Academic European E-identity Management Framework

Nuno Mendes, January 2021

Abstract

The electronic IDentification, Authentication and trust Services (eIDAS) regulamentation, also known as EU Regulation 910/2014, has drastically changed how European Member States look at the prospect of a Digital Single Market in the European Union. While the eIDAS integration with Service Provider is still in its infancy stage there have been great prospects for it's future.

The article Academic European E-identity Management Framework and the accompanying European project eID for Univeristy (eID4U) had two objectives: the first objective is to enhancing the initial specification of eIDAS to support new attributes, extending the personal attributes supported by the eIDAS Nodes and also creating a new set of attributes for academic purposes; the second is to support the practical implementation of eIDAS in real services.

This article presents three eIDAS-enabled services; eRegistration, eLogin and eAccess; developed during the project eID4U, these services have been designed, implemented and deployed at University of Lisbon. These services use the eIDAS infrastructure to authenticate and retrieve attributes of real users. They also provide solutions to typical problems encountered during the integration of eIDAS with legacy systems.

Index Terms

eIDAS, Cross-border authentication, Identity Management, electronic identification (eID)

I. Introduction

The Internet has changed the lives of billions of people around the world, the services and technologies offered by it are rapidly changing our world. Despite the lack of physical barriers there still exist digital barriers that prevent people to fully benefit from it.

Europe and the world is becoming increasingly aware of these barriers. To tackle them the European Union (EU) and the European Comission (EC) have made intensive efforts to create a Digital Single Market (DSM)[1] between the Member States (MSs). In a DSM any citizen belonging to a MS would be able to access services in any other MS. One of the most important measures taken towards this effort was the EU Regulation 910/2014 on electronic identification and trusted services for electronic transactions in the DSM, also known as the electronic IDentification, Authentication and trust Services (eIDAS) Regulation [2].

The project eID for University (eID4U) which includes this master article is a implementation and extension of the eIDAS regulamentation, which was drafted according to the conclusions of some european projects such as the Secure idenTity acrOss boRders linKed (STORK)[3] and Secure idenTity acrOss boRders linKed 2.0 (STORK 2.0) projects. The motivation for this project is aligned with the EC's intentions of creating and promoting a DSM.

The goal of Academic European E-identity Management Framework (AEEMF) corresponds to the goals of the european project eID4U, which is divided in 3 different eIDAS-enabled services with different objectives.

In general terms eID4U wants to enhance the original eIDAS regulamentation by adding new attributes (academic attributes) and also to support the practical implementation of the eIDAS Regulamentation by adding new services within it's scope, increasing it's range of services.

The eID4U project has 3 eIDAS-enabled services, these are: eRegistration, eLogin and eAccess. These new services will use the existing personal attributes and the newly implemented academic attributes[4].

II. eidas

A. eIDAS Infrastructure

The eIDAS Infrastructure is composed of proxies called eIDAS Nodes. There is a single eIDAS Node per country, except for Germany and Austria, and every MS is responsible for their own eIDAS Node [5]. Due to Germany and Austria's legislation eIDAS must support two different authentication models.

In the proxy model each eIDAS Node is composed of two modules the eIDAS Service and the eIDAS Connector. The eIDAS Connector connects to the national Service Providers (SPs), this module is the same for all eIDAS Nodes in the eIDAS Network. The eIDAS Service connects to the national infrastructure of the MS, therefore this module has to be altered due to the different specifications of the implemented Electronic Identity (eID) schemes, for example Portugal has only one Identity Provider (IdP) while Italy has several IdPs so they had to create an IdP Proxy.

The middleware model relies on a country-specific Middleware (MW) present in every eIDAS Node. Instead of using the eIDAS Connector - eIDAS Service connection Germany's citizens use the MW present in the eIDAS Connector which interacts with a citizen's eID token (smart card) providing the authentication necessary for the SP.

In order to provide cross-border authentication, eIDAS Nodes communicate via the eIDAS communication protocol [6], this protocol is based on Security Assertion Markup Language (SAML) [7].

B. eIDAS Authentication Flow

In this example an Italian Citizen wants access to a protected resource from a Portuguese Service, so this Italian user has to authenticate at an Italian IdP. For reasons of clarity the example the SP is just a web service with an eIDAS login option. Figure 1 depicts the example flow of an Authentication Request.

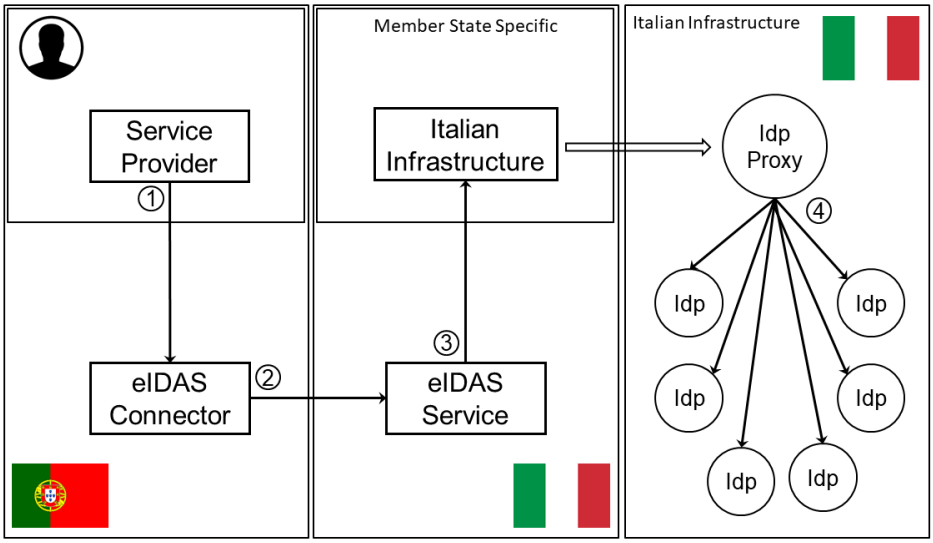

Fig. 1: eIDAS Authentication Flow

1) The Service Provider (SP) creates a eIDAS compliant SAML Authentication Request sends it to the Portuguese eIDAS Node, requesting the Minimum Data Set (MDS);
2) The Portuguese eIDAS Node sends a SAML Authentication Request to the Italian eIDAS Node;
3) The Italian eIDAS Node sends a SAML Authentication Request to the Italian Infrastructure;
4) Due to Italian's eID infrastructure another step is required, the Authentication Request from step 3 is received by an IdP Proxy, this proxy allows the Italian citizen to choose from a variety of IdPs available to him. The proxy sends an Authentication Request to the IdP selected.
5) The user is now at the IdP where he can use his credentials to authenticate.

The steps 1,2,3 must use the SP Initiated POST-POST Binding of the SAML specification, this is because the 1st step needs to also send a "CountryCode" attribute in the POST message, the "CountryCode" determines the eIDAS Node the eIDAS Service will send the Authentication Request to. The fourth step is MS specific but in the case of Italy it is also a SP Initiated POST-POST Binding started by their IdP Proxy, in the case of Portugal there is no step 4, eIDAS connects directly to the only national IdP.

III. EID4U

The eID for University (eID4U) is a project that builds upon the eIDAS regulamentation, enhancing and adding to its services. The goal of the project is to implement three eIDAS-enabled academic e-services. eRegistration, eLogin and eAccess[4]. To implement these new services a set of new attributes (personal and academic attributes) need to be created and implemented.

An eID4U Node is an eIDAS Node which supports the attributes declared in the eID4U project, an improvement of the original eIDAS specification with the objective of allowing new and more diversified services to work with the eIDAS Network. The eID4U and eIDAS nodes can work with each other but only to exchange non eID4U attributes.

In this project a standard set of attributes was defined, due to the purpose of each attribute they were divided into two categories:

- **Personal Attributes** - Contain personal and identification information about a person, e.g. name, surname, date of birth and others. These attributes have a broader range of uses, a sector such as eHealth or eCommerce could take advantage of a higher variety of personal attributes.

- **Academic Attributes** - Contain information regarding the academic career of a student. These attributes are specific to the academic sector and it's services. These attributes contain information pertaining to both current and past studies, like the home institution, home institution's country and level of studies.

A. Portuguese eIDAS Node

Each eidas node has a Member State (MS) specific part that needs to be developed in order to connect the eIDAS Service to the IdP from that MS (or IdP equivalent if the MS doesn't use a federated identity model), this development was made by Caixa Mágica for the portuguese eIDAS Node. During this development the mapping of attributes is defined between the eIDAS attributes and the MS specific attributes. As other Nodes, the portuguese Node must also be configured and managed, an effort provided by the national agency Agência para a Modernização Administrativa (AMA).

At the portuguese IdP, Fornecedor de Autenticação (FA), the user can authenticate using different methods, however only two are relevant for eIDAS due to the trust level required:

- **Cartão de Cidadão** - Authentication via smart card, the most secure method available that has access to all FA attributes;
- **Chave Móvel Digital (CMD)** - A One Time Password (OTP) method that sends a code to a phone number linked to the citizen, less secure than the smart card and as such cannot provide all attributes to a SP.

There are three types of attributes in the Portuguese eIDAS Node: the notified attributes, attributes that had been already implemented; the personal attributes which were not sector specific that were added to the Portuguese eIDAS Node; the academic attributes, sector specfic attributes, planned to be used by universities and other academic services.

Since some of the notified attributes, presented in table I, were not implemented or were not working as intended, an evaluation of the current state was necessary, after the evaluation a proposal was created with an implementation or fix for each of the misconfigured attributes. The proposal was accepted and integrated with the Portuguese eIDAS Node.

Friendly Name	**Uniform Resource Identifier (URI)**
FirstName	http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName
FamilyName	http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName
DateOfBirth	http://eidas.europa.eu/attributes/naturalperson/DateOfBirth
PersonIdentifier	http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier
Gender	http://eidas.europa.eu/attributes/naturalperson/Gender
PlaceOfBirth	http://eidas.europa.eu/attributes/naturalperson/PlaceOfBirth
CurrentAddress	http://eidas.europa.eu/attributes/naturalperson/CurrentAddress

TABLE I: Portuguese eIDAS notified attributes

Personal attributes are attributes which can be retrieved directly from the portuguese IdP, Fornecedor de Autenticação (FA). FA either stores these attributes or retrieves them from the national identity card. The academic attributes are not directly provided by FA instead the portuguese IdP uses an Attribute Aggregator (AG), Interoperabilidade na Administração Pública (iAP). FA constructs the Response on a per attribute basis, it only asks iAP for the academic attributes, iAP has an internal mapping for each attribute linking it to a certain Attribute Provider (AP).

B. eRegistration

The eRegistration service aims to register or enroll foreign students, particularirly EuRopean Community Action Scheme for the Mobility of University Students (ERASMUS) students, in University of Lisbon (ULisboa) using their national Electronic Identity (eID) retrieved using the eIDAS Network. I will be using the new attributes declared in the eID4U project to fill ERASMUS application forms. ERASMUS registration will give access to the academic platform of ULisboa for the accepted foreign students.

The ERASMUS registration process predates theeIDAS infrastructure and therefore it is independent from it, however the process can be improved usingthe eID4U's new attributes, refactoring the process. Enabling ERASMUS registration via eIDAS Network, is a usability improvement of the Account and ERASMUS application creation, with the single action of authenticating in the eIDAS Network. The process is initiated by selecting the ERASMUS application in FenixEdu the academic system of the schools of University of Lisbon (ULisboa). After choosing the degree the student wishes to apply to, FenixEdu redirects the user to a page where he can choose one of the supported eID4U countries to start the authentication process.

After authenticating in the eIDAS Network and retrieving all the attributes necessary FenixEdu creates an Account and an ERASMUS Application by attempting to fill the student's personal and academic information and attaching the necessary documents. Although FenixEdu can do a simple validation based on the attributes returned in the authentication process using the eIDAS Network, the International Relations Office and Academic Services must proceed with the validation of certain requirements, but with more assurance on the information provided by eIDAS than provided by the student.

1) Integration of FenixEdu in eIDAS as a Service Provider: In this role FenixEdu will connect to the the Portuguese eIDAS Proxy Connector with the objective of retrieving attributes and authenticating users, so they can apply to the ERASMUS program. Each ULisboa School has its own FenixEdu platform instance, which at the time of writing this article is 16 instances, identified by their own domain and accessible publicly by their Uniform Resource Locator (URL).

The integration code to connect with eIDAS node is based on the **Demo-SP**, since FenixEdu also runs in a Java Virtual Machine (JVM) and is programmed in Java. Here FenixEdu acts as a SP, connecting to the eIDAS Portuguese Connector. First tested using the ULisboa eID4U machine and then changed the endpoint to the pre-production PT eIDAS node, in this node all 16 FenixEdu instances had to be white-listed, however due to the instances sharing SP properties Agência para a Modernização Administrativa (AMA) only had to import one set of Metadata, Sign and Encryption certificates.

2) Integration of FenixEdu in eIDAS as an Attribute Provider: In this role FenixEdu will connect to the the Portuguese Infrastructure, specifically to Interoperabilidade na Administração Pública (iAP), with the objective of publishing the academic attributes not present in the Portuguese Infrastructure to eIDAS, the academic attributes.

Each school has an academic system, a FenixEdu instance, so iAP doesn't know which instance to query to obtain the data of the student, since the data of the student might be scattered between the instances. The chosen solution was to name one of the FenixEdu instances as the master instance, FenixEdu-REIT, and connect it to the iAP. The master instance receives the request from the iAP and conveys it to all other instances. The request contain the Portuguese Citizen Card Number to identity the respective student, along with the requested academic attributes. FenixEdu-REIT will query each slave instance including it's own instance for the academic attributes using a WebService. The workflow is detailed in the figure 2.

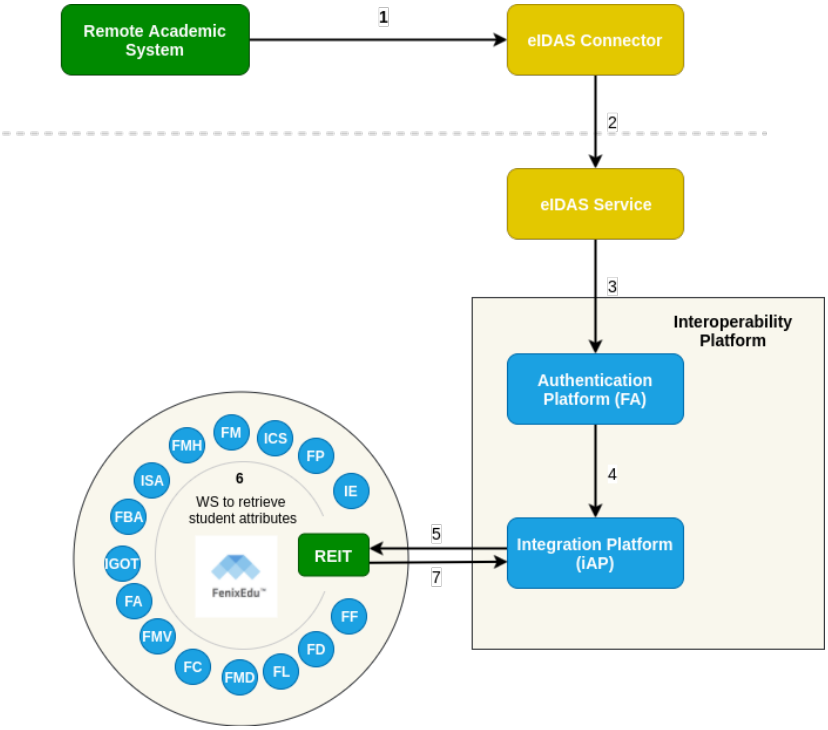

Fig. 2: eIDAS academic attributes Request Flow

For a Portuguese student to apply, via eRegistration, to an ERASMUS program in an Italian University he must follow this sequence of steps:

1) Portuguese student navigates to the Italian eRegistration page, by following the designated steps at the Italian academic service. The academic service, also known as a SP, will send a SAML Authentication Request asking for personal and academic attributes to the Italian eIDAS Connector:
2) the Italian eIDAS Connector will send a SAML Authentication Request and redirect the student to the Portuguese eIDAS Service, the Authentication Request will request the same attributes with no mapping or translation.
3) Now on Portuguese ground, the eIDAS Service will send one more SAML Authentication Request and redirect to Fornecedor de Autenticação (FA) the portuguese IdP, asking for the personal and academic attributes.
4) FA authenticates the user, asks for consent for each attribute requested and fetches the personal attributes from an internal database and request the academic attributes from iAP, through a WebService.
5) Interoperabilidade na Administração Pública (iAP) is an Attribute Aggregator (AG), it checks the attributes requested and creates a request for the appropiate AP, in this case ULisboa. The iAP formulates an asynchronous request via Simple Object Access Protocol (SOAP) to the master FenixEdu instance, FenixEdu-REIT.

6) FenixEdu-REIT queries each FenixEdu system from each school for the academic data of the student and also for the consent to share their data with eIDAS and other entities. A student can have data from several schools, in that case the data is evaluated so the attributes only send the most relevant data, so the following precedence is applied:
   a) The group of academic attributes in which the student is currently enrolled in a degree has more precedence.
   b) If the student is enrolled in more than one degree, the one with higher academic level has more precedence.
   c) If the student is not enrolled in any degree, the degree with higher academic level takes precedence.
7) Fenix-REIT aggregates the data and responds via SOAP to the iAP.

C. eLogin

The purpose of the service eLogin is to allow ULisboa's users to authenticate with the eIDAS Network: european citizens should be able to authenticate using the eID from their country and portuguese citizens should also be able to authenticate with the portuguese national IdP, Fornecedor de Autenticação (FA). The most challenging issue for this service is the lack of a practicable unique identifier in eIDAS so the identification of an user is done using attribute matching.

For an user to be authenticated in the ULisboa Identity Management (IdM) system, NetIQ's Identity Manager (IDM), some requirements need to be met there are different requirements for Portuguese citizens and European citizens but the important thing is that we can join the attributes sets from both types of requirements into one thanks to one of NetIQ's Access Manager (AM)'s functionality. NetIQ's Access Manager (AM) directly connects to the IDM and provides it with the attributes needed for authentication. An unique match is required, only one unique user in IDM must match with the attributes received.

To connect NetIQ's Access Manager (AM) and the portuguese eIDAS Service there are a challenges that need to be solved. These challenges can be divided into three categories: eIDAS SAML requirements, attribute mapping and country selection. The first and third challenge are in the process of creating a SAML Authentication Request valid for the eIDAS Node, the second challenge is present when receiving the Authentication Response from the eIDAS Node.

One of the biggest issues with the eIDAS Network is the connection of a new SP to the eIDAS Nodes, this project is no exception. It is not possible to directly connect NetIQ's Access Manager (AM) to an eIDAS Node, the only challenges AM can directly resolve are the Authentication Request signing and the Level of Assurance. To solve the challenges present in this section a proxy was created, ULisboa eIDAS Proxy (ULEP).

1) ULEP: ULisboa eIDAS Proxy (ULEP) is a Legacy Proxy developed to connect AM and the Portuguese eIDAS Node. It was created to solve the usual issues legacy SPs have when connecting to an eIDAS Node, with the proper configuration this solution can be used with other legacy SPs.

Due to it's role as a Proxy, ULEP is composed of three modules all developed using Java, the SP module that creates and receives messages from the eIDAS Node, the IdP module that creates and receives messages from the legacy SP, in this case AM, and the *CountryCode* resolver.

The SP module is based on the **Demo-SP** provided by the eIDAS package. There are two objectives the SP module must achieve: the first objective is to create the Hypertext Transfer Protocol (HTTP) POST message sent to eIDAS that consists of the SAML Authentication Request, meeting the eIDAS SAML requirements, and also the parameter *CountryCode*; the second objective is to validate and decrypt the encrypted eIDAS SAML Authentication Response and extract the user's attributes so they can be used in the IdP module.

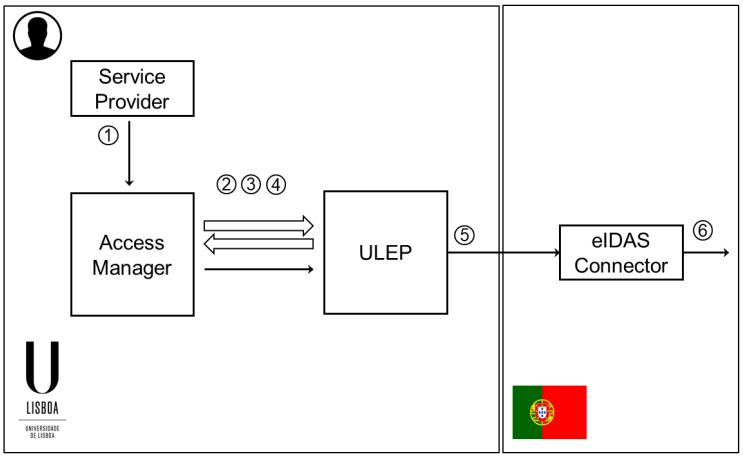

Fig. 3: eLogin Authentication Request Flow

The *CountryCode* resolver is a page that allows the user to choose the destination eIDAS Node. AM cannot send a SAML Authentication Request and a POST parameter (*CountryCode*) at the same time, so a page was created in AM, where the user

can choose his destination country, AM sends the parameter to the *CountryCode* resolver, ULEP then stores the *CountryCode* in the user's browser session and then redirects the browser to AM's SAML creation page.

The IdP module uses the SAML library OpenSaml v2 to create the SAML messages. The objectives of the IdP module are: to receive the Authentication Requests from AM and forward the important information to the SP module; to translate and map the attributes received from the eIDAS Network into the attribute set of AM; create an Authentication Response to send to AM with the translated attributes.

2) eLogin Authentication Flow: Figure 3 depicts the flow of the Authentication Requests of a user trying to access ULisboa's services and using the eIDAS Network as his means of authentication.

An user is trying to access a service connected to ULisboa's Single Sign-On (SSO) system:

1) The SP sends an Authentication Request to AM;
2) In the landing page of AM the user can choose one of several IdPs to authenticate with, one of them being eIDAS, after choosing the eIDAS option a new page is shown to the user where he can select which country he will authenticate with. When the country is selected by the user AM redirects to ULEP with the *CountryCode*;

Fig. 4: ULisboa SSO page

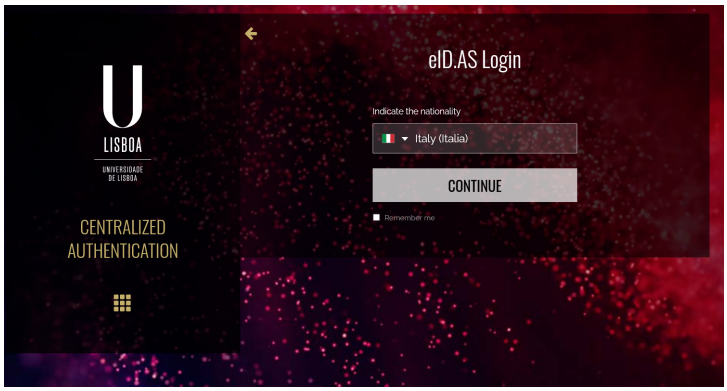

Fig. 5: eIDAS Page

3) ULEP stores the *CountryCode* in a session and promptly redirects to AM, this step is not shown to the user.
4) Now AM creates an Authentication Request and sends it to ULEP;
5) ULEP creates a POST message to the Portuguese eIDAS Connector with the *CountryCode* from the session and a SAML Authentication Request with the attributes necessary for login and the requirements necessary for eIDAS.
6) The Portuguese eIDAS Connector sends an Authentication Request to the respective eIDAS Node which is dictated by the *CountryCode*.

After the user authenticates at one of the IdP supported in the eIDAS Network the Portuguese eIDAS Connector will receive an Authentication Response related to the previously sent Authentication Request, depicted in figure 6.

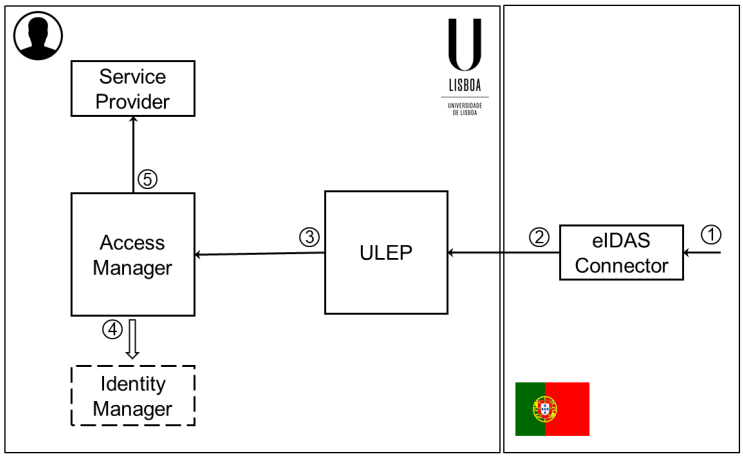

Fig. 6: eLogin Authentication Response Flow

1) The Portuguese eIDAS Connector receives an encrypted Authentication Response by another eIDAS Node;
2) The Portuguese eIDAS Connector sends an encrypted Authentication Response to ULEP;

3) ULEP receives an encrypted Authetication Response, it decrypts the Response and extracts the eIDAS attributes. It takes the eIDAS attributes and translates them into AM attributes, i.e joining the attributes "FirstName" and "FamilyName" to create the attribute "FullName" or changing the format of "DateOfBirth". Then it creates an Authentication Response with the AM attribute set and sends it to AM.
4) Depending on the type of authentication, national or european (dictated by *CountryCode*), AM translates the attributes received from ULEP to IDM attributes and connects to IDM's eDirectory to verify the identity of the user.
5) If a match is found it sends an Authentication Response to the SP with the unique identifier of the master identity of the user and some personal data.

Friendly Name	eIDAS Attribute
First Name	FirstName
Family Name	FamilyName
Citizenship Country	CountryCode
Date of Birth	DateOfBirth
Citizenship ID	IdNumber

TABLE II: eLogin eIDAS Attribute Set

D. eAccess

At it's core eAccess plans to solve a Wireless Local Area Network (WLAN) access problem, it is planned to be used during events organized by universities (such as project meetings, open conferences and seminars). In these events, there are several ways to provide WLAN access, each method with it's own issues.

To accomplish this goal, Zeroshell will be used as a gateway, Dynamic Host Configuration Protocol (DHCP) server, Captive Portal, and Security Assertion Markup Language version 2.0 (SAML v2.0) SP. ULEP will be used as an application that can relay and transform the Authentication Requests and Authentication Responses between Zeroshell's SP and the portuguese eIDAS Node (Connector). The authentication provider will be the eIDAS Network.

In the following figure 7 is the flow of the authentication process implemented. This is how a captive portal with an external authentication service must authenticate.

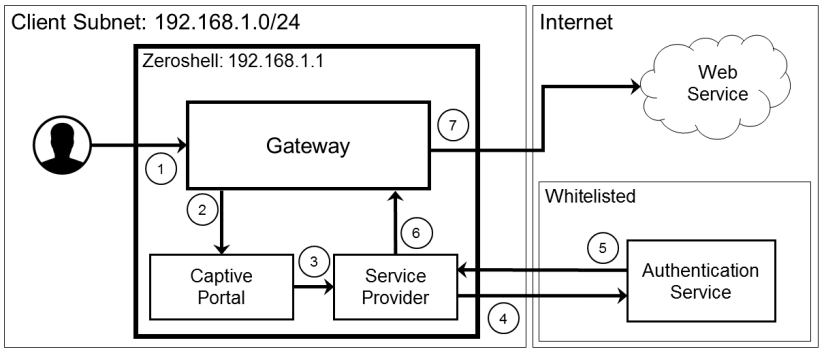

Fig. 7: eAccess Authentication flow using Zeroshell's Captive Portal with external SAML authentication

In the figure 8 we can see the flow of the authentication process inside the Authentication Service (AS). The first entity of the AS will receive the request sent by the SP (4), due to previous mentioned limitations of the SP the application that receives this SAML Request (ULEP) will have to transform it in order to be in compliance to the eIDAS standards, this includes providing a web page where the user chooses his country so the eIDAS Connector knows which eIDAS Service it needs to redirect to. In step (A) ULEP will send an Authentication Request with the attributes necessary, the attribute set required to perform a successful authentication, to the portuguese eIDAS Connector which will promptly redirect the user to the eIDAS Service corresponding to the country the user selected (B). In the eIDAS Service the user will be asked for consent about the attributes that were requested in the Authentication Request made to the eIDAS Connector and then he will be redirected to the national IdP of the country (C) (simplified, different countries have different eID systems).

The IdP will authenticate the user and will trigger a chain of responses to the previous requests, starting with step (D), it will send an Authentication Response with the attributes necessary, the SAML Assertion will be encrypted by the eIDAS Service and the user will be redirect to the eIDAS Connector (E). Finally ULEP will receive the SAML Response from the eIDAS Connector (F), with an encrypted SAML Assertion. Before ULEP responds to Zeroshell's Shibboleth it decrypts the Assertion so the Shibboleth can retrieve the attributes of the user, triggering the final Authentication Response (5) to the SP.

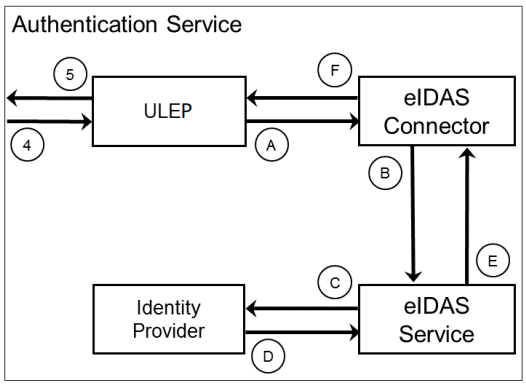

Fig. 8: eAccess' AS individual components and authentication flow

IV. Conclusion

A. Discussion

This article has provided some maturity to the eIDAS environment, especially on the Portuguese eIDAS Node. Some flaws with the previous implementation of the eIDAS Node in Portugal were discovered and a proposal was made to fix them, which was accepted, these flaws had to do with the translation and mapping of attributes from the Portuguese IdP, Fornecedor de Autenticação (FA), and the eIDAS Service module of the Portuguese eIDAS Node.

The Portuguese eIDAS and 4 others (Italy, Spain, Slovenia and Austria) have also added two different sets of attributes to their supported attributes, the personal attribute set and the sector-specific academic attribute set. The support of these attributes in an eIDAS Node implies the proper retrieval of these attributes from the Member State (MS) Electronic Identity (eID) scheme, which was also implemented in this project. The support of new attributes increases the possible use cases for SP connected to eIDAS, maturing the eIDAS environment and also increasing the incentive for new SP to adopt eIDAS as either an authentication mechanism or a way to retrieve attributes for it's users.

Once more the maturity of the eIDAS environment has been increased by the creation of 3 different eIDAS-enabled services in eRegistration, eLogin and eAccess. The implementation of these services can serve as an example to the community in how to integrate with eIDAS and also the benefits of using eIDAS over other authentication systems. These services have also contributed to an influx of real users into the eIDAS environment.

One of the biggest challenges of eIDAS is it's takeoff, by that I mean the difficulty for the project to gain wide adoption, this issue is shown by the fact that few users know of eIDAS therefore they don't know how to use the system or what is is for. This issue is exacerbated by the lack of usage of the eID systems of some MSs by it's citizens, in recent years the services that use national authentication and the users that use these systems have increased which helps eIDAS because eIDAS relies on the eID infrastructure of each MS and so it relies on citizens knowing how to use their own MS eID.

Despite the lack of real users using the eIDAS Network the most concerning issue for the takeoff challenge is the lack of adoption of the eIDAS system by SPs. The lack of adoption is caused by two main reasons: the lack of real users that can use the eIDAS system but primarily the difficulty of integrating legacy systems with the eIDAS Network due to it's high security requirements.

In this article I have presented one possible solution to integrate legacy SPs with the eIDAS Network, this solution is to create a legacy proxy that can adhere to eIDAS security requirements and can also communicate with the legacy system. ULEP is the manifestation of this idea for ULisboa it adheres to all of eIDAS requirements and connects to the legacy systems of ULisboa, NetIQ's Access Manager (AM). This solution can be configured to work with other systems besides ULisboa since it is a eIDAS compatible legacy proxy.

The service eRegistration has also shown the possible utility of adding new attributes to the eIDAS Network, with a wider variety of attributes eIDAS can be used in a wider variety of services. eRegistration has also paved the way for more Portuguese Attribute Providers (APs) to connect to the Portuguese infrastructure through Interoperabilidade na Administração Pública (iAP). By integrating more APs into the Portuguese infrastructure more attributes are available to be used by Portuguese services connected to FA or by foreign services connected to the eIDAS Network. The lessons learned during the development of this service can serve as stepping stones for the integration of other types of attributes into the eIDAS Node for example e-Health attributes already available in the Portuguese infrastructure and these lessons can also help with the AP connection to iAP.

Finally these services have improved the services of ULisboa: eRegistration has improved the ERASMUS application process for foreign users also decreasing errors in the process and decreasing the need of validation resources at the International Relations Office; eLogin has improved the authentication system of ULisboa by providing a new IdP choice for the user, both for national users and foreign users (it has also resulted in the normalization of data in ULisboa's identity management system); eAccess has improved wi-fi access in ULisboa by adding a new network to the university's Access Point (AcP).

B. Final Thoughts

Complex Identity Management (IdM) systems are needed to solve identity validation issues on a university, national or european scale. These complex systems have to thread a fine line between usability and giving too many options to users. In order to support various independent systems with different implementations standards have to be created, validated and implemented by all parties involved.

This project developed a possible inclusion to the eIDAS standard by implementing new attributes, personal and academic, these attributes would allow the independent services to extract more value from the eIDAS protocol being implemented little by little all across europe. The creation of new use cases for eIDAS compliant services is a stimulant for new organizations to adopt the eIDAS standard, maturing the environment itself. Standard work better the more ubiquitous they are, just like the usb battery charger standard has completely improved the landscape for the users.

The objective to improve the eIDAS standard and also the improvement of the national Electronic Identity (eID) infrastructure was complete with also the implementation of three services as a proof of concept using the proposed changes to the standard.

REFERENCES

[1] E. Commission, "A Digital Single Market Strategy for Europe," https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192, 2015

[2] E. Union, "Regulation (eu) no 910/2014 of the european parliament and of the council of 23 july2014 on electronic identification and trust services for electronic transactions in the internal mar-ket and repealing directive 1999/93/ec," inISSE 2010 Securing Electronic Business Processes.European Union, 2014

[3] H. Leitold and B. Zwattendorfer, "Stork: architecture, implementation and pilots," inISSE 2010Securing Electronic Business Processes. Springer, 2011, pp. 131–142.

[4] D. Berbecaru and A. Lioy, "On integration of academic attributes in the eidas infrastructure to sup-port cross-border services," in2018 22nd International Conference on System Theory, Control andComputing (ICSTCC). IEEE, 2018, pp. 691–696

[5] D. Berbecaru, A. Lioy, and C. Cameroni, "Electronic identification for universities: Building cross-border services based on the eidas infrastructure,"Information, vol. 10, no. 6, p. 210, 2019.

[6] "eidas saml message format, version 1.1. available online:https://ec.europa.eu/cefdigital/wiki/download/attachments/80183964/eIDAS%20Message%20Format_v1.1-2.pdf?version=1&modificationDate=1497252919575&api=v2."

[7] "Hughes, j.; cantor, s.; hodges, j.; hirsch, f.; mishra, p.; philpott, r.; maler, e.profiles for the oasissecurity assertion markup language (saml) v2.0. oasis standard. march 2005. available online:http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf."