specific to the Erasmus programme, such as the contact person at the international Erasmus office (his address, fax, phone number, email) or the advisor of the student at his home university (along with his address, faculty name of the academic advisor, his phone and email address).

Thus, in eID4U, we have divided the attributes in three types or categories: the personal ones, the academic ones and the programme-specific ones. The personal attributes contain the data used for identifying the person, so in this category we can include the eIDAS minimum data set for natural person attributes plus some other additional attributes, such as attributes regarding the identification document (passport or identity card) such as the `ID Number`, `ID issued by` or `ID expiration date`.

The academic attributes are the (minimum) ones that contain data about the academic career of a student, such as the `country of study`, the `university name`, `the field/area of study` and the `level` (e.g. undergraduate, graduate, PhD).

The programme-specific attributes are the ones that concern or are required by specific study programs, such as the `period of stay` or the `proposal of learning agreement (study plan)`. In our approach, these attributes will not be transferred through eIDAS but they will be communicated through other means, for example they might even be self-declared by the student directly on the university's dedicated portal.

Next, for the defined (academic) attributes, an XML schema needs to be created (indicating the type and usage of each attribute). Moreover, the attribute XML schema needs to be further included in the eIDAS node and the eIDAS reference implementation code has to be modified both in the *Generic* part as well in the *Specific* part to support the new (simple and complex) academic attributes.

Moreover, since the academic attributes do not have a Level of Assurance (LoA) by default, we have defined a property (of the attribute) allowing an AP to mark/indicate how the AP valued that attribute. A possibility would be for example, to assign the property "primary" when the AP values the attribute based on the information it has in its internal database (so the quality of the attribute value is considered "high"). For example, the `country of study` or the `university name` will typically have the "primary" property. Alternatively, it could be assigned the property "secondary" when the AP values the attribute based on some information extracted from some official document (e.g. the passport number can be valued by an AP by reading it from a scanned copy of a document) so in this case the quality of the attribute is considered "medium". Finally, the property "self-declared" could be set when the AP values an attribute based on self-declarations (so, in this case the quality of the attribute value is considered "low").

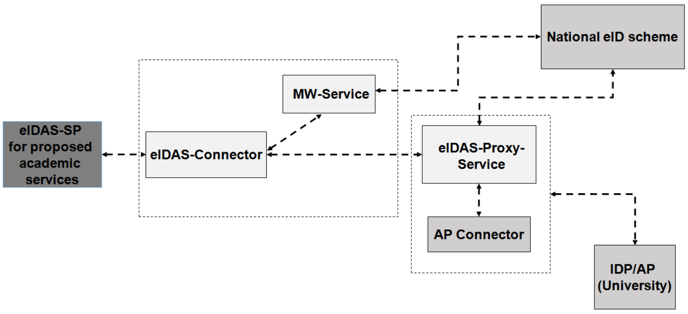

Fig. 1. Providing attributes through the AP Connector module.

B. Connecting the eIDAS node to the academic APs

First, the current eIDAS nodes do not allow to select either the countries or the APs from where the attributes for a citizen may be retrieved. The possibility to select the AP from where to retrieve the attributes is relevant especially for those countries in which the national eID infrastructure does not provide the (requested) academic attributes together with the eIDAS attributes that are part of the minimum data set for natural persons. So, if an eIDAS node requests attributes containing both the minimum data set and academic attributes, either it manages to obtain them directly from the MS eID national infrastructure (in eIDAS format) or it has to contact an additional service/module. In the eID4U project, we proposed the AP Connector module, which is illustrated in Fig. 1. Note that the AP Connector is optional, some countries might not need it because the support for academic attributes could be added/integrated (in)to the national eID scheme and thus they would be provided directly through the eIDAS node.

In other countries, the IdPs (issuing notified eIDs and providing typically person attributes like name, surname or date of birth) are separate from AP/IdPs providing academic attributes. In particular, the entities acting as APs in eID4U are universities that typically already have in place a system for identity management, attribute transfer and processing. For example, some universities have adopted Shibboleth [15], which is a SAML based open-source framework, while others are in the process of installing or running other similar systems or systems that may be part of a national system connecting the APs in a specific domain (in our case, academic domain).

The AP Connector module acts as an adapter between the eIDAS protocol and the specific protocol(s) used for academic attribute exchange. Note that AP Connector is foreseen to be exploited by the APs that fulfill one of the following conditions: (1) their national eID scheme/infrastructure do not provide academic attributes (together with the eIDAS minimum data set attributes for natural persons); (2) they do not have a specific solution for mapping/filtering of academic attributes from specific format to eIDAS format and provision of such attributes to the eIDAS node.

The AP Connector is foreseen to have a common part (for example for AP selection, for processing the eIDAS messages exchanged with the eIDAS node) and a specific

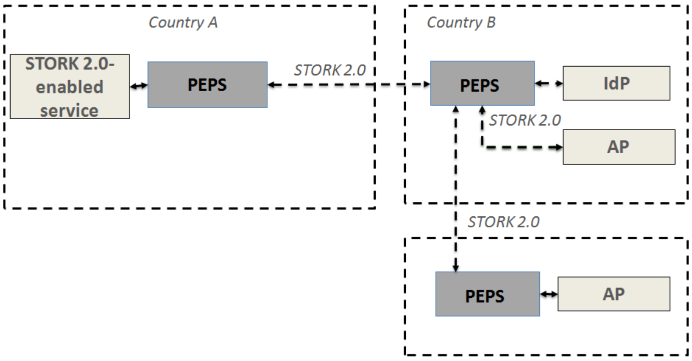

Fig. 2. Academic attribute retrieval from (demo) AP in STORK 2.0.

part, which has to be design/implemented by the Member States according to the specific solution used for attribute handling. The "AP Connector" module will be in charge with performing the following operations: (a) it allows the citizen to select from which AP the attributes will be retrieved from; (b) it maps (if necessary) the attribute requests/responses from eIDAS protocol to the protocol specific for academic attribute exchange supported by the university. (c) it filters (if necessary) the attributes that have not been requested, in accordance to the principle of data minimisation.

V. Some solutions for retrieval of additional attributes through the eIDAS infrastructure

We have proposed the AP Connector in eID4U based on the experience we have gained in two solutions we have developed to transfer additional attributes through an eID infrastructure. Each of these solutions has its pros and cons, that will be discussed in brief, none of them can be fully adopted in eID4U.

A. Retrieval of academic attributes in STORK 2.0

The first solution aimed to retrieve additional academic attributes (besides the ones used for identifying a person) was developed in the STORK 2.0 project. A person was authenticated through the STORK 2.0 system at a national IdP, and in case additional attributes (that were requested by an SP) have not been valued by the IdP, it was possible to contact an external AP from where to retrieve the attributes, as shown in Fig. 2.

In STORK 2.0, the PEPS code was extended to support new attributes that have been defined in the project for several specific domains, like academia, banking or business. Examples of defined academic attributes are the `hasDegree`, `isStudent`, `isTeacherOf`, `isAcademicStaff`, `diplomaSupplement`, or `currentStudiesSupplement`) attributes. Moreover, the PEPS (the predecessor of the eIDAS node) was also extended to allow the selection of external APs and performed also attributes collection and linking.

In this solution, we have developed a custom AP (named demo AP in STORK 2.0 project) that provided several academic attributes to the PEPS component in the STORK 2.0 infrastructure [16].

The custom AP we have developed was composed of several logical modules: the *interface* (towards the PEPS), a *SAML processing module* in charge with processing the attribute requests and responses such as checking the signature on the SAML message, an *attribute processing module* in charge with extracting the attribute from the attribute request and performing other operations on attributes, and a *database interface module* in charge with extracting the attribute values from data sources in various formats, such as from a text file or a database in Oracle or MySQL formats.

The *SAML processing module* was also called *SAML Engine* in STORK 2.0, it was based on OpenSAML and it incorporated all SAML related functionality for processing STORK messages. The custom AP was a web application developed in Java and we have used also Spring and Apache Struts frameworks for its implementation. Additionally, we have used also the Hibernate ORM (Object Relational Mapping) [17] in order to map Java classes into tables or views of a relational database, allowing us to connect the AP to various types of backend databases by creating queries in various SQL dialects.

In this solution, our main goal was the design of an application that could be used on the AP to retrieve and return attributes in STORK 2.0 format back to the PEPS node. A similar application could be developed eID4U to be used by the AP to communicate with the AP Connector. A limitation of this application in STORK 2.0 project was the necessity to re-authenticate a user at the AP before providing academic attributes for him. This resulted in several co-related problems, such as re-authentication hypothetically allowed an SP to receive two set of attributes belonging to two different citizens (e.g. two diplomas belonging to 2 different universities in different countries). Moreover, no AQAA (Attribute Quality Assurance Level) was assigned to attributes gathered from different APs.

B. Connection of eIDAS node to SPID system

In the meantime, Italy adopted the SPID system, so the eIDAS node has been connected to the IdPs in the SPID domain through a dedicated adaptation layer, named *IdP Proxy* and to the SPs in the SPID domain through an *SP Proxy* [18]. These proxies have basically the role to map or to transform the eIDAS messages (authentication requests and responses) to SPID messages that can be processed by the national IdPs and SPs that are SPID-enabled.

Currently, the SPID system provides basically a limited set of attributes, like name, surname, and date of birth of a person, together with a national identifier (i.e. "codice fiscale", the Italian fiscal code), which are obtained from the notified IdPs. Currently, the notified IdPs in SPID do not return academic attributes.

To allow the transfer of an additional attribute through the Italian eIDAS node, we have slightly modified the eIDAS node (in its configuration part). Next, we developed a specific attribute mapping application that allowed to request and transfer an additional attribute used in a health scenario, named `patient identifier`. The mapping application was

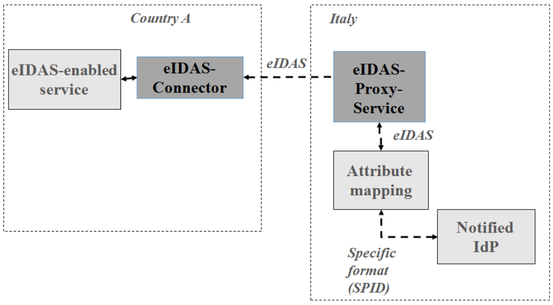

Fig. 3. Simple attribute retrieval from (Italian) SPID system to eIDAS node through attribute mapping/conversion.

in charge with receiving an eIDAS request (containing also the additional `patient identifier` attribute), then it converted the request into a new authentication request (in SPID format), which was subsequently sent to a notified IdP, as shown in Fig. 3. Moreover, the `patient identifier` attribute was also converted in `codice fiscale` attribute, which is recognized by the SPID system. After the person authenticated successfully at the notified IdP, the SPID authentication response was sent back to the mapping application, which converted it into an eIDAS response that is sent back to the SP.

The mapping application not only converts the attributes to/from eIDAS format to the SPID format, but it allows also to ask for an additional attribute, besides the ones that are part of eIDAS minimum data set for a natural person. Thus, the mapping application is a simplified format of AP Connector, but presents several limitations. First of all, it was designed to contact a notified IdP in Italy, which does not typically provide sector specific attributes, like the academic attributes. So, in the eID4U project, we will extend our attribute mapping application to collect attributes from several sources (e.g. from a notified IdP and from an academic AP) and construct a unique eIDAS response containing such attributes. Secondly, the mapping application does not recognize complex (structured) attributes. For example, the `current address` of a person can be seen as a complex attribute, which may contain several several (sub)fields, for `street`, `house number` a.s.o. The complex attributes need to be further processed so that their content should be visible to the user so that he/she can provide user consent to transfer them to the eIDAS node. This functionality will be added in the AP Connector in eID4U.

VI. Conclusions

Building an efficient and scalable eIDAS infrastructure requires at the European level the integration and harmonisation of several systems, that originally were designed, implemented and maintained by different entities, with different tools and approaches. For example, the national governments or public agencies basically handle the eIDAS node, the eID systems are managed by public or private IdPs (recognized through mechanisms specific to each country) connected to the eIDAS node, while the sector-specific attributes, like the academic ones, are provided by the universities.

With the deadline of 29 September 2018 rapidly approaching, an intensive effort is spent by all European countries to make recognition of eIDs a reality and accept them as valid in getting access to a wide range of services. In this paper, we proposed the integration of academic attributes into the eIDAS infrastructure to support some cross-border academic services. We have presented the steps we have performed so far and we have discussed some solutions allowing to transfer academic attributes through the eIDAS nodes, together with their pros and cons. The full realization of the AP Connector presented in this paper is regarded as future work.

Acknowledgment

This work was developed in the framework of eID4U project, co-funded by the European Union's Connecting Europe Facility (CEF) under the grant agreement no. INEA/CEF/ICT/A2017/1433625.

References

[1] Infocert, "The process to have an European Digital Identity has started". https://infocert.digital/the-process-to-have-a-digital-european-idenity-has-started/

[2] European Union, "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec," European Union, 2014.

[3] Secure Identity Across Borders Linked (Stork) project - Towards pan-European recognition of electronic IDs (eIDs) (2008-2011). http://www.eid-stork.eu.

[4] Secure Identity Across Borders Linked (Stork) 2.0 project (2012-2015). http://www.eid-stork2.eu

[5] eIDAS Technical Specifications v1.1, https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10, 16 May 2018.

[6] eIDAS-Node software releases, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node+-+Current+release

[7] eIDAS Conformance Testing, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Conformance+testing+-+eID

[8] eID4U project. https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2017-eu-ia-0051

[9] The EMREX Project, http://emrex.eu/

[10] EMREX implementation details, https://confluence.csc.fi/display/ EMREX/Implementation+of+EMREX

[11] European Student Card project, http://europeanstudentcard.eu

[12] European Student Card specifications, http://europeanstudentcard.eu/wp-content/uploads/2017/02/2017_03_21_European-student-card-Specifications-v1.pdf

[13] eIDAS SAML Message Format, version 1.1, https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/ eIDAS%20Message%20Format_v1.12.pdf?version=1&modificationDate=1497252919575&api=v2

[14] J.Hughes, et al., Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005. http://docs.oasis-open.org/security/saml/v2.0/samlprofiles2.0os.pdf

[15] Shibboleth, https://www.shibboleth.net/

[16] D. Berbecaru and A. Lioy, "On the design, implementation and integration of an Attribute Provider in the Pan-European eID infrastructure," ISCC-2016: IEEE Symposium on Computers and Communication, Messina (Italy), 2016, pp. 1263-1269. doi: 10.1109/ISCC.2016.7543910

[17] http://www.hibernate.org

[18] P. Smiraglia, M. De Benedictis, A. Atzeni, A. Lioy, and M. Pucciarelli, "The FICEP Infrastructure: How we deployed the Italian eIDAS node in the cloud". E-Democracy 2017: Privacy-Preserving, Secure, Intelligent E-Government Services, Athens (Greece), Communications in Computer and Information Science, vol. 792. Springer, pp. 96-210. doi: 10.1007/978-3-319-71117-1_14