Article

Enhancing University Services by Extending the eIDAS European Specification with Academic Attributes [†]

Álvaro Alonso ^{1,*} , Alejandro Pozo ¹ , Aldo Gordillo ² , Sonsoles López-Pernas ¹ ,
Andrés Muñoz-Arcntales ¹, Lourdes Marco ¹ and Enrique Barra ¹

¹ Departamento de Ingeniería de Sistemas Telemáticos, Escuela Técnica Superior de Ingenieros de Telecomunicación, Universidad Politécnica de Madrid, 28040 Madrid, Spain; alejandro.pozo@upm.es (A.P.); sonsoles.lopez.pernas@upm.es (S.L.-P.); joseandres.munoz@upm.es (A.M.-A.); lourdes.marcosp@alumnos.upm.es (L.M.); enrique.barra@upm.es (E.B.)

² Departamento de Sistemas Informáticos, Escuela Técnica Superior de Ingeniería de Sistemas Informáticos, Universidad Politécnica de Madrid, 28031 Madrid, Spain; a.gordillo@upm.es

* Correspondence: alvaro.alonso@upm.es

[†] This paper is an extended version of our paper published in Alonso, A.; Gordillo, A.; Pozo, A.; López-Pernas, S.; Marco, L.; Barra, E. Extending the eIDAS European Specification for Supporting Academic Attributes. Proceedings of the 12th International Conference of Education, Research and Innovation (ICERI 2019), Seville, Spain, 11th–13th November 2019; pp. 2008–2014.

Received: 19 December 2019; Accepted: 17 January 2020; Published: 21 January 2020

Abstract: The European electronic IDentification, Authentication and trust Services (eIDAS) regulation makes available a solution to ensure the cross-border mutual recognition of electronic IDentification (eID) mechanisms among Member States. However, the basic set of attributes currently provided by each country only contains citizens' personal and legal attributes, preventing e-services to take full advantage of citizens' domain-specific information, such as academic or medical data. In this article, we propose an extension of the eIDAS specification to support academic attributes as part of citizens' profiles. In addition, we present an architecture to enable the connection of eIDAS nodes to national attribute providers to enrich citizens' profiles with additional academic attributes. We have deployed the eIDAS extension in the specific case of the Spanish eIDAS infrastructure, and we have connected it to an attribute provider of the Technical University of Madrid (UPM). We have also improved a set of institutional services of that university by enabling the connection to eIDAS and enhancing the features offered to students based on their academic profiles retrieved from the eIDAS extended infrastructure. Finally, we have evaluated the resulting services thanks to real students from two different countries, concluding that the widespread adoption of the proposed solution in the academic services of European universities will greatly improve their quality and usability.

Keywords: academic attributes; electronic identification; eIDAS; erasmus; identity; e-Services; student mobility

1. Introduction

Secure electronic IDentification (eID) is one of the key factors that facilitates privacy, data protection, and prevention of online fraud [1]. It can guarantee the unequivocal identification of a person, ensuring that services are only delivered to individuals who are truly entitled to them. However, to date, the shortage of a common legal basis prevented European Member States from recognizing and accepting eIDs issued by other Member States, thus preventing citizens and companies from completely taking advantage from the digital single market [2].

The electronic IDentification, Authentication and trust Services (eIDAS) Regulation [3] solves the aforementioned problems by guaranteeing the cross-border reciprocal recognition of eIDs. In 2015, the Connecting Europe Facility (CEF) program published the technical specifications and reference implementations of the interoperability between eIDAS nodes for enabling the eID mechanisms (which have been updated to their last version recently [4]). The ultimate goal of this initiative is to allow citizens of any European Member State to use their national eIDs to gain access to public and private e-services provided by other Member States in a secure way.

Since 2017, the CEF program also aims to promote the use of nationally issued eIDs for cross-border student authentication, as well as the integration of eIDAS in existing e-services in the higher education sector in order to facilitate the mobility of students within the European Union (EU). However, the basic set of attributes provided by the Member States (known as the “minimum dataset”, MDS) only contains citizens’ personal and legal attributes. As a consequence, academic services cannot exploit the advantages of integrating students’ eIDs to the same extent as though they included attributes related to their academic profile as well.

The objective of this research is to provide an extension of the eIDAS Regulation to support academic attributes. Thanks to this extension, academic e-services can guarantee the unequivocal identification of students and enhance the functionalities offered thanks to the integration of their academic profiles. Moreover, we provide details about how to modify the eIDAS reference code to include new attributes so the same methodology can be applied to services of other domains such as e-health, e-banking, etc.

Thus, in this article we extend our work from [5] by proposing an extension of the eIDAS specification to academic attributes, and by reporting on how this extension has been successfully implemented in Spain. Thanks to this extension, digital educational services can request students’ information from the eIDAS nodes, including not only their personal profiles but also additional attributes related to their academic profiles, such as their field of study, the institution where they are pursuing their studies, and their language proficiency certificates among other relevant information. This sort of data is especially useful for enhancing higher education student mobility programs across Europe, which require students to use educational e-services in foreign universities that need to have access to their academic information.

For the eIDAS nodes to provide academic attributes to services, these attributes need to be procured by certified institutions beyond the national identity providers (e.g., the sending institution in the student mobility example). In this work, we also propose an architecture that allows the connection of the national eIDAS nodes to academic attribute providers to enrich the student MDS with academic attributes.

With the aim of validating our proposal, we have implemented and deployed the architecture necessary for making the solution compatible with the specific case of the Spanish eIDAS infrastructure and an attribute provider of the Technical University of Madrid (*Universidad Politécnica de Madrid*—UPM). Moreover, we have connected this infrastructure with other eIDAS nodes deployed in Portugal, Slovenia, Italy and Austria that also support the proposed extension. Finally, we have adapted a set of Spanish academic e-services offered by UPM to allow students’ authentication through eIDAS-compliant national eID, as well as to exploit the students’ academic profiles received from the eIDAS infrastructure. Taking advantage of this deployment, we have tested the proposal with two groups of users: (1) Spanish students who access foreign eIDAS-enabled services and whose academic profile is provided by the UPM attribute provider, and (2) foreign users who consume eIDAS-enabled services delivered by UPM which exploit their academic attributes.

After analyzing the results of the performed tests, we extract several conclusions about the implementation of the proposal in the case of Italian and Spanish academic e-services. Moreover, thanks to our proposal, we establish the base for extending the eIDAS regulation with extra attributes in other domains such as e-banking and e-health, in which the use of eID can improve security and confidentiality. On the other hand, the presented experience with the integration of external

attribute providers to enrich the citizens profiles can be applied to those other domains using specific attribute providers.

The manuscript is structured as follows. In Section 2, we present an overview of the existing related works in the literature. Section 3 introduces the basis of the eIDAS regulation and the attributes currently provided. Then, in Section 4, we describe our extension proposal to support academic attributes and to connect the eIDAS infrastructure to attribute providers. The implementation, deployment and tests conducted with real users to validate the proposal are provided in Section 5. Finally, Section 6 concludes the work and suggests future lines of research.

2. Related Work

The European Union has embarked upon several efforts to facilitate the mobility of citizens across Member States by improving the management of their digital identity. The European project STORK (Secure idenTity acrOss boRders linKed) focused on securing and providing cross-border authentication and established the basis of what would later be eIDAS. Several studies [6–8] have described the STORK architecture and brought some insights that should be taken into account in any deployment using the new eIDAS infrastructure, such as the need to preserve privacy.

There are some similarities between the eIDAS infrastructure and that of STORK (described in [6]). The main one lies in the fact that in both solutions, each Member State is in charge of deploying their own infrastructure, which is connected to those of other countries, thus enabling cross-border authentication. Nevertheless, in contrast with STORK, the new eIDAS regulation complies with some new critical security requirements, such as ciphering connections between peers to preserve the confidentiality of citizens.

The authors of [9] support the idea of eIDAS as the optimal way of addressing the new requirements regarding cross-border authentication for sectors such as e-banking [10] and e-Health [11]. They urge Member States to continue with the implementation of the eIDAS regulation due to the expected increase in mobility of European citizens among Member States.

From a technical point of view, in order to provide cross-border authentication, the eIDAS nodes of Member States are interconnected using the SAML 2.0 standard [12]. Although each Member State is free to decide how their services need to be connected to their national eIDAS node, these services are usually connected through SAML 2.0 as well. In this regard, it should be pointed out that this standard implies several limitations in the integration of services with eIDAS nodes [13].

On the other hand, OAuth 2.0 [14] is recognized as the most widespread protocol for delegated authentication [15–17], standing out over SAML 2.0 for its simplicity, scalability, ease of integration and lightness [18,19]. As can be seen in a recent study by some of the authors of the present article [20], service providers can delegate and ease the login process of the eIDAS infrastructure through an identity manager based on OAuth 2.0. The aforementioned study proposes an architecture based on a gateway, which is a single sign-on authentication point between services and eIDAS nodes. This gateway translates simple OAuth 2.0 requests made by services into more complex SAML requests towards eIDAS nodes.

The aforementioned work also reported on the integration of eIDAS with an access control architecture that allows services to manage access policies for their resources based on citizens' eID profiles. The authors of [21] faced the same topic, proposing a system based on the Extended Access Control (EAC) protocol and oriented to the German identity card that also provides strong cryptographic guarantees, including the privacy of the attributes against outsiders.

Regarding security and privacy, other approaches are trying to improve the eIDAS specification taking advantage of new concepts and technologies. The authors of [22] compared the way in which pseudonymization is addressed by eIDAS with respect to the General Data Protection Regulation (GDPR). They concluded that the two regulations employ different notions of the concept and opened a discussion to establish a common terminology. On the other hand, Abraham [23] proposed the

connection of eIDAS nodes to a decentralized identity management system to provide a self-sovereign identity approach.

Some authors have proposed approaches for including human-related factors when designing innovative services and demonstrate how their performance can be improved [24,25]. In this sense, the eIDAS regulation for providing electronic identification to citizens has drawn the attention of educational institutions due to the potential benefits of integrating electronic identification in academic services [26]. In this regard, [27,28] outlined the benefits of integrating higher education services such as eAccess and eDiploma into the eIDAS infrastructure.

Meanwhile, the CEF Telecom program is promoting the use of eIDAS by funding several projects that aim to integrate eIDAS-compliant eID authentication in educational services. The two main concerns when integrating services into an eIDAS infrastructure are: (1) the definition of domain-specific attributes and (2) the improvement of e-services exploiting such attributes. In this sense, Stasis et al. [11] pointed out the need for including health attributes of patients for better management of healthcare. Likewise, in academic services, the set of attributes of citizens provided should be extended with student data such as language certificates and the degree name.

ESMO Project [29], one of the CEF Telecom financed projects, propose the deployment of proxies between the service providers and the eIDAS infrastructure to retrieve students' academic profiles from attribute providers. The main advantage of this design is that the eIDAS reference implementation, and consequently the implementation of the eIDAS nodes, remains unaltered. However, additional federation mechanisms between the attribute providers must be developed to ensure cross-border authentication.

Moreover, two additional CEF Telecom projects (TREATS and StudIES+) [30] have proposed several use cases in which the integration of eID authentication could definitively improve the user experience. One of these use cases is used to manage students' university credentials and the other one for administering research contracts. On the other hand, authors of [31,32] proposed the integration of the eIDAS regulation in the Erasmus registration process of the Agricultural University of Athens. However, any of these two works addressed the inclusion of academic attributes in the eIDAS specification.

Finally, eID4U project [33] proposes a solution for improving academic services in five Member States thanks to the inclusion of academic attributes into the eIDAS profile of citizens. In the scope of eID4U, the authors of this article together with professors and researchers from Politecnico di Torino, Universidade de Lisboa, Graz University of Technology, and Jozef Stefan Institute, have proposed a list of the most suitable academic attributes to be included in the extension of eIDAS profiles. Section 4 explains the details of this proposal. On the other hand, Liroy et al. [34–36] proposed the application of this extension to specific services provided by Politecnico di Torino as well as an architecture to obtain the new attributes from Italian certified sources. In the same line, Klobučar [37,38] showed the integration of the Slovenian higher education system with the extended eIDAS infrastructure.

3. eIDAS Bases

CEF eID is one of the several building blocks [39] provided by the European Commission, whose principal mission is to help service providers to enable the use of their online services to citizens from other Member States, being these services compliant with the eIDAS regulation in terms of trust, security and interoperability. This last requirement is accomplished thanks to, among other factors, the reciprocal recognition of national eID schemes (including mobiles, smartcards and digital certificates) among Member States. As a result, all citizens of EU countries can use their nationally issued eID to access to European services in a secure way.

Not only public services can benefit from an eIDAS integration, but also private services in need for an extra security level regarding the identification of users. Moreover, all web public application and services requiring electronic identification assurance [40] corresponding to a 'substantial' or 'high' level must be able to accept the notified eID schemes of other EU countries.

Citizens from any Member State can be authenticated by services deployed in any other EU country by using their national eID. As can be seen in Figure 1, citizens from a Member State who want to access a service deployed in a foreign one, are redirected to the eIDAS node of their country of origin to perform the authentication process. This delegation can be accomplished thanks to the SAML 2.0-based specification, which is used to connect eIDAS nodes from Member States to one another. Afterwards, citizens are redirected to the corresponding Identity Provider (IdP) through which they will be able to identify themselves by means of an eID of their country of origin. Once citizens authenticate through the eIDAS infrastructure, a SAML response containing the attributes requested by the service is created, encrypted and sent to the service.

Figure 1. eIDAS basic architecture.

As has been stated before, interoperability between eIDAS nodes is one of the key points to be addressed by the eIDAS regulation. Apart from the mutual recognition of national eID schemes, the definition of a common set of attributes of citizens' profiles in the eIDAS specification has been of crucial importance. These attributes can be of type *Natural Person* or *Legal Person*. The specification also describes the *eidas* namespace to unequivocally designate eIDAS attributes with the aim of avoiding ambiguity between identically named elements from other XML vocabularies [41]. Tables 1 and 2 show the attributes available in the eIDAS specification for each type of attribute. Mandatory attributes are marked with an asterisk.

Table 1. Available natural person attributes in eIDAS nodes.

FriendlyName	NameUri (http://eidas.europa.eu/attributes)	Namespace
PersonIdentifier*	/naturalperson/PersonIdentifier	eidas
FamilyName*	/naturalperson/CurrentFamilyName	eidas
FirstName*	/naturalperson/FirstName	eidas
DateOfBirth*	/naturalperson/DateOfBirth	eidas
BirthName	/naturalperson/BirthName	eidas
PlaceOfBirth	/naturalperson/PlaceOfBirth	eidas
CurrentAddress	/naturalperson/CurrentAddress	eidas
Gender	/naturalperson/Gender	eidas

Table 2. Available legal person attributes in eIDAS nodes.

FriendlyName	NameUri (http://eidas.europa.eu/attributes)	Namespace
LegalPersonIdentifier*	/legalperson/LegalPersonIdentifier	eidas
LegalName*	/legalperson/LegalName	eidas
LegalAddress	/legalperson/LegalPersonAddress	eidas
VATRegistration	/legalperson/VATRegistrationNumber	eidas
TaxReference	/legalperson/TaxReference	eidas
D-2012-17-EUIdentifier	/legalperson/D-2012-17-EUIdentifier	eidas
LEI (Legal Entity Identifier)	/legalperson/LEI	eidas
EORI (Economic Operators Registration and Identification)	/legalperson/EORI	eidas
SEED (System for Exchange of Excise Data)	/legalperson/SEED	eidas
SIC (Standard Industrial Classification)	/legalperson/SIC	eidas

When a service provider tries to authenticate a citizen, it is mandatory to request an MDS composed by CurrentFamilyName, FirstName, DateOfBirth and PersonIdentifier from Natural Person and LegalPerson and LegalPersonIdentifier from Legal Person. However, as stated before, we detect an increasing need for a more complete profile to be used in public services in sectors such as education and health. Therefore, it becomes apparent that the integration of domain-specific attributes into the eIDAS infrastructure is of high relevance. The following section describes which specific attributes have been integrated and how.

4. Proposed Solution

In this section, we propose a solution for enabling the use of academic attributes in the eIDAS infrastructure. Currently, many academic e-services provided by universities or other higher education institutions offer their students the possibility of logging in by using their national eIDs. Thanks to our proposed solution, these services can be enhanced taking advantage of the students' extended profiles provided by the eIDAS nodes that include academic information such as their field of study, the institutions where they carried out their studies, and their language certificates.

To enable the use of academic attributes in services connected to the eIDAS infrastructure, two important challenges must be addressed. As explained earlier, the current eIDAS specification only supports a set of personal and legal attributes known as MDS. This implies that services can only request these attributes when authenticating users by means of their eID since, if an authentication response coming from an IdP contains attributes not belonging to the MDS, the corresponding eIDAS node will remove them before sending the response to the service. Therefore, the first challenge consists of extending the eIDAS specification to support new attributes, specifically the academic attributes we have identified as the most common ones in scholar services.

The second challenge is related to the way in which the academic attributes of a specific student are provided for being consumed by services. Currently, the MDS provided by the Member States' IdPs includes personal and legal attributes. The solution to enrich that profile with academic attributes consists of including connections to third-party attribute providers in the authentication flow. The solution we propose to address these two challenges is presented below.

4.1. eIDAS Extension to Support Academic Attributes

To define the list of academic attributes that are typically used by university services, we have analyzed several services of UPM, Politecnico di Torino, Universidade de Lisboa, Graz University of Technology, and Jozef Stefan Institute, together with professors and researchers from said institutions. As a result of this analysis, we have identified the list of attributes shown in Table 3. All of them correspond to the type *NaturalPerson*. We have reused the namespaces defined by eIDAS and Europass [42] when possible and defined new ones when not. Table 4 summarizes the used namespaces and XML schemas.

Table 3. Academic attributes proposed for extending the eIDAS specification.

FriendlyName	NameUri (http://eidas.europa.eu/attributes)	Namespace
IdType	/sectorspecific/eid4u/naturalperson/id/Type	eid4uP
IdNumber	/sectorspecific/eid4u/naturalperson/id/Number	eid4uP
IdIssuer	/sectorspecific/eid4u/naturalperson/id/Issuer	eid4uP
IdExpiryDate	/sectorspecific/eid4u/naturalperson/id/ExpiryDate	eid4uP
EHICId (European Health Insurance Card Id)	/sectorspecific/eid4u/naturalperson/EhicId	eid4uP
Nationality	/sectorspecific/eid4u/naturalperson/Nationality	europass3
Citizenship	/sectorspecific/eid4u/naturalperson/Citizenship	europass3
MaritalState	/sectorspecific/eid4u/naturalperson/MaritalState	eid4uP
CountryOfBirth	/sectorspecific/eid4u/naturalperson/CountryOfBirth	europass3
Email	/sectorspecific/eid4u/naturalperson/Email	eid4uP
Phone	/sectorspecific/eid4u/naturalperson/Phone	eid4uP
TemporaryAddress	/sectorspecific/eid4u/naturalperson/TemporaryAddress	eid4uP
CurrentPhoto	/sectorspecific/eid4u/naturalperson/CurrentPhoto	eid4uP
TaxIdentificationNumber	/sectorspecific/eid4u/naturalperson/TaxIdentificationNumber	eid4uP
HomeInstitutionName	/sectorspecific/eid4u/studies/homeinstitution/Name	eid4uS
HomeInstitutionIdentifier	/sectorspecific/eid4u/studies/homeinstitution/Identifier	eid4uS
HomeInstitutionCountry	/sectorspecific/eid4u/studies/homeinstitution/Country	europass3
HomeInstitutionAddress	/sectorspecific/eid4u/studies/homeinstitution/Address	eid4uP
CurrentLevelOfStudy	/sectorspecific/eid4u/studies/CurrentLevelOfStudy	eid4uS
FieldOfStudy	/sectorspecific/eid4u/studies/FieldOfStudy	eid4uS
CurrentDegree	/sectorspecific/eid4u/studies/CurrentDegree	eid4uS
Degree	/sectorspecific/eid4u/studies/Degree	eqf
DegreeAwardingInstitution	/sectorspecific/eid4u/studies/DegreeAwardingInstitution	eid4uS
GraduationYear	/sectorspecific/eid4u/studies/GraduationYear	eid4uS
DegreeCountry	/sectorspecific/eid4u/studies/DegreeCountry	europass3
LanguageProficiency	/sectorspecific/eid4u/studies/LanguageProficiency	eid4uS
LanguageCertificates	/sectorspecific/eid4u/studies/LanguageCertificates	eid4uS

Table 4. Namespaces used in the attributes definition.

Namespace	URL
eid4uP	http://eidas.europa.eu/attributes/naturalperson
eid4uS	http://eidas.europa.eu/attributes/sectorspecific/eid4u/studies
europass3	http://europass.cedefop.europa.eu/Europass
eqf	http://europass.cedefop.europa.eu/EQF/08

To support the new academic attributes, we have modified the eIDAS sample implementation provided and maintained by CEF. The new version of the code has been published under the European Union Public License (EUPL) and it is publicly available at <https://github.com/eID4U/eIDAS-node>. The following changes have been introduced:

- XSD (XML Schema Definition) schemes for the new academic attributes have been defined. These schemes can be found at the `eID4U_commons/src/main/resources/schema/eid4u/` directory.
- A sample configuration for the new version of the eIDAS components has been elaborated based on the sample configuration of the eIDAS sample implementation. This configuration has been included in the `EIDAS-Config-eID4U` directory. In addition to a sample configuration for the eIDAS components, samples of definitions for all the new academic attributes are provided in the `server/idp/user.properties` file.
- The academic attributes have been added to the `saml-engine-additional-attributes*` files placed in the `EIDAS-Config-eID4U/server` directory and its subdirectories.

- The corresponding attributemarshallers have been developed and added in the files contained by the `eID4U_commons/src/main/java/at/gv/egiz/eid4u/` directory.

4.2. Connection to Academic Attribute Providers

Thanks to the proposed extension of the eIDAS specification, service providers can make a request to an eIDAS node for retrieving the users' academic attributes included in the proposed list. However, IdPs used by Member States to authenticate citizens in the eIDAS network typically provide only personal and legal attributes. Therefore, when the eIDAS node of the users' country of origin makes an authentication request to the corresponding national IdP, this IdP will respond including only the MDS attributes. In order to enrich the users' profile with academic attributes, third-party attribute providers must be consulted and hence included in the authentication flow. With the aim of achieving this objective, we propose to make use of a proxy between the eIDAS nodes and the IdPs, which will be in charge of requesting the extra attributes to the attribute providers.

Figure 2 shows an overview of the architecture we propose. Below, each component of the architecture is explained:

Figure 2. Connection to attribute providers.

- The **Local Service Provider** represents each of the Service Providers (SPs) deployed for offering a specific service for students, teachers and/or researchers. Each SP is registered and connected to the Local eIDAS Node of its country. Thus, it can send authentication requests for authenticating users by means of their eID.
- The **Local eIDAS node** represents an eIDAS node in which the deployed SPs are registered. This node must include the extension to support academic attributes explained above. The node is connected to the rest of the eIDAS nodes of European Member States, so requests sent by SPs for authenticating foreign citizens are redirected to the corresponding eIDAS node. The local eIDAS node also receives authentication requests delegated from foreign eIDAS nodes when a local citizen tries to authenticate to a foreign SP.
- **Foreign eIDAS nodes** receive authentication requests delegated from the local node when a foreign citizen tries to authenticate to a Local SP. On the other hand, foreign eIDAS nodes delegate authentication requests to the Local eIDAS node when a local citizen tries to authenticate to a foreign SP.
- **IdP Proxy and Attribute Provider Connectors.** The IdP Proxy intercepts authentication requests sent from an eIDAS node to the IdP for checking the attributes requested by an SP. After the authentication success in the IdP and its responses to the eIDAS node, the IdP proxy intercepts the flow again to verify the attributes received and to calculate the difference between these attributes

and the requested ones. If extra attributes are required, the IdP Proxy must request them to attribute providers (APs). Since many APs can be supported and the protocols to access them may be different, a specific connector (termed AP connector) must be used for each case. Therefore, each AP Connector is in charge of requesting attributes to a specific AP. If specific authentication methods are required by an AP, the corresponding AP Connector is also in charge of managing these methods (e.g., by showing authentication challenges and privacy consents directly to users). After receiving the requested attributes, an AP Connector is responsible for transforming them into the format imposed by the communication protocol between the eIDAS node and the Local IdP. If this protocol imposes the encryption or the signature of the messages, the IdP Proxy needs access to the corresponding certificates. When all the attributes provided by the APs have been included in the authentication response, the IdP Proxy sends the response back to the eIDAS node.

- **Attribute providers** offer access to academic attributes of students. When connecting the IdP Proxy to a specific AP, the communication protocol and the list of available attributes must be configured in the corresponding AP Connector.
- The **Local IdP** authenticates local citizens by means of their national eID. Depending on the protocol that each national IdP uses, both the connector module of the eIDAS node and the IdP Proxy, must be configured one way or another.

Figure 3 illustrates the flow for authenticating a foreign user accessing a Local SP. As explained above, the Local SP sends an authentication request to the Local eIDAS node, which redirects the request to the corresponding eIDAS node of the citizen's country. If the SP has requested academic attributes and the foreign country implements the extension to support them and the connection to an AP, the authentication response would include the extra attributes in the user profile. In that case, the SP could use these attributes to improve the user experience of the service.

Figure 3. Authentication flow for a foreign user.

Lastly, Figure 4 shows the authentication flow when a local user accesses an SP deployed in a foreign eIDAS infrastructure. In this case, when the foreign eIDAS node redirects the request to the local one, the authentication request sent to the Local IdP is intercepted by the IdP Proxy. The IdP Proxy analyzes the requested attributes and temporally saves a list with their keys. After authenticating the user in the Local IdP, the IdP Proxy calculates the difference between the list of attributes previously saved and the ones received in the authentication response. If extra attributes are required and some of the available APs provide them, the corresponding AP Connectors send a request to retrieve them. If any extra attribute is provided, the corresponding AP Connector parses it to the required format and

the IdP Proxy includes the result in the authentication response. Once all extra attributes have been included in the authentication response, the IdP Proxy sends this response back to the local eIDAS node, which in turn forwards it to the foreign eIDAS node that finally sends it to the SP.

As mentioned before, the authentication response received by the IdP Proxy from the IdP can be encrypted and signed. If that is the case, the IdP Proxy requires access to the certificates or keys used by the eIDAS node and the IdP for ensuring security and privacy in the process.

Figure 4. Authentication flow for a local user.

5. Validation and Results

To validate our proposal, we have implemented and deployed the architecture necessary for achieving compatibility with the specific case of the Spanish eIDAS infrastructure and an attribute provider of UPM. We have also connected this infrastructure with other eIDAS nodes deployed in Portugal, Slovenia, Italy and Austria that also support the proposed extension to provide academic attributes to services.

Furthermore, we have adapted a set of institutional e-services offered by our university (i.e., UPM) to exploit the connection to the eIDAS infrastructure and the new academic attributes. Thanks to this adaptation, students from any of the aforementioned Member States can now access such services using their national eIDs. Moreover, after the authentication, the available academic attributes of the students can be used by the services to enhance their functionalities and hence provide a better user experience. Lastly, we have tested the selected services with a set of Spanish and foreign (i.e., non-Spanish) students.

This section shows the details of the deployment we have carried out, the adapted e-services and the results of the tests with real students.

5.1. Implementation and Deployment

Figure 5 shows how we have replicated the architecture shown in Figure 2 with the following components:

- **Service Providers:** We have deployed a total of four academic e-services and connected them to the Spanish eIDAS node. Details about these services are explained in the following subsection. In order to provide the single-sign-on feature, we have connected a subset of the services to

the eIDAS node through an OAuth 2.0-based Identity Manager compliant with the eIDAS regulation [20].

- **eIDAS node:** We have deployed a testing instance of the Spanish eIDAS node running the new version of the eIDAS node sample implementation that we developed (whose code is available at <https://github.com/eID4U/eIDAS-node>). Therefore, this eIDAS node supports the transport of academic attributes. The node is connected to the eIDAS nodes of Italy, Portugal, Austria and Slovenia so requests sent by SPs for authenticating non-Spanish citizens are redirected to the corresponding foreign eIDAS node. The Spanish eIDAS node also receives authentication requests delegated from foreign eIDAS nodes when a Spanish citizen tries to authenticate to a foreign Service Provider. We have connected the node to an instance of the IdP Proxy that is connected to the official Spanish IdP and to the official UPM's AP. Therefore, real Spanish students' identities and academic attributes are used despite using a testing eIDAS node.
- **Foreign eIDAS nodes:** The eIDAS nodes of Italy, Portugal, Austria and Slovenia are connected to the Spanish eIDAS node. They receive authentication requests delegated from the Spanish node when a non-Spanish citizen tries to authenticate to a Spanish Service Provider. Each of the foreign eIDAS nodes uses a custom mechanism to connect to the foreign IdPs and APs. On the other hand, foreign eIDAS nodes delegate authentication requests to the Spanish eIDAS node when a Spanish citizen tries to authenticate to a foreign Service Provider.
- **IdP Proxy and AP Connector.** We have implemented and deployed an IdP Proxy compliant with the eIDAS specification and SAML 2.0. The IdP Proxy intercepts authentication requests sent from the Spanish eIDAS node to the Spanish IdP for checking the requested attributes. When the IdP authenticates a user and responds to the eIDAS node, the IdP proxy intercepts again the flow for checking the attributes received and calculating the difference with the requested ones. If extra attributes are required, the AP Connector asks the user for consent, including the list of attributes to be requested. Figure 6 shows an example of the consent form shown to the users.

Figure 5. Infrastructure deployment.

EIDAS NODE IS REQUESTING THE FOLLOWING ATTRIBUTES

The following attributes are going to be requested to the ETSIT (UPM Telecommunications School). If you click on next you allow the application to read your personal information.

Personal and academic attributes

- ✓ PlaceOfBirth
- ✓ CountryOfBirth
- ✓ Email
- ✓ Degree
- ✓ FieldOfStudy
- ✓ HomeInstitutionName

CANCEL **NEXT**

Figure 6. Spanish IdP Proxy Consent.

After the acceptance of the consent, the AP Connector sends an HTTP request to the UPM AP. In order to identify a certain student, the AP Connector includes the student hashed eID number in the HTTP requests (using *SHA1*). To secure the HTTP requests when interchanging personal and academic attributes between AP Connectors and APs, the secure version of this protocol (HTTPS) should be used. Some sample requests for personal and academic attributes of a student with eID number 123456789A are the following:

HTTP request for getting personal attributes
<i>GET /apRest/persona.php?token=be472353ac1c55ca42df82c73bd40a8ce8420a28</i>
<i>Host: ap-host.upm.es</i>
HTTP request for getting academic attributes
<i>GET /apRest/academico.php?token=be472353ac1c55ca42df82c73bd40a8ce8420a28</i>
<i>Host: ap-host.upm.es</i>

In our deployment, the AP only accepts requests from registered AP Connectors by means of their IP address and returns a list with all the attributes available for the student. The IdP proxy receives these attributes by means of a JSON object, filters them to select the requested attributes subset and transforms them into the format required for them to be included in the SAML Response. Then, the response is sent back to the Spanish eIDAS node. The IdP Proxy is in charge of decrypting, encrypting, and signing the SAML response to meet the security requirements of the data exchange.

- **UPM Attribute Provider:** It is a web server providing a REST API deployed by UPM, which allows retrieving personal and academic attributes of UPM students. The current version of the UPM AP offers the following personal attributes for a specific student: FamilyName, FirstName, DateOfBirth, CountryOfBirth, PlaceOfBirth, Gender, Email, and PhoneNumber. On the other hand, the AP provides the following academic attributes for a student: Degree, CurrentDegree, HomeInstitutionAddress, HomeInstitutionCountry, HomeInstitutionIdentifier, and HomeInstitutionName.
- **Spanish IdP:** This system authenticates Spanish citizens by means of their national electronic card (DNIE) and provides their MDS attributes. The attributes provided by the IdP have priority over the ones provided by the AP. Therefore, attributes requested by an SP and provided by the IdP will not be requested to the AP.

5.2. Academic e-Services

We have adapted the following four e-services deployed at UPM to allow students to authenticate using their eIDAS-compliant national eIDs, as well as to enhance their functionalities by making use of students' academic attributes. Table 5 summarizes the attributes used by each service.

Table 5. Attributes used by services.

Attribute	Registration portal	ViSH	Moodle	WiFi Access Point
FirstName	×	×	×	×
FamilyName	×	×	×	×
PersonIdentifier				×
DateOfBirth	×	×		×
PlaceOfBirth	×	×	×	
CountryOfBirth		×	×	
Nationality	×			
CurrentAddress	×			
Phone	×			
Email		×		
Gender	×			
CurrentPhoto	×	×		
FieldOfStudy	×	×		
CurrentLevelOfStudy	×			
HomeInstitutionName	×	×	×	×
HomeInstitutionAddress	×			
LanguageProficiency	×			
LanguageCertificates	×			
CurrentDegree	×			
Degree	×			

- Erasmus registration portal:** The UPM Telecommunications School offers an online registration service that helps incoming students and administrative staff working in the international office in the mobility sign-up process. We have adapted this service to support the use of eIDAS-compliant eIDs in addition to the traditional email/password combination for logging in. In both cases, the registration service consists on a set of steps students must follow for filling their personal and academic data. However, in case a student selects the eID option, the personal and academic attributes provided by the eIDAS infrastructure are automatically filled in. The service is available at <https://erasmus-eid4u.dit.upm.es/erasmus>.
- ViSH e-Learning platform:** ViSH [43,44] is a social and collaborative e-Learning platform offered by the UPM that supports the creation, distribution and use of Open Educational Resources (OER). It consists of an OER repository enriched with additional features including authoring tools [45,46], a recommender system [47], a social network, collections, open licensing and integration with Learning Management Systems (LMSs). For logging in to the platform, users had to previously register with an email and password. Thanks to the integration with eIDAS, users have now an alternative authentication method for using their eID, so their user profile is automatically filled in with personal and academic attributes. Therefore, ViSH can provide users with personalized suggestions of OERs based on their user profile immediately after their first access. The service is available at <https://vishub.org>.
- Online courses portal:** This service offered by UPM consists of a web platform built using Moodle (a free open source LMS) that offers courses on different subject matters. In the same manner than in the ViSH service, users had to register in Moodle with an email and password for being able to access it. Thanks to the integration with eIDAS, users can now log in the web portal using their eID so the Moodle user profile is automatically filled with the personal and academic attributes retrieved from the eIDAS infrastructure. The service is available at <https://moodle.vishub.org>.

- **WiFi Access Point:** We have deployed a WiFi access point for enabling incoming students, professors and researchers to obtain WiFi access by means of their eID. Thus, they can log in to the captive portal using their eID instead of other traditional methods such as username/password. Thanks to this integration we can enforce the access based on the personal and academic attributes provided by the eIDAS infrastructure. For instance, in our deployment we only grant access to the WiFi network to UPM students, professors and researchers. We have implemented a captive portal based on the PacketFence (<https://packetfence.org/>) open source tool and taken advantage of its OAuth 2.0 support to connect it to the eIDAS infrastructure thanks to the aforementioned OAuth 2.0 Identity Manager.

5.3. User Evaluation

To evaluate the infrastructure and e-services deployed in the scope of this work, we conducted a survey to gather students' opinions. We aimed to evaluate two main points: (1) whether Spanish UPM students consuming services provided by a foreign university are convinced that the use of their academic profile improves the user experience of such services, and (2) whether the incoming students notice an improvement in the UPM e-services thanks to the integration of their academic attributes in their profiles.

The requirement for accessing the services and then evaluating the proposal was to own a valid and up-to-date eID mechanism of the specific country. In the case of Spanish students, they used their electronic card (DNIE). Foreign students needed to make use of their own country's nationally issued eIDs. For instance, Italian students had to use the SPID (the Italian Public System of Digital Identity).

Before testing the services, students had to answer an initial question inquiring them about the convenience of including their academic profile provided by their national eID when accessing University e-services. Then, they were provided with instructions to consume each service, authenticate using their eID and explore how their digital identity and academic attributes were used for the enrichment of the services. After using the services, they had to answer four additional questions inquiring their opinion on each service and the application of the presented solution in other services and universities.

A total of 42 students volunteered to participate in the study. These students belonged to two different groups: (1) 21 Spanish students who have accessed a set of eIDAS-enabled services provided by the Politecnico di Torino (and also connected to the extended eIDAS infrastructure) with their academic profile provided by the UPM AP, and (2) 21 Italian students who have consumed eIDAS-enabled UPM services which exploit their academic attributes for enhancing their experience.

Table 6 shows the results of the survey for both groups of students (Spanish and Italian). As explained earlier, the first question was answered before testing the services and the answers were clearly positive.

Regarding the services tested and in view of the survey results, we conclude that overall students noticed that the use of our solution for enhancing academic e-services thanks to their academic profiles improves the experience and facilitates the access. This becomes especially apparent in the case of the Erasmus registration service, in which students typically must provide a large amount of information and documents to the international office of the foreign institution. Based on the survey results, it can be concluded that thanks to this solution, students detect a simplification in the registration process.

However, in the case of the remaining university services as well as the WiFi access point, we see a difference in opinions provided by Italian and Spanish students. Several Italian students were not sure whether the integration of the eID authentication improves the ViSH and Moodle services. It is possible that in this case, they would feel more comfortable using their institutional username and password (provided when they are admitted in the university) to access the services, and that the functionalities added thanks to the integration of their academic profiles are not attractive enough to change their minds.

Table 6. Results of the survey.

Question	Spanish Students (N = 21)			Italian Students (N = 21)		
	Yes	No	Not sure	Yes	No	Not sure
1. I think that including my academic profile provided by my national eID when accessing university e-services will improve the usability and the quality of those services.	100 %	0 %	0 %	90.5 %	4.75 %	4.75 %
2. I have used my eID in the eRegistration service (e.g., Erasmus registration) of the university and I think that the possibility of using my citizen eID extended with my academic profile facilitates the registration and improves the user experience.	90.5 %	4.75 %	4.75 %	90.5 %	0 %	9.5 %
3. I have used my eID to log in other university services (e.g., Moodle, online courses, digital library) and I think that the possibility of using my citizen eID extended with my academic profile facilitates the access and improves the user experience.	90.5 %	4.75 %	4.75 %	66.7 %	0 %	33.3 %
4. I have used my eID to connect to the WiFi network through eIDAS and I think this may help me in various environments and services where network access is required.	19.1 %	33.3 %	47.6 %	81 %	9.5 %	9.5 %
5. After testing this pilot, I would like the inclusion of this initiative in the academic services of other European universities.	100 %	0 %	0 %	95.2 %	4.8 %	0 %

On the other hand, we have detected that initiatives such as *eduroam* (education roaming) that provides free WiFi to academic staff (including students, professors and researchers) makes it unnecessary to offer alternative ways of providing wireless connections at universities like the ones proposed in this article. Nevertheless, the global opinion about the initiative was very positive and almost 100% of users would like the inclusion of this initiative in other European universities and academic services. It is also relevant to mention that the small number of users that responded negatively to the initiative prior to performing the test, changed their mind afterwards.

The strict requirements for using the eIDAS infrastructure presently is one of the reasons that justifies the number of students that have tested the deployed pilots. As explained before, for being able to test the services, students need to have an up-to-date eID card. On the other hand, only students interested on coursing their studies in the foreign university were asked to participate in the experiment. However, the validity of the proposed extension, the connection to the attribute providers, and the convenience of including the eID authentication in services to facilitate the students experience and the administration processes have been demonstrated thanks to the performed evaluation.

6. Conclusions and Future Work

This article proposes an extension of the eIDAS specification to support academic attributes. Thanks to this extension, e-services offered by higher education institutions can enhance their features by allowing students' identification through their eID and by exploiting their academic profiles. Furthermore, this extension ensures the veracity of the academic information and saves time in scenarios in which students must provide big amounts of data and documents (e.g., Erasmus students registration processes).

In addition to the definition of new attributes to be included in the eIDAS specification, this work presents an architecture that allows the connection of the eIDAS infrastructure to attribute providers

of authorized institutions. Thanks to this architecture, citizens' eIDAS profiles can be dynamically extended to include attributes provided by third-party institutions of different sectors.

We have included the proposed extension in the Spanish eIDAS infrastructure, which is connected to the eIDAS nodes of other Member States that also support this extension. Moreover, we have deployed an instance of the proposed architecture to connect the eIDAS infrastructure to attribute providers, specifically, to an academic attribute provider of UPM. Finally, we have implemented new features in a set of UPM institutional services, to exploit the use of students' academic profiles to facilitate their use and enhance their features.

We have collected the opinions of a total of 42 Italian and Spanish students who have tested the services deployed by means of a survey. The feedback received was very positive, with more than 95% of the students in favor of including this initiative in the academic services of other European universities.

Once the proposal has been validated, it is important to take into account its limitations. The current status of the eIDAS regulation implies the coordination between all the member states to introduce changes and updates into the reference. Presently, there is not a common approach for managing the inclusion of extra attributes in the eIDAS profile of citizens. As explained before, several projects are being financed for proposing different solutions and the CEF Telecom is discussing the pros and cons of each of them to provide an agreed directive. However, until then, any improvement that implies a modification in the source code of the nodes is not going to be deployed by member states.

Regarding future works, being the proposed solution extensible to other areas, it opens the way to entirely new possibilities for public institutions and private companies to create more robust, secure, and easy-to-use services, not only in the academic sector but also in many others, such as e-health or smart cities. Further research is needed to identify domain-specific attributes that allow adapting the eIDAS specification to meet the requirements of different sectors and to evaluate the convenience of including them in the e-services offered to citizens.

Furthermore, it would be advisable to standardize the way in which attribute providers are connected to eIDAS nodes so as to have a common European framework for all Member States and fields of application. Using attribute mapping services like the one proposed in [48] could definitively facilitate this task. Finally, regarding security, our proposal permits the privacy preservation of the citizens' academic attributes thanks to the encrypted connections and the control they could exercise over them. However, other generic security aspects about the integration of the attribute providers into the eIDAS infrastructure should be analyzed in the future [49,50].

Author Contributions: Conceptualization, Á.A. and A.G.; Funding acquisition, Á.A. and E.B.; Investigation, A.P.; Project administration, Á.A.; Software, A.P., A.G., S.L.-P. and A.M.-A.; Supervision, E.B.; Validation, A.P. and E.B.; Visualization, S.L.-P. and L.M.; Writing—original draft, Á.A. and A.P.; Writing—review & editing, A.G. and S.L.-P. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the CEF Telecom under the action eID4U (2017-EU-IA-0051) with Grant Agreement no INEA/CEF/ICT/A2017/1433625.

Acknowledgments: Authors would like to thank the collaboration of partners from Politecnico di Torino, Universidade de Lisboa, A-SIT, Graz University of Technology and Jozef Stefan Institute in the scope of the CEF Telecom eID4U project.

Conflicts of Interest: The authors declare no conflict of interest.

References and Notes

1. Murrell, S.; Einspruch, N.G. Electronic identification, personal privacy and security in the services sector. In Proceedings of the 2008 International Conference on Service Systems and Service Management, Melbourne, VIC, Australia, 30 June–2 July 2008; pp. 1–7. [\[CrossRef\]](#)
2. Wihlborg, E. Secure electronic identification (eID) in the intersection of politics and technology. *Int. J. Electron. Gov.* **2013**, *6*, 143. [\[CrossRef\]](#)

3. 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. 2014. Available online: <https://eur-lex.europa.eu/eli/reg/2014/910/oj> (accessed on 16 December 2019).
4. CEF Telecom. eIDAS Technical Specifications v 1.2. 2019. Available online: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile> (accessed on 16 December 2019).
5. Alonso, A.; Gordillo, A.; Pozo, A.; López-Pernas, S.; Marco, L.; Barra, E. Extending the eIDAS European Specification for Supporting Academic Attributes. In Proceedings of the 12th International Conference of Education, Research and Innovation (ICERI 2019), Seville, Spain, 11–13 November 2019; pp. 2008–2014.
6. Koulolias, V.; Kountzeris, A.; Leitold, H.; Zwattendorfer, B.; Crespo, A.; Stern, M. STORK e-privacy and security. In Proceedings of the 2011 5th International Conference on Network and System Security, Milan, Italy, 6–8 September 2011; pp. 234–238. [\[CrossRef\]](#)
7. Ribeiro, C.; Leitold, H.; Esposito, S.; Mitzam, D. STORK: A real, heterogeneous, large-scale eID management system. *Int. J. Inf. Secur.* **2018**, *17*, 569–585. [\[CrossRef\]](#)
8. Hernandez-Ardieta, J.L.; Heppe, J.; Carvajal-Vion, J.F. STORK: The European Electronic Identity Interoperability Platform. *IEEE Lat. Am. Trans.* **2010**, *8*, 190–193. [\[CrossRef\]](#)
9. Aavik, G.; Krimmer, R. Integrating Digital Migrants: Solutions for Cross-Border Identification from E-Residency to eIDAS. A Case Study from Estonia. In Proceedings of the International Conference on Electronic Government and the Information Systems Perspective (EGOVIS 2019), Linz, Austria, 26–29 August 2019; pp. 151–163. [\[CrossRef\]](#)
10. Aguilà Vila, J.; Serna-Olivera, J.; Fernández, L.; Medina, M.; Sfakianakis, A. A professional view on ebanking authentication: Challenges and recommendations. In Proceedings of the 2013 9th International Conference on Information Assurance and Security (IAS), Gammarth, Tunisia, 4–6 December 2013; pp. 43–48. [\[CrossRef\]](#)
11. Stasis, A.C.; Demiri, L.; Chaniotaki, E. eIDAS - Electronic Identification for Cross Border eHealth. *Int. J. Reliab. Qual. E-Healthc.* **2018**, *7*, 51–67. [\[CrossRef\]](#)
12. Cantor, S.; Kemp, J.; Philpott, R.; Maler, E. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*; Technical Report; OASIS Standard: Burlington, MA, USA, 2005.
13. Zwattendorfer, B.; Tauber, A. Secure cross-cloud single sign-on (SSO) using eIDs. In Proceedings of the 2012 International Conference for Internet Technology and Secured Transactions, London, UK, 10–12 December 2012; pp. 150–155.
14. Hardt, D. *The OAuth 2.0 Authorization Framework*; Technical Report; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2012.
15. Kaur, G.; Aggarwal, D. A survey paper on social sign-on protocol OAuth 2.0. *J. Eng. Comput. Appl. Sci.* **2013**, *2*, 93–96.
16. Boyd, R. *Getting Started with OAuth 2.0*; O'Reilly Media: Sebastopol, CA, USA, 2012.
17. Leiba, B. OAuth Web Authorization Protocol. *IEEE Internet Comput.* **2012**, *16*, 74–77. [\[CrossRef\]](#)
18. Naik, N.; Jenkins, P. Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect. In Proceedings of the IEEE 11th International Conference on Research Challenges in Information Science (RCIS 2017), Brighton, UK, 10–12 May 2017; pp. 163–174. [\[CrossRef\]](#)
19. Odyurt, U. Evaluation of Single Sign-On Frameworks, as a Flexible Authorization Solution: OAuth 2.0 Authorization Framework. Bachelor's Thesis, Linnaeus University, Växjö, Sweden, 2014.
20. Alonso, A.; Pozo, A.; Choque, J.; Bueno, G.; Salvachua, J.; Diez, L.; Marin, J.; Alonso, P.L.C. An Identity Framework for Providing Access to FIWARE OAuth 2.0-Based Services According to the eIDAS European Regulation. *IEEE Access* **2019**, *7*, 88435–88449. [\[CrossRef\]](#)
21. Morgner, F.; Bastian, P.; Fischlin, M. Attribute-Based Access Control Architectures with the eIDAS Protocols. In *Security Standardisation Research*; Chen, L., McGrew, D., Mitchell, C., Eds.; Springer International Publishing: Cham, Switzerland, 2016; pp. 205–226.
22. Tsakalakakis, N.; Stalla-Bourdillon, S.; O'Hara, K. What's in a name: The conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation. In *Proceedings of the Open Identity Summit 2016: Rome, Italy, 13–14 October 2016*; Hühnlein, D., Roßnagel, H., Schunck, C.H., Talamo, M., Eds.; Gesellschaft für Informatik: Bonn, Germany, 2016; Volume P-264; pp. 167–174. (Please note that this is an amended version

- of the original published (version of record) article. The amendments presented in this version aim to further clarify the points raised about selective disclosure and national unique identifiers).
23. Abraham, A. *Importing National eID Attributes Into a Decentralized IdM System Concept of the Qualified eID Attribute Derivation into a Self-Sovereign Identity System Version 1*; DasE-Government Innovationszentrum ist eine gemeinsame Einrichtung des Bundeskanzleramtes und der TU-Graz: Graz, Austria, 2018.
 24. Tajeddini, K.; Martin, E.; Altinay, L. The importance of human-related factors on service innovation and performance. *Int. J. Hosp. Manag.* **2020**, *85*, 102431. [CrossRef]
 25. Tajeddini, K.; Altinay, L.; Ratten, V. Service innovativeness and the structuring of organizations: The moderating roles of learning orientation and inter-functional coordination. *Int. J. Hosp. Manag.* **2017**, *65*, 100–114. [CrossRef]
 26. Klobučar, T.; Gabrijelčič, D.; Pagon, V. Cross-border e-learning and academic services based on eIDs: Case of Slovenia. In Proceedings of the eChallenges e-2014 Conference Proceedings, Belfast, UK, 29–30 October 2014; pp. 1–9.
 27. Strack, H.; Wefel, S. Challenging eID & eIDAS at University Management. In Proceedings of the Open Identity Summit 2016, Rome, Italy, 13–14 October 2016; pp. 159–165.
 28. Strack, H.; Wefel, S.; Molitor, P.; Räckers, M.; Becker, J.; Dittmann, J.; Altschaffel, R.; Marx Gómez, J.; Brehm, N.; Dieckmann, A. eID & eIDAS at University Management—Chances and Changes for Security & legally Binding in cross boarder Digitalization. In Proceedings of the EUNIS 23rd Annual Congress, Münster, Germany, 7–9 June 2017; pp. 133–142. [CrossRef]
 29. ESMO Project. ESMO_D2.1_Cross-Border Mechanisms Technical Design. 2018. Available online: <http://www.esmo-project.eu/content/esmod21cross-border-mechanisms-technical-design> (accessed on 16 December 2019).
 30. Strack, H.; Otto, O.; Klinner, S.; Schmidt, A. eIDAS eID & eSignature based Service Accounts at University environments for cross boarder/domain access. In *Open Identity Summit 2019*; Roßnagel, H., Wagner, S., Hühnlein, D., Eds.; Gesellschaft für Informatik: Bonn, Germany, 2019; pp. 171–176.
 31. Gerakos, K.; Maliappis, M.; Costopoulou, C.; Ntaliani, M. Electronic Authentication for University Transactions Using eIDAS. In *E-Democracy—Privacy-Preserving, Secure, Intelligent E-Government Services*; Katsikas, S.K., Zorkadis, V., Eds.; Springer International Publishing: Cham, Switzerland 2017; pp. 187–195.
 32. Maliappis, M.; Gerakos, K.; Costopoulou, C.; Ntaliani, M. Authenticated academic services through eIDAS. *Int. J. Electron. Gov.* **2019**, *11*, 386–400, doi:10.1504/IJEG.2019.103721. [CrossRef]
 33. CEF Programme. eID4U (2017-EU-IA-0051). 2017. Available online: <https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2017-eu-ia-0051> (accessed on 22 September 2019).
 34. Berbecaru, D.; Liroy, A. On integration of academic attributes in the eIDAS infrastructure to support cross-border services. In Proceedings of the 2018 22nd International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romani, 10–12 October 2018; pp. 691–696. [CrossRef]
 35. Berbecaru, D.; Liroy, A.; Cameroni, C. Electronic Identification for Universities: Building Cross-Border Services Based on the eIDAS Infrastructure. *Information* **2019**, *10*, 210. [CrossRef]
 36. Berbecaru, D.; Liroy, A.; Cameroni, C. Providing digital identity and academic attributes through European eID infrastructures: Results achieved, limitations, and future steps. *Software Pract. Exp.* **2019**, *49*. [CrossRef]
 37. Klobučar, T. Improving Cross-Border Educational Services with eIDAS. In Proceedings of the World Conference on Information Systems and Technologies (WorldCIST 2019), Galicia, Spain, 16–19 April 2019; pp. 932–938. [CrossRef]
 38. Klobučar, T. Facilitating Access to Cross-Border Learning Services and Environments with eIDAS. In Proceedings of the International Conference on Human-Computer Interaction (HCI 2019), Orlando, FL, USA, 26–31 July 2019; pp. 329–342. [CrossRef]
 39. CEF Telecom. CEF Building Blocks. 2019. Available online: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Building+Blocks> (accessed on 16 December 2019).
 40. CEF Telecom - Marina KIROVA. Overview of Pre-Notified and Notified eID Schemes under eIDAS. 2019. Available online: <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS> (accessed on 16 December 2019).
 41. Bray, T.; Hollander, D.; Layman, A.; Tobin, R.; Thompson, H.S. Namespaces in XML 1.0 (Third Edition). Technical Report, World Wide Web Consortium (W3C). 2009. Available online: <https://www.w3.org/TR/xml-names/> (accessed on 16 December 2019).

42. European Union. Decision No 2241/2004/EC of the European Parliament and of the Council of 15 December 2004 on a Single Community Framework for the Transparency of Qualifications and Competences (Europass). 2004. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32004D2241> (accessed on 16 December 2019).
43. Gordillo, A. Contribution to the Authoring, Distribution, Evaluation and Integration of Learning Objects. Ph.D Thesis, Universidad Politécnica de Madrid, Madrid, Spain, 2017.
44. Barra, E.; Gordillo, A.; Quemada, J. Virtual Science Hub: An Open Source Platform to Enrich Science Teaching. *Int. J. Soc. Educ. Econ. Manag. Eng.* **2014**. [[CrossRef](#)]
45. López-Pernas, S.; Benito, A.; Marco, L.; Gordillo, A. Improval of an educational platform through the integration of an extensible e-learning authoring tool. In Proceedings of the 11th International Conference of Education, Research and Innovation (ICERI 2018), Seville, Spain, 12–14 November 2018; pp. 10117–10124.
46. Gordillo, A.; Barra, E.; Quemada, J. An easy to use open source authoring tool to create effective and reusable learning objects. *Comput. Appl. Eng. Educ.* **2017**, *25*, 188–199. [[CrossRef](#)]
47. Gordillo, A.; Barra, E.; Quemada, J. A hybrid recommendation model for learning object repositories. *IEEE Lat. Am. Trans.* **2017**, *15*, 462–473. [[CrossRef](#)]
48. Lenz, T. Enhancing Cross-border eID Federations by Using a Modular and Flexible Attribute Mapping Service to Meet National Legal and Technical Requirements. *IADIS Int. J. WWW/Internet* **2016**, *13*, 52–68.
49. Morgner, F.; Bastian, P.; Fischlin, M. Securing Transactions with the eIDAS Protocols. In *Proceedings of the International Conference Information Security Theory and Practice (IFIP)*, Heraklion, Greece, 26–27 September 2016; Foresti, S., Lopez, J., Eds.; Springer International Publishing, Cham, Switzerland, 2016; pp. 3–18. [[CrossRef](#)]
50. Kutylowski, M.; Hanzlik, L.; Kluczniak, K. Pseudonymous Signature on eIDAS Token—Implementation Based Privacy Threats. In *Information Security and Privacy*; Liu, J.K., Steinfeld, R., Eds.; Springer International Publishing: Cham, Switzerland, 2016; pp. 467–477.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).