Feasibility Study on Cross-border Use of eID and Authentication Services (eIDAS compliant) to support Student Mobility and Access to Student Services in Europe

FINAL REPORT

A study prepared for the European Commission
DG Communications Networks, Content & Technology
by:

Tenderer

Subcontractor

Digital Single Market

This report was carried out for the European Commission by:

Logo	Company	Authors
	Atos Spain Universitat Jaume I	Vicente Andreu Navarro, Francisco José Aragó, Alberto Crespo, Nuria Rodríguez

Internal identification

Contract number: 30-CE-0823082/00-44

SMART number 2016/0064

DISCLAIMER

By the European Commission, Directorate-General of Communications Networks, Content & Technology.

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

ISBN 978-92-79-80164-8

doi:10.2759/735197

Abstract

This document analyses the feasibility of eID and Authentication Services (eIDAS The Feasibility Study on Cross-border Use of eID and Authentication Services (eIDAS compliant) to support Student Mobility and Access to Student Services in Europe) aims at analysing tertiary education student services in the EU that are accessed through a student e-card or other similar eID solutions. It assesses the technological solutions and standards that are being used to provide access those services and presents a cross-border pilot scenario based on eIDAS compliant solutions.

More specifically, this document assesses the opportunities generated by the eIDAS regulation on services offered by higher education institutions. It also studies possibilities of convergence with already implanted initiatives, such as eduGAIN and other projects dealing with student services and mobility with a focus on identity management and academic information exchange. Regarding eIDAS compliance, a two-level approach is considered: on the one hand, the development of an eID system with full technical interoperability with eIDAS (even as Identity Provider), and on the other hand, the need of a fully legal-compliant system with the potential to become a notified identity provider.

Abstrait

L'étude de faisabilité de services d'identification électronique (eID) et d'authentification (conforme à eIDAS) pour faciliter la mobilité des étudiants, ainsi que l'accès aux services aux étudiants en Europe (*Étude de viabilité à propos de l'utilisation transfrontalier des services d'identité et authentification électronique (conforme au Règlement eIDAS) en soutenant la mobilité des étudiants et l'accès aux services pour étudiants en Europe)* commissionnée par la Commission Européenne a pour but d'analyser les services tertiaires offerts aux étudiants en Europe qui sont accédés au moyen d'une carte électronique ou autres solutions pour valider l'identité électronique. Cette étude évalue les solutions techniques et les standards qui sont utilisés pour fournir l'accès à ces services et présente un scenario de pilote transfrontalier basé sur des solutions conformes à eIDAS.

En particulier, l'analyse présentée dans ce rapport évalue les opportunités générées par le règlement sur les services offerts par les institutions d'études supérieures et les possibilités de convergence avec des initiatives déjà implantées, comme c'est le cas d'eduGAIN, ainsi que d'autres projets traitant de services aux étudiants et mobilité, se centrant sur la gestion de l'identité et l'échange des informations académiques. En ce qui concerne la conformité avec eIDAS, deux approches sont considérées : d'une part, le développement d'un système eID totalement interopérable avec eIDAS (même en tant que fournisseur d'identité) et d'autre part, la nécessité d'avoir un système entièrement conforme d'un point de vue légal avec le potentiel de devenir un fournisseur d'identité qualifié.

Executive Summary

This document analyses the feasibility of eID and Authentication Services (eIDAS The *Feasibility Study on Cross-border Use of eID and Authentication Services (eIDAS compliant) to support Student Mobility and Access to Student Services in Europe)* aims at analysing tertiary education student services in the EU that are accessed through a student e-card or other similar eID solutions. It assesses the technological solutions and standards that are being used to provide access those services and presents a cross-border pilot scenario based on eIDAS compliant solutions.

More specifically, this document assesses the opportunities generated by the eIDAS regulation on services offered by higher education institutions. It also studies possibilities of convergence with already implanted initiatives, such as eduGAIN and other projects dealing with student services and mobility with a focus on identity management and academic information exchange. Regarding eIDAS compliance, a two-level approach is considered: on the one hand, the development of an eID system with full technical interoperability with eIDAS (even as Identity Provider), and on the other hand, the need of a fully legal-compliant system with the potential to become a notified identity provider.

Consequently, **this report proposes a pilot scenario** aiming at filling the gaps detected in identity federation and academic information exchange, based on the background and expertise obtained from the STORK and STORK2.0 academic pilots. The approach implies building an identity system providing a solution not only to the current needs of the Higher Education sector eID ecosystem, where multiple identities for a single individual exist, with different levels of trust, as well as a system of interconnected federations revolving around eduGAIN, but also taking into account the eID compliance constraints. Therefore, one of the major goals within the pilot scenario is the convergence of eIDAS and eduGAIN.

In this context, the most challenging barrier for the adoption of federated services is the multiple existing identities for a student, which can indeed be different depending on the purpose (e.g., for identification against the services and for information retrieval). This multiplicity of identities can be solved by issuing a **single European Student Identity** in line with other European initiatives, such as European Student Card, and by developing methods to trustfully link former identities to this new unique student identity, which would persist and be unique for the student's lifetime. This identity could be issued only once and should be accepted by all European academic institutions.

Despite the fact that there are many different approaches to technically address the requirements stated above, this report proposes a **centralised service** to be operated by a reference entity in the Higher Education sector. This approach solves many of the sustainability and governance issues detected in other initiatives and projects, such as STORK, and which are also noticeable in eIDAS implementation. It must be stressed that the proposed model could be developed within a decentralised system operated by Member States, with information synchronisation mechanisms. But given previous experiences, the legal and administrative barriers, the problematic governance of this network of entities, the different strategies and timelines for deployment and maintenance, it might cause a serious difficulty for adoption and sustainability, reducing sector confidence and increasing development and maintenance costs.

The **proposed Central Identity Service** allows the generation of a single European Student Identity and grants its unicity using multiple and modular mechanisms, being eIDAS authentication the fundamental one that would assign to the new identity the **highest level of assurance** and the only accepted method to create this identity online. It would be similar to the one offered by the in-person registration at academic institutions, which could also be done by the universities involved. The role of eIDAS would not end here, as it would be one of the available alternative authentication methods and thanks to the Domain Specific Attribute interface, eIDAS could act as an Attribute Provider for services. From this point of view, the Central Identity Service is designed to act as a proxy for all the eIDAS functionalities, although adding new ones, especially to converge towards GÉANT.

One of the main characteristics of the proposed pilot is that it is built on top of existent authentication and authorisation mechanisms. Thus, linking the new European Student Identity to other identities is of crucial importance for the engagement of Service Providers and for having a wide base of potential users. This functionality is also provided by the Central Identity Service and can be used either with eIDAS credentials or with a previously created European Student Identity. Different gateways for linking existing identities (for instance, eduGAIN, specific institutional identities…) are available for integration by Service Providers.

The Central Identity Service is expected to constitute an alternate hub for Service Providers to delegate authentication. Any student trying to access a service can be redirected to it in order to be authenticated, independently of the academic institution that runs the service. The student would be able to use any of the available authentication methods, which would be implemented as local authentication methods or gateways to other identity providers or federations.

Finally, the generation of derived identities for specific purposes is also a functionality that can be offered by the Central Identity Service and fills a number of needs demanded either by Service Providers or by students. Examples of these are the generation of a temporary identity when there is no possibility of obtaining the trustable European Student Identity (non-European students applying to a European university), or the need to access a service with identity guarantee but in a risky environment where credentials could be stolen (eduroam temporary credentials, for example).

To sum up, the main characteristic of the proposed infrastructure design for the pilot scenario is flexibility. The following points are functionalities available in a single hub and that can play multiple roles in the identity federation scenario (i.e. bridge between eIDAS and eduGAIN, academic attribute provider hub for eIDAS, identity provider for a diversity of services, etc.):

- Registration of a European Student identity
- Trusted linking of this identity to other eIDs belonging to the same student
- Authentication delegation for Service Providers and provision of attributes
- Identity derivation for particular purposes

Synthèse

L'étude de faisabilité de services d'identification électronique (eID) et d'authentification (conforme à eIDAS) pour faciliter la mobilité des étudiants, ainsi que l'accès aux services aux étudiants en Europe (*Étude de viabilité à propos de l'utilisation transfrontalier des services d'identité et authentification électronique (conforme au Règlement eIDAS) en soutenant la mobilité des étudiants et l'accès aux services pour étudiants en Europe)* commissionnée par la Commission Européenne a pour but d'analyser les services tertiaires offerts aux étudiants en Europe qui sont accédés au moyen d'une carte électronique ou autres solutions pour valider l'identité électronique. Cette étude évalue les solutions techniques et les standards qui sont utilisés pour fournir l'accès à ces services et présente un scenario de pilote transfrontalier basé sur des solutions conformes à eIDAS.

En particulier, l'analyse présentée dans ce rapport évalue les opportunités générées par le règlement sur les services offerts par les institutions d'études supérieures et les possibilités de convergence avec des initiatives déjà implantées, comme c'est le cas d'eduGAIN, ainsi que d'autres projets traitant de services aux étudiants et mobilité, se centrant sur la gestion de l'identité et l'échange des informations académiques. En ce qui concerne la conformité avec eIDAS, deux approches sont considérées : d'une part, le développement d'un système eID totalement interopérable avec eIDAS (même en tant que fournisseur d'identité) et d'autre part, la nécessité d'avoir un système entièrement conforme d'un point de vue légal avec le potentiel de devenir un fournisseur d'identité qualifié.

Par conséquent, ce rapport propose un scenario de pilote qui a pour principal objectif de couvrir les lacunes détectées au niveau du scenario sur la fédération d'identités et l'échange de données académiques et procède de l'expérience acquise à l'occasion des pilotes associés au domaine académique des projets STORK et STORK2.0. L'approche adoptée implique la construction d'un système d'identité qui fournit une solution qui répond non seulement aux exigences de l'écosystème eID du secteur de l'éducation supérieure, où de multiples identités pour un individu coexistent, avec différents niveaux de confiance, ainsi qu'un système de fédérations autour d'eduGAIN interconnectées, mais qui tient compte aussi la conformité à l'eID. C'est pourquoi un des buts principaux du scenario de pilote est la convergence entre eIDAS et eduGAIN.

Dans ce contexte, l'obstacle le plus difficile à surmonter est l'adoption de services fédérés identifiées dans le contexte de la mobilité soient liées au problème des multiples identités qu'un étudiant peut avoir et qui peuvent différer entre-elles. Par exemple, l'identité qui

sert à s'identifier pour accéder aux services ou pour retrouver des informations. Cette multiplicité d'identités peut être résolue en générant une **Identité Européenne d'Etudiant** unique (European Student Identity), solution qui serait d'ailleurs alignée avec d'autres initiatives européennes, comme la Carte Européenne d'Etudiant (European Student Card). Il s'agirait aussi de développer des méthodes pour connecter des identités précédentes à cette identité unique de manière fiable et qui pourrait persister et rester unique tout au long du parcours de l'étudiant.

Bien qu'il y ait différentes approches technologiques possibles pour répondre aux exigences mentionnées ci-dessus, le rapport propose un **service centralisé** qui pourrait être opéré par une organisation de référence dans le secteur de l'enseignement supérieur. Cette approche contribue à résoudre plusieurs problèmes de durabilité et gouvernance détectés pendant le déploiement des pilotes STORK dans le domaine académique et qui sont visible aussi à la mise en œuvre du projet eIDAS. Il est important de remarquer que le même modèle pourrait être développé sous la forme d'un système décentralisé opéré par les Etats Membres, avec des mécanismes de synchronisation de l'information. Mais, sur la base de l'expérience acquise, les barrières légales et administratives, les difficultés de gouverner le réseau d'organisation, les différentes stratégies et planifications, ainsi que pour le déploiement et la maintenance du système pourraient causer de sérieuses difficultés en ce qui concerne l'adoption et la durabilité de cette approche. Il est possible que ces facteurs aient un effet négatif sur la confiance des acteurs du secteur et augmenter les coûts de développement et maintenance.

Le **Service Central d'Identification** (Central Identity Service) proposé permettrait de générer l'Identité Européenne d'Etudiant et d'accorder son unicité en utilisant des mécanismes variés et modulaires ; l'authentification eIDAS serait l'élément fondamental qui pourrait assigner à la nouvelle identité le niveau le plus haut de sécurité (le seul à être accepté pour créer une identité online), similairement à celui offert par les universités participantes. Le rôle d'eIDAS ne serait pas limité à cela, puisque ce serait l'une des méthodes alternatives (celle avec le niveau de sécurité le plus haut). Grâce à l'interface d'attribution spécifique au domaine (Domain Specific Attribute interface), eIDAS serait capable de d'agir comme un fournisseur d'attributs pour les services. Depuis ce point de vue, le Service Central d'Identité serait désigné pour agir comme un proxy pour toutes les fonctionnalités eIDAS, ainsi que d'autres additionnelles, surtout pour converger vers GÉANT.

Une des caractéristiques du système pilote est qu'il pourrait être construit complémentairement aux mécanismes d'authentification et d'autorisation existants. Ainsi, relier la nouvelle Identité Européenne d'Etudiant à d'autres identités revêtirait une

importance cruciale pour l'engagement des Fournisseurs de Service et pour obtenir bonne base d'utilisateurs potentiels. Cette fonctionnalité serait aussi fournie par le Service Central d'Identité et pourrait être utilisée soit avec des certificats eIDAS ou avec une Identité Européenne d'Etudiant créée précédemment. Différentes passerelles pour relier les identités existantes (par exemple, eduGAIN, des identités institutionnelles spécifiques, …) pourraient être disponibles pour être intégrées par des Fournisseurs de Service.

Il est prévu que le Service Central d'Identité constitue un centre pour les Fournisseur de Services afin qu'ils puissent déléguer l'authentification. N'importe quel étudiant qui essayerait d'accéder au service pourrait y être redirigé pour authentification, indépendamment de l'institution académique qui opère le service. L'étudiant serait donc capable d'utiliser n'importe quelle méthode d'authentification disponible qui pourrait être implémentées comme méthodes locales d'authentification ou passerelles vers d'autres fournisseurs d'identité ou des fédérations.

Finalement, la génération d'identités dérivées pour des raisons spécifiques, est aussi une fonctionnalité qui peut être offerte par le Service Central d'Identité. Cela pourrait satisfaire certaines demandes tant du côté des Fournisseurs de Service, comme du côté des étudiants. Par exemple, la nécessité de générer d'une identité temporaire quand il n'y a pas la possibilité d'obtenir une Identité Européenne d'Etudiant fiable (ce qui est le cas pour des étudiants non-européens qui voudraient s'inscrire à une université européenne), ou la nécessité d'accéder à un service avec une identité certifiée, mais dans une situation à risque où les codes d'accès pourraient être dérobés (par exemple, code d'accès temporaire à *eduroam*).

En conclusion, la flexibilité est la principale idée sous-jacente au design de l'infrastructure pour le scénario de pilote proposé. Les points suivants correspondent aux fonctionnalités disponibles dans un centre unique qui joue plusieurs rôles dans le scenario de la fédération d'identités, c'est-à-dire exercer de pont entre eIDAS et eduGAIN, être le centre fournisseur d'attributs académiques pour eIDAS, le fournisseur d'identité pour une diversité de services, etc.):

- Enregistrement d'une Identité Européenne d'Etudiant
- Lien fiable de cette identité avec d'autres eID appartenant au même étudiant
- Délégation du service d'authentification aux Fournisseurs de Service et la provision d'attributs
- Dérivation d'identité pour des exigences particulières

Table of Contents

1. Introduction 15
1.1. Focus and aims of the report 15
2. Conclusions on the state of eID and student services 17
2.1. eID technologies in the context of European higher education 17
2.2. Trends on higher education online services 22
3. Potentials and barriers of a Pan-European eIDAS-compliant eID 25
4. Convergence with eduGAIN and other European initiatives 30
4.1. EduGAIN 30
4.2. Other initiatives: EMREX, Erasmus without Papers, European Student Card. 34
5. Pan-European eID solution Piloting Scenario 36
5.1. Scope and Goals 36
5.2. Scenario Description 40
5.3. Expected Outcomes and Success Criteria 55
5.4. Challenges to address and pilot requirements 57
5.5. Selection criteria 63
5.6. Work packages 65
5.7. Feasibility and proposed planning 67
5.8. Risk assessment 68
5.9. Pilot communication and engagement guidelines 69
5.10. Pilot sustainability guidelines 71
6. Conclusions and Next Steps 76

List of Tables

Table 1: Risk assessment 69
Table 2: Target groups per level of engagement 71

List of Abbreviations

Abbreviation	Explanation
eIDAS	Electronic identification system
eID	Electronic identity
EC	European Commission
EDS	Electronic Diploma Supplement
EU	European Union
HEI	High Education Institution
MOOCS	Massive Open Online Courses
NREN	National Research and Education Network
SAML	Security Assertion Markup Language
SAML2	Security Assertion Markup Language 2
WP	Workpackage

1. INTRODUCTION

1.1. Focus and aims of the report

The specific goal of this document is to "Assess the feasibility of piloting a European-wide eIDAS compliant student e-card or other similar eID solution in the EU". It is the result of WP3 which is focused on "identification of legal, economic and technological barriers that should be considered for the wider adoption of an eID solution for cross-border access to student services. In this report, we will attempt to provide an advanced outline and the set of requirements and recommendations for the definition of a pilot to proof the feasibility of the implantation of an eIDAS compatible European student eID system for the trusted and secure offering of e-services in a cross-border environment. This pilot will address the most poignant needs and gaps in the academic eID scene in order to provide a solution capable of generating enough added value to attract a critical mass of users and institutions.

The report will present the scenarios where the piloting should take place, along with a proposed planning and work organisation distribution, designed over a wide and ambitious frame for future development, fully aligned with the objectives of the EC on education and of the eIDAS regulation. Also, an analysis is provided of the risks and challenges that the pilot execution will probably have to face, both at a technological, legal and organisational level, as well as the measures and technical solutions that should be considered to overcome them successfully, with a focus on future sustainability and adoption.

Based on the outcomes of the WP1 and WP2, this workpackage aims at assessing of implementing a pilot that provide access to cross-border student services in European-using a wide eIDAS compliant card or similar solution. The workpackage will come up with a set of conclusions and recommendations that would boost the progress towards cross-border electronic identification in Europe for the academic services". More detailed information can be found in description of tasks T3.1, T3.2 and T3.3Opportunities generated by the eIDAS regulation.

According to the results of the conducted surveys, most HEIs would appreciate using officially issued identities for the authentication and authorisation on their online services other than having to issue their own corporate identities. The academia sector has had a long time view on the benefits of cross-border services, as proven by the results of the eduGAIN project, but there is a perception on the general lack of services specifically designed to help students in mobility, especially in regard of the

Erasmus programme. This lack may seem strange given the long running and well established experience of identity federations like eduGAIN. But the lack of trust on the identities might be a drawback for the implementation of such services, and here is where eIDAS can be a breakthrough by providing eID with good level of assurance (like official eIDs under eIDAS) that could be very relevant for such cross-border services.

However, survey sample was small and it is more important to consider the outcome from interviews where a majority of NRENS seemed to indicate the preferred solution should be based on current credentials used by HEIs which are compatible with eduGAIN services. However these are usually of a low level of assurance (password-based) and for services that do require a higher level of identity assurance, it was indicated that eIDAS-based solution could be complementary and very beneficial, without replacing current solutions.

The offering of cross-border services is a very valuable asset to help break language barriers to students and staff on mobility, as it allows access to new services with credentials the citizen already possesses and without the need for issuing local credentials, helping on the insertion of the citizen on the destination institution. eIDAS is also a key actor in simplifying administrative work as it can become the trusted and standard mechanism to exchange student attributes, achievements and other academic information, which can only be achieved through a federation based on national eIDs, allowing also to obtain information to allow authorization to access different resources and services at pan-European level.

The main outcomes of this part of the study will consist of:

1. Analysis of any kind of barriers for the wider adoption of a student e-card or other similar eIDAS compliant eID solution for cross-border access to student services. These barriers are considered from different perspectives: legal, economic, technical or semantic and organisational and can be found in Section 3.

2. Identification of the key elements for piloting eIDAS compliant eID solutions providing access to cross-border student services, as described in Section 5.

2. CONCLUSIONS ON THE STATE OF EID AND STUDENT SERVICES

Online services are a crucial asset for research and education nowadays, as they allow the information to be accessible and usable to everyone breaking physical barriers. E-mail, e-learning platforms for teaching, remote conferencing and conference registration and publication, data processing and sharing and bibliographical content access are some examples of the applications of e-services for the research and education field. Despite electronic credentials have simplified life for European students, providing easy and convenient access to both teaching resources and to administrative procedures, each addressed institution requires the user to obtain its institution-specific credentials, generally through a not so convenient procedure. **Enabling easy and convenient access to end users**, in particular students, is a key part of delivering a service, and that's why cross-border access is a natural forward step in the field, as it allows the access to said services to individuals outside of the influence are of an institutions. So, *how must cross-border be understood?* Thanks to the Internet, on-line services in universities can be accessed worldwide, but restricted to be used only by the users owning a credential locally issued by the same institutions, often with the need for in-person registration. The aim of cross-border offering the services is to allow the use of a single identity in services from different universities.

2.1. eID technologies in the context of European higher education

A **high proportion of students actually need an eID solution to access the services** provided by its HEI, both for teaching and for administrative purposes. The most used solution, as excerpted from the former report results, exceeding the 50% of scenarios, is the **user name** and **password authentication**, followed by **digital certificates** in a software support, **one time passwords** and digital certificates on **smartcards**, with comparatively much smaller incidence. Besides this, 66% of institutions support some sort of cross-border authentication, mainly eduroam and eduGAIN. From the user perspective, the report showed that over 90% of students of interviewed HEIs have access to online student services with at least username and password credentials.

The choice of mechanisms depends on a variety of requirements, like it would be the availability of a non-expired eID at the moment a user needs it (especially in non-frequent usage scenarios), the difficulty of remembering the assigned PIN of the identity device, the reluctance to obtain, configure and operate an eID that requires

local configuration at the user's terminal, deployment and distribution costs, and other convenience factors (i.e. mobile eID is usually preferred over smartcards).

User and password, or software OTPs are mature, compatible technologies, easy to integrate, deploy and maintain. They are also the most easy to use by the end user, and the knowledge gap on their side is quite reduced. The bad side is that passwords are prone to threats, especially credential theft. It is the most used one but probably one of the weaker systems from a security point of view.

Software certificates are also a mature technology in most implementations, but with a limited compatibility (not all browsers/operative systems support them well, especially on mobile devices). Moderately easy to integrate, deploy and maintain, the biggest drawbacks are the need for a registration infrastructure more complex than that of the username and password, the expiration that requires periodic visits to the registration point and some user knowledge gap, as it is a more advanced and less intuitive model. On the good side, it is not much prone to threats, as only a violation of the client terminal could end in the private key theft.

Mobile identity (using a registered device via an installed app or through SMS, OTP through this device, either a software on a Smartphone or a specific dedicated hardware device) is a quite mature and compatible technology, moderately easy to integrate deploy and maintain. It presents some user knowledge gap and requires some setup by the end user. It is moderately prone to threats, especially on device violation and theft. Plus, some users may not be able to acquire the needed device if they are not provided by the organisation.

Something similar happens with smartcards and hardware certificate devices. Although a mature technology, it is expensive for moderate to large amounts of users, and the poor standardisation and platform compatibility makes them quite difficult to setup, maintain and operate (they are expensive to scale and require specific technological environment). It also presents to the user a bigger knowledge gap and usability problems than software certificates (more complex for users to configure the needed environment and to remember PINs), but on the other hand, they are fairly secure to threats, although not immune (violation of the client terminal can be used to gain limited access to the key functions, despite not being able to steal the private key).

eID technologies based on RFID are not mature enough, and even less compatible or easy to deploy or integrate than smartcards (although some systems are staring to integrate RFID readers). They are used mostly for restricted environments with

specific terminals (access control to physical facilities). User experience is quite satisfactory, but depending on the RFID technology being used, they are vulnerable to hijacking (through physical proximity or through controlled client terminals) to some degree.

The same issues are present on biometric eID systems. They are expensive as they need specific readers to be deployed (most affordable readers present serious security issues, as the biometric source can be faked). They are poorly integrated, although some devices are starting to include fingerprint readers or face recognition systems through device cameras are being deployed, but they not easy to integrate nor to deploy, and the margin of error is quite high if a minimum level of trust is required, and as always, they are vulnerable to client terminal violations. Again, they are usually deployed in restricted environments.

For the above mentioned reasons, **user and password is still the most used authentication mechanism**. A **majority of online services for students** are **offered with this method** (over 90% are, as shown on the interviews), and virtually all or almost all students can access these services with at least the username and password credentials supplied by the institution, thus eID coverage for access to student services is close to 100% and certainly over 90%. Although the username and password initially looks the most adequate method for its easy deployment and usability, the threats associated are very high as well.

In a few cases, students may use PKI (software or card based) certificates for a limited range of services like printing, but only some HEIs provide this form of authentication to students, as only a minority of existing student services are seen as requiring higher level of assurance credentials. These kind of higher assurances of identity are more commonly deployed for teachers, researchers and administrative staff to access more sensible applications like payroll, student qualifications registration, human resources services, or some specialised NREN services where a security or data breach could have dire consequences.

According to the survey, some HEIs will consider introducing stronger authentication mechanisms for such services in the near future. This special needs have been generally covered with software certificates or smartcards, but in the last twenty years, thanks to the popularity of the mobile phones and lately the Smartphones, OTPs are gaining terrain, either through trusted messaging channels or through registered mobile applications, as mobile identity is also growing fast. Using mobile identity, the most common factors involved in authentication were

password/passphrase, followed by One Time Passwords. The current tendency among HEIs is to deploy OTP or mobile identity as second factor of authentication, although this tendency is still beginning, as slightly less than 20% of HEIs confirmed the combined use of 2 or more factors to authenticate students, but an increase on identity theft incidents or the introduction of more services giving access or managing sensitive academic information may boost this tendency. Among the ones currently using multifactor, 30% of the interviewed institutions used SMS to send the OTP, and 70% generated or sent it through a software method (usually, a mobile application). The usual drawback to the multifactor introduction, besides the usability of the method, is the cost of this second factor of authentication. Smartcards cost is often seen as prohibitive, and even the cost of mobile OTP can be substantial. Contactless solutions are distributed over a variety of physical supports and reader devices, protocols and ciphering algorithms, making it more difficult to decide on a solution to deploy. It offers strong usability for end-users but specific attention on their part needs to be devoted to security measures to minimize threats against the communication channel or the physical embodiment of the solution, which could be a drawback in the end. Despite this, they are becoming increasingly demanded and can complement with mobile identity solutions. Same happens with biometrics, as it can offer good levels of usability, as users are authenticated based on inherent features, but the techniques are quite varied and in some cases, to reach a high rate of recognition accuracy, they require combining a number of modalities (e.g. face with fingerprint). Scalability can be problematic (especially when specialized equipment is required, although mobile devices are starting to include the needed input peripherals), and management can be expensive (in particular enrolment, which requires to ensure the best possible quality of the obtained samples). This can, in the end, result in deployment issues and, depending on the solution, in a non-satisfactory experience for the end-user. The combination of various authentication factors appears to be the most suitable approach. One Time Passwords (OTP) over a costless channel can be a very good system for a second factor of authentication and are thus usually combined with the other authentication methods in order to reduce the impact of attacks aimed against the end-users. They offer an intermediate level of deployment difficulty and end-user usability as well as dynamic possibilities both to generate (based on time, events or challenge response) and deliver the one-time valid token (via SMS, mobile app, HW/SW token, QR-codes).

The most balanced method apart from the username and password would be Mobile identity, due to its relatively good deployment difficulty and cost, and a fair usability degree but with less associated threats. The usability and availability of this method is

directly associated to the fact that HEI students are Digital Natives and most of them own a Smartphone device and are users of mobile-based solutions. This is the reason why this sector is probably the most adequate for this choice of solution. Facilities for other methods, like contactless, OTP and biometrics, are being introduced in mobile devices at a considerable rate, with a better usability and integration results than what was achieved on desktop and laptop devices. The use of multiple factors of authentication is also possible from the mobile, and recommended for student services requiring a higher level of assurance, as new student services are emerging that require stronger trust in the identity of the user, such as access to courses requiring previous enrolment, online exams, academic results or student-initiated processes for mobility between universities. Username and password will not be enough and multi-factor authentication should be seriously considered, combining mobile with OTP, PKI, contactless or biometrics.

Nowadays, **many universities participate in identity federations** to share some of their services and resources with all of the academic community, thus it is shown the perception of the growing importance of eID enabled service access and cross-border eID solutions. According to the research and interviews, SAML is the most common eID standard (> 50% interviewed), followed by kerberos, with growing interest towards OpenID and FIDO. HEIs also perceive official identities as beneficial, so services connected to a cross-border identity federation with official identities (with a higher level of assurance) seems a desirable approach for the sector if their needs are met. Despite all of this, regardless of the method used, the most common scenario is that authentication and authorization are run locally in each HEI, and the common trend across HEIs in all countries is that Erasmus students are given local accounts and credentials to use the online services just like local students instead of trusting a cross-border identity. That is, the majority of the services offered in HEIs are oriented only for local users and require local credentials, even for mobility students. This gives a perspective over the long road still ahead in the field of service federation. But what can be holding back this advance? HEIs are likely to benefit from some of the eIDAS approach to levels of assurance to establish higher levels of multi-party trust in their services and exchanges, opening the door to the offering of new services with more demanding identity assurance needs, and despite they can fulfil the eIDAS requirements in what respects to the enrolment and authentication means aspects of the legislation, it is highly unlikely that a HEI issuing credentials to its students will formally fulfil all requirements established in eIDAS for even level of assurance Low.

Thus, HEIs are starting to look and plan for solutions to address this need for the services that need to control access using an eID of a higher level of assurance. Cross-

border use of national eID (eIDAS) is preferred because HEIs need high level of assurance for some services, especially for enrolment, access to diplomas and online exams, and services that grant access to research sensitive data. An eIDAS-enabled eID would be acceptable as it takes a lot of cost away for doing verifications themselves. This tendency can be observed also in the fact that a number of HEIs opt for outsourcing part of the IAM process. Some countries issue a central identity which is then used to bootstrap local credentials at the institutions, which is enriched by them acting as APs, asserting whether a person is a student, and providing diploma information. This model can be reproduced at a larger scale but backed upon a European student identity. When asked about the different options to deploy such infrastructure, most interviewees didn't consider that a physical electronic student card would be likely to be widely adopted, as complete production and distribution mechanisms would need to be built. Generally the perceived tendency is to do everything on purely electronic basis, which drives us nearer to eduGAIN or eIDAS, as HEIs prefer for supporting student mobility solutions based on credentials they currently issued and Member-State endorsed eID. HEIs offering only distance learning services may have a stronger motivation to use identities with a higher assurance level on authentication and, especially, on the identity registration process. Some interviewee even proposed that government IDs (local and foreign) could be used to bootstrap more trusted eduGAIN credentials.

Adoption of eIDAS by the academic sector would have also an impact on the interest of private sector non-academic legal entities, as they are potential consumers of information. Some services commonly offered to students, such as job selection or job qualification validation, could have value added if interaction with private sector was allowed by eIDAS enabled services. The same thing would be possible in the case of services directly offered by the private sector.

2.2. Trends on higher education online services

The most popular online student services, taken from the institutions that were interviewed, include **virtual teaching** and **access to facilities**, like Wi-Fi or printing. Eduroam, indeed, is a major service, as great numbers of universities provide access to it (twice the affiliation to the EduGAIN federation) and a substantial number of students use it on their home institutions and abroad, providing an overview on the importance of federation. In some countries like Sweden, all web-based services are integrated on a SAML-based identity federation, and have a central system for student admission. Other remarkable services in popularity are the services and products offered with discount price for students.

The use of federated identity is more commonly addressed to access services which are offered or managed through the NREN, like network storage space, videoconference services, rather than to access the local systems of a different HEI. This last trend happens more when referring to the sharing of institutional resources, like research databases or computing grids, which are usually addressed to researchers more than to students.

As the popularity of eduroam proves, university students take the offering of services for granted everywhere, therefore given them access to their welcome university e-services from the very beginning is very relevant for their experience abroad, and through federated services they can have instant access to the commodities from the beginning of their mobility stay, without the need to request a local credential. Also, as STORK 2.0 eAcademia pilot results pointed out, students will be encouraged to use federated services as they are more able to transfer complex academic information through a trusted and automated channel instead of requiring in-person paper appliance.

So, the services with the highest potential for cross border use are the Erasmus programme related services, starting from the application and admission process to virtual campus services as well as accommodation management and basic facilities as network access, welcoming and insertion services like directory services, discounts or access to purchase/reservation of transport titles, meal acquisition/reservation and so on. Access to library, international student mobility services and in general any function of study systems, like virtual learning systems or access to exam qualifications are other examples of services accessed after the mobility term with a high potential for cross-border access. Admission of foreign students is a especially challenging use case, that would largely benefit from eIDAS-based authentication. Some of these services can be quite delicate in terms of a privacy breach or impersonation; that is why providing students with multi-factor authentication solutions when the accessed student services involve procedures where it is of particular importance to minimize the risk of identity fraud. The kind of student services offered by HEIs that would require authentication using a credential with an intermediate/high level of authentication assurance would include the Virtual Learning Environments and MOOCs, online examinations as well as enrolment and admission services, including the booking of admission exams, or the access to diploma information.

As stated above, a **majority of HEIs allow cross-border services**, usually through eduGAIN, but using low level of assurance credentials only. A significant number of

HEIs are yet to integrate with eduGAIN, and eIDAS can become an important actor to improve credential quality as well as for improving cross-border interoperability. New services for which eID-based access would make sense include scholarships, house rentals, printing services, automation of class attendance controls for teachers and students, mobile apps to send notifications and public transport payment system and discounts for students. These new services would cause the facilitation of the administrative work and the improvement of the reputation of the institution due t a simplified and efficient services provision, with the derived management costs lowering and the simplification and friendlier use of authentication processes, especially for foreign students, and would also provide a method to obtain reliable attributes for foreign students. Besides this, it was seen valuable by the interviewees to consider extending HEI business model by offering more courses with the support of eduGAIN.

3. POTENTIALS AND BARRIERS OF A PAN-EUROPEAN EIDAS-COMPLIANT EID

Given the conclusions on the state of student service offering and eID usage, we can state some of the potentials and challenges that a pan-European student eID solution compliant with eIDAS would present.

Governance can be seen as the first challenge. In an environment where Member States have a high level of autonomy and different approaches and legislation regarding eID and education sector management, severe issues should be expected on the setup, maintenance and governance of a student eID system, as was observed on STORK, STORK 2.0 and can be currently seen in eIDAS: different agendas and efforts make it difficult to achieve a common base of service status, and this base usually only covers a basic set of the whole specification. On the other hand, a centralised system approach would be more efficient and easy to govern but will probably face more opposition from the Member States, as it would not be under their own direct control.

At a ***technical level***, several opportunities can be excerpted from the current picture: **different unconnected federations**, or **connected to a low degree of interoperability** with a still **low level of coordination**, while the academic institutions contain big amounts of highly valuable data ready to be exported (securely and under the control of the owner of the information) to offer a wide array of potentially beneficial services. Manual procedures still dominate the landscape for student mobility related processes. They require cross-border exchange of information but still rely on **non-standardised and not-so-reliable manual procedures**, also with the associated high costs in time and personnel that they imply both for the institutions and for the students, due to the lack of an efficient and eID-based procedure with cross-border interoperability (i.e. for the exchange of diploma information, for credit recognition on the home institution or Erasmus registration on the destination institution). To address these potential services, *eIDAS offers a promising alternative* but is hindered by its high-demanding assurance measures and the low demand for high trust credentials, required only for some specific services.

High-trust credentials, like those based on smartcards, present a low demand due to the complex setup process and the operational issues, due to reader or card driver compatibility issues. The **different technologies used by existing federations** are another drawback, requiring a carefully planned interoperability scheme and the generation of auxiliary software modules, usually in the form of bridges. Also, eIDAS is

not flexible enough to quickly support sector specific business processes, especially for private sector, so the sectors will opt for less suitable but more immediate solutions, like eduGAIN would be for the education sector. To this, eIDAS should need to allow the transferring of academic data, at least a reduced dataset like what's offered in eduGAIN.

Due to these reasons, high-trust demanding services are not available, so citizens do not take the effort to obtain the high trust credentials, and since there is not a high credential user base, services needing them are not deployed at the expected rate. If an eID system can be developed to flexibly address the low-trust demanding services and high-trust demanding services, and allowing the end-user to gradually increase his authentication assurance through an array of convenient methods, this eID system could break this vicious circle and increase both the high-trust service offering and the end-user access to high-trust credentials.

Another barrier would be the **low trust on the continuity of the service**, and the level of service offering. A strong compromise on the European authorities and time to convince the stakeholders would be essential. That's another reason to opt for a centralised structure, as **different status of maturity** on the deployment of the **infrastructure** on each member state or the current availability of a reliable production environment doesn't provide the solid image required to gain the stakeholder trust. Some member state operators lack of resources and commitment and lack of communication channels, or even of technical expertise, while a single organisation running this eID system with the proper backing could quickly gain the required trust.

Lack of adequate technical knowledge on the institutions part, together with the **lack of interest** on federated identity or even the **lack of scope** to offer alternatives to their own corporate eIDs is one of the most difficult to overcome barrier. Lack of human or economic resources is a cause, but the key factor is the ignorance about the potential benefits of identity federation and service interoperability, especially the lack of knowledge on the benefits of eIDAS. Potential stakeholders are poorly informed of the existence of eIDAS and its benefits. Besides, the **non-existence of a single point of contact** to start the integration procedure, or a clear specification of said procedure and requirements to connect with eIDAS is another major drawback, aggravated by the fact that these are member state specific and also their own responsibility. So, a factor to be considered would be the integration costs.

Although improving, **poor documentation**, **poor integration facilities** and **support** are a drawback for eIDAS, and similar initiatives, like this would be. There is willingness to adopt, but the lack of a well-known procedure for application to integrate and a plan for integration testing or technical support, especially as it is a member state specific competence keeps eIDAS outside of the private sector agenda. To overcome these barriers, sector specific gateways should be created to channel the information to the potential stakeholders and also to channel their demands to the eIDAS group for their consideration.

To run a pan-European student eID, reference organisations in the sector should be appointed and funded to provide a stronger visibility campaign, offer integration and end-user support and to develop more suitable admission/management processes, adapted for the specific sector organisations (i.e. in HEIs, the NRENs are a good candidate). Also, adaptations of commonly used software for service offerings should be developed to reduce integration costs.

From a ***legal viewpoint***, a barrier could derive from the fact that **local regulations** apply also for foreign students, so there could be a conflict regarding the home country of the citizen and the destination country regarding eID. For example, Finnish law explicitly forbids the use of official eID to proof identity for academic purpose, which can be a problem for a distributed eID approach. Besides, there exist known technical issues regarding the linking of the identity of existing users in institutions to the MS eIDAS identities, as in some countries, identifiers can be opaque and targeted. The most trusted solution to this goes through an in-person identification and identity linking process at each institution, which is not a free and easy process. This **logistic effort** is the main barrier against the introduction of a European student eID, but as it would solve one of the most important barriers for interoperability and gaining access to sector-specific data, this effort would pay off on the long term and stakeholders must be properly informed of this fact in order to secure the needed budget and commitment from the member states to deploy the needed infrastructure to support the process at a large enough scale.

Semantic interoperability of the attributes is another factor to be considered. As learnt from the eduGAIN experience, even at a basic level involving a reduced set of simple attributes, it is difficult for different institutions to have similar criteria on matching their user base data sets to the attributes. The problem grows bigger in the case of different attribute profiles needing translation between them. And this would surely aggravate in the scenario of transferring more complex data sets such as academic records, course or degree information. In this aspect and to minimise

semantic interoperability issues, a reduced set of academic attributes should be developed on top of the eIDAS minimum dataset to represent the main needs on the academic environment services, which should include institution contact and affiliation information, and desirably an extendable entitlement definition and interoperability framework. Any such initiative requires a carefully planned and sustainable governance structure for academic information interoperability, involving the definition of data schemas and semantics.

Another barrier to be considered is the **take-up by students of this eID system**. They need to perceive it as a useful and convenient tool, worth the effort of getting and operating it. Negative factors influencing this include the availability of a non-expired eID, remembering PINs and passwords, personal effort to obtain, configure and operate the eID system (mobile eID is commonly preferred over smartcards), stability over time. Offered services need to provide enough value or save enough effort for the end user to prefer complex eID systems. Availability of academic data, especially in a cross-border environment and compatible across institutions, have access to diplomas or additional services, like those related to work placement. STORK 2.0 eAcademia pilot determined that students will be encouraged to access the services if they can transfer their personal information from all the institutions they have been in to the service provider of their choice. Since this information is retrieved from the education institutions themselves, the main strategy to secure adoption is encouraging the connection of academic data sources preferably through national attribute providers built on a coordinated national programme, but they can also be individually targeted. To achieve this, it is needed that the academic institutes and universities fully buy in to the idea of cross-border mobility of academic attributes and their support by eIDAS specifications (beyond the minimum data set) and that they value the benefit that it offers to the academic community in offering online services with eID access for cross-border use as well as national citizens. Benefit is mutual and very high for all higher education institutions if all or most of them connect their data sources, so the amount of potential users raises and the business benefits are made obvious. The more rich and complex the exported dataset, the more interest it will generate on service providers and on the users themselves, but this needs coordination and commitment at the business sector level.

In short, having a unique identifier, instead of targeted ids, that could be used from system to system would be very helpful for the trusted integration and interoperability of services, but **there are several organisational and legal issues that should be analysed carefully before choosing a technical solution and its scope and design**. Chosen technical solutions should offer more mature integration packages

and be better documented and more prepared for the target institutions; all of this accompanied with support and consultancy services that reach the institutions and encourage them to adopt. At national level, Ministries have a decisive influence, but the image and strategy should be homogeneous across Europe. That's one of the reasons to encourage a centralised solution. Regarding authentication, a second authentication factor should be available in but usability considerations are very important to address when choosing the combination of authentication factors. Mobile identity should be considered.

4. CONVERGENCE WITH EDUGAIN AND OTHER EUROPEAN INITIATIVES

Convergence between electronic identity initiatives is a key factor of success for the spreading of reliable on-line services. There exist several initiatives that deal with student identity management and academic information exchange, come of them well established and popular and others that are currently either in piloting or in steadily growing phase.

4.1. EduGAIN

eIDAS has proven to be an **ambitious initiative** that presents **many benefits** and **opportunities** for the whole European e-services environment, but due to its distributed nature and the security and information authenticity requirements, it is not able to properly cover some sector specific needs. In the academia sector, these are being met by the eduGAIN project inside GÉANT, which has been able to cover the needs starting from the basic ones and with an incremental and open approximation. NRENS maintain their own national identity federations, sometimes with different levels of complexity, and nearly all of them are interconnected through the eduGAIN inter-federation, so the flexibility and complex topologies are a characteristic of such federations, a factor eIDAS shouldn't ignore when engaging. Flexibility and data availability are the keys for the popularity of eduGAIN and its growth potential[1], but at the cost of being able to provide a growing but still reduced common and interoperable data set and present authentication assurance issues that hinder the cross-border deployment of more advanced and sensitive services.

Main barriers for the convergence identified during the previous tasks of this project can be summarized as follows:

- eIDAS specifications are relatively recent, are linked to general administrative purposes and, in many cases, are still not known at academic level.
- eIDAS includes a relatively restricted metadata flow and trust model.
- Academic institutions have a long experience in the development of collaborative solutions that have historically demanded electronic identity management and that do not fit into eIDAS strict guidelines.

Relevance of eduGAIN and other GÉANT initiatives in the academic sector is out of question. Projects suchs as eduroam, which allow university users to access wireless networks spread not only in Europe but also around the world, are popular and well

[1] https://refeds.org/a/1676

known by University's communities. That is the reason that justifies the need of defining the pilot around the convergence with eduGAIN services, putting the focus on an enhanced sectorial data set approved and managed by eIDAs, converging towards international de facto standards like eduPerson.

A future GÉANT-eIDAS pilot should aim at **proving the convenience of using eIDAS identities in providing trust for cross-border authentication of individuals in services** such as the admission and pre-registration of foreign students. This is especially important considering that these two services are traditionally burdensome in terms of time and human resources and a pose a drawback on student applications, especially in case of cross-border mobility, where students can be discouraged to apply by the complexity of the required procedures. Additionally, this scenario aims to generate added value by proving the convenience and variety of advantages for HEIs and students that arise from the exchange of domain-specific (sectorial) attributes.

As stated in the previous deliverables, some NREN experts saw the interviews as an opportunity to send a clear message of the importance of dialogue with eIDAS experts and governance bodies, also recommending that scope of future actions is broadened beyond student mobility to consider as well needs of researchers and other faculty staff. Probably, what they expect is a global solution for electronic identity management and not a specific one for students, as the institutional cost of implementing it partially is close to the cost of a more generalised implementation.

In Portugal, HEIs installing the last provided common plugin for federation, can use the NREN or connect directly to the national system, however, when using the latter for authentication, users lack some of the needed (academic) attributes (and, conversely, when authenticating through the NREN some national eID information is missing). Thus, it seems a convergence between NREN identity services and national and pan-European eID is a well justified option (more on this below). NRENs do confirm that a cross-border ID system is necessary, and it would be optimal if it manages well privacy risks.

In Sweden, experts indicated as one of the big challenges with eIDAS the fact that a global identifier is missing and identity reconciliation (knowing that person identified over eIDAS is the same as a previously registered person by other means) is hard, as is the case when person changes legal name. The intention is to make as good use of eIDAS as possible, but it is seen that eIDAS will never replace the identity federations. These identity federations don't, on the other hand, provide high identity assurance.

As eIDAS is more used and experience grows, improvements will be identified and will need to be addressed. To sum up, Swedish experts expressed that "eIDAS is good for enrolment, eduGAIN for the rest"

HEIs would be enabled to accept eIDAS credentials, it is perceived very strongly that this would be a major initiative to be supported from the NRENs (they are actually doing so already in several cases) in order to maximize cross-border interactions and even that it is a centralized initiative. The support of multiple protocols in this context is important. Use case of eIDAS SPs accepting eduGAIN credentials is much less likely due to the Low LoA of the latter. Government eID is perceived as very good to obtain a standardised set of authentication attributes and eduGAIN is considered as perfect candidate bridge to connect the countries. Thus, NRENs and GÉANT expect that ways to collaborate with eIDAS are promoted and consolidated soon.

It was also perceived as quite useful possibility (although HEIs may not press for it) that of using eIDAS Network as a means to exchange simple academic attributes (i.e. indicating HEI of origin of a student and the fact that the person is an enrolled student) between HEIs in different countries, as long as the student controls the process

The general perception is that synergies can be found: **eduGAIN would benefit from strong and trusted identities, as eIDAs would benefit from the wide user base that the academic world has**. In the short term, the most feasible option seems to **adapt eduGAIN for the use of official eID credentials endorsed by Member States over eIDAS**, this would be the preferred option for strong authentication (as discussed in previous deliverables). A higher degree of assurance would be granted by the combination of eduGAIN and national eID.

The research and education world (eduGAIN) has proven expertise on eID interoperability issues that would allow circumventing certain common failures and a vast number of users that would provide a critical mass of participants. Both aspects, number of potential users and lessons learned and experiences available from the NRENs, must eventually be considered by eIDAS.

This approach is not new. There is some work carried out in GÉANT (eduPEPS[2] which started as collaboration with STORK 2.0 and GN4-2 Task 3.4 Cross Sector Interoperability with eduGAIN[3]). This initiative of GÉANT to converge with eIDAS is

[2] See https://github.com/edugain-stork/edupeps/wiki
[3] See https://wiki.geant.org/display/gn42jra3/T3.4+Cross-sector+interoperability+with+eduGAIN

very relevant as it can pave the way for adaptable interface (Hub) and other convenient services to allow connecting existing sources of academic information to the eIDAS network with minimal adaptation costs. Interoperability between eduPEPS and eIDAS technical specifications (v1.1) is not granted yet, becoming then a necessary step for interoperability envisaged between eIDAS Network and eduGAIN (inter-)federation of academic digital identity federations.

Providing eIDAS identities for the eduGAIN services is important, but what would increase cross-border interoperability at a huge extent and could serve as a test for other fields of public administration, would be the **exchange of sets of attributes** (beyond the eIDAS minimum dataset) that represent academic information. This information could be used in a variety of service providers and would plant the seeds for a trusted, centralised and cross-border academic information transfer. Coordination between GÉANT and eIDAS is mandatory for minimizing the impact on eIDAS Network while maximizing possibilities to enlarge user base and potential benefits of a pan-European cross-border infrastructure.

It is possible, in the academic world, to find organizations which are are already capable of exchanging identity data via SAML assertions using the popular Saml2Int profile. These organizations would not need to develop a specific interface for integrating with their national eIDAS Node (Connector) if a translation service between eIDAS SAML and Saml2Int were offered via a centralised gateway. A hub structure can accommodate for different deployment decisions allowing different countries to implement different topologies, with sector divisions and number of levels depending on their needs or views.

Academic sectorial gateways, acting as single contact points for national eIDAS nodes, could also be designed to be able to connect between themselves using multiple protocols. This possibility would allow for a richer, more flexible and versatile topology.

With preservation of the technological neutrality of eIDAS specifications and infrastructure in mind, national sector-specific hubs can mirror the eIDAS node network topology with a clear goal of proving the strategic benefits that the adoption of such approach by the eIDAS-Network would represent in terms of centralising trust and sector specific data transport. This would put the eIDAS-Network in a strategic position as the provider of a simpler federation network topology, and acting, if so decided, as the mediator on cross-border sectorial interoperability and information

exchange by providing a top-down and more structured approach in organising the interoperability of academic institutions.

The academic world cannot miss the opportunity to become fully aligned with eIDAS. Secure and seamless cross-border electronic transactions depend on the widespread use and uptake of electronic identification and trust services (eIDAS services) by Higher Education sector, but this approach should not enter into conflict or competence with eduGAIN-issued credentials intended for other services in which the level of assurance required is not so demanding. Additionally, this scenario would establish the basis for remaining challenges such as the standardised exchange of the Electronic Diploma Supplement (EDS) and other types of academic information.

4.2. Other initiatives: EMREX, Erasmus without Papers, European Student Card.

The core of EMREX and Erasmus without Papers initiatives is the trusted and user-driven exchange of academic records between HEIs and management of mobility services. Emrex pursues a solution for electronic transfer of student records between HEIs in Europe, currently tested in Denmark, Finland, Italy, Norway and Sweden. Erasmus without paper (EWP) aims to render the administrative workflow of Erasmus paperless by creating a network supporting the electronic exchange of student data and documents by interlinking HEIs and their information systems. The development of data standards and connectors intends to allow an automatic exchange of information.

Both objectives are fully aligned with previous initiatives like STORK2.0, which explored the same scenario. The projects have faced the same challenges in order to grant semantic interoperability and to link the identity between the source and destination institution that were experienced in STORK2.0. On their current application for Erasmus+, both projects plan to develop an integration module with eIDAS to this end, but the pilot proposed in this document would add a wider interoperability layer to provide a trusted link between more identities apart from eIDAS. This last aspect would facilitate integration of Attribute and Service Providers by providing a framework to link local identities to eIDAS identities and, thus, to European Student Identity. Regarding the initiative proposed by European Student Card (ESC), there are some synergies between both projects, but also some differences. The aim of ESC card project is to make the student status recognition possible by all HEI in Europe, so that by presentation of a student's card, a student can assert his / her rights with the HEI that is involved in the project. The card is not necessarily a physical one, but the project provides to HEIs an infrastructure to generate physical cards (and to adapt

existing ones or generate stickers with a QR code and the hologram) besides the generation of the identifier. The proposed identifier is built on a centralised node based on the nationality, the specific institution and personal identifier in the university. This identifier is not unique neither persistent. It has limited validity and registration in two different universities would produce two different identifiers. The model proposed for the pilot in this document could be regarded as an approach that could be run on top of ESC, as it would provide trust by using eIDAS as a trustable source of identity and also, unicity and persistence of the identifiers. Reciprocally, the pilot could benefit from the inputs that ESC could provide for the generation of the identifiers and additionally obtain expertise and guidenace for the planning, development and management of in-person registration procedures at HEIs. Also, the efforts made for dissemination and adoption of the ESC model would be highly beneficial for the pilot as it would contribute to obtain a wider base of potential users through ESC's stakeholders.

5. PAN-EUROPEAN EID SOLUTION PILOTING SCENARIO

During the project, both in the documentation analysis and on the survey and interviews, valuable information has been gathered to create a picture of the current scene on eID use and service offering at the European HEIs. Based on this feedback gained regarding the widespread and commonly used student services accessed by electronic means in the different countries and the proportion of students that access these services per country (WP1); the maturity of use, costs and usage of eID solutions used to access student services (WP2), weaknesses and opportunities have been identified and analysed to design the specifications of a large scale pilot for of eIDAS compliant cross-border electronic authentication to student services in the EU will be drafted.

The proposed pilot will revolve around the **generation of a single European student identity through a European Student Number** (ESN), based fully on **online and not physical card solutions**, as the observations on the preliminary research encouraged to. It will aim to overcome known blind-spots in the academic eID scenario, like the existence of multiple eID federation infrastructures, like eIDAS and eduGAIN, through a decisive step towards eIDAS interoperability with GÉANT. Also, the existence of multiple unrelated identities for a same individual in different institutions (for example, the eIDAS identity and the identity at each visited HEI), with no means for a trusted pairing, will be tackled by the pilot, as it is a demand for advanced interoperability services observed in projects like STORK 2.0. Most research during the last years has led to use domain-based identifiers and not nationally persistent identifiers in HEIs, but there is an increasing demand on raising the level of authentication assurance, which is a clear opportunity for eIDAS through the interoperability this pilot will provide.

5.1. Scope and Goals

The main objective of the pilot will be to develop and implement an eIDAS compliant eID system to allow online identification for academic cross-border student services within the EU. Although the main focus will be on the MS citizens studying in other MS, the pilot will also set the grounds for a more trusted, coordinated registration of non-MS students coming to European HEIs and also for former students, as they are another potential group for this kind of services.

There currently are solutions that allow for a cross-border authentication of students, like eduGAIN, but the implantation of a common European eID solution has many additional advantages. The foremost and most visible one is that eIDAS compatibility

of **HEI identities will provide a high level of trust on cross-border processes**. Current HEI identities offered through eduGAIN suffer from this lack of eIDAS compliance, and that prevents the possibility of implementing cross-border access procedures with higher data protection and identity assurance needs. One of the biggest problems in this higher education environment is the existence of multiple unlinked identities associated to the same person (as an individual may have enrolled in several HEIs, owning an identity on each one of them), which on some processes could present a risk of multiplicity and identity theft or impersonation, which could greatly damage the business process and taint the results.

To solve this multiple identity linking issue, which is a necessary step for trusted cross-border sharing of academic information between institutions, the pilot will develop the **means to deploy a trusted centralised system** where this European student identity will be generated and maintained, allowing for any other existing identity to be associated to the European identity at different levels of trust and through different methods, including eIDAS and eduGAIN identities. This solution based around a centralised identity managed by a trusted European authority will also help overcome legal issues due to national regulations on students and academic sector and on citizen data transfer, observed at large on the documentation and interview phase, as it also was on STORK and STORK 2.0 projects, and will allow for a more flexible while trusted management and cross-border implementation of the business processes in education sector.

As it was identified in STORK 2.0, the poignant need for a trusted link between the different electronic identities associated to a same citizen derives directly from the wide array of potential applications that securely and trustfully exchanging information between different institutions has, and not only on the academia sector. These needs are currently covered by complex manual procedures which require a great deal of time and effort, even monetary, from the student and from the implied HEIs. In an ecosystem with so many institutions keeping valuable data, we have the need to coordinate the delivery of such information under the conditions required by these potential business applications and the security and privacy conditions required by the citizen, to support new and more efficient ways of interaction and evolve towards a more connected Europe.

Despite the apprehension that centralised systems in Europe may cause, the possibility of solving the multiple identity problem shows the need for this solution in this specific case. The **generation and custody of identities in this centralised server** will enable them to be of a higher level of assurance than what's usual in HEIs.

Another advantage of this centralised approach is that the authentication system can be used to serve additional attributes on the academia field, to act as a hub. This can be achieved through a series of interfaces: through eduGAIN, eIDAS or through an internal interface to query attribute providers, which can be used as a means to overcome the issues related to the deployment of the domain-specific attributes module at most MS in eIDAS.

Despite what it may seem, **this pilot doesn't try to override eduGAIN**. In fact, the aim is to **efficiently reuse as many as possible from what's available on the current identity federation environment** and take a big leap towards convergence with GÉANT, taking into account the key role they currently have on the academic sector cross-border service provision scene and including it as a central actor on the development of this pilot.

The pilot will focus on **developing the tools and procedures to allow for a limited scale but representative enough field deployment of the building blocks needed to proof the viability of deploying a European-wide infrastructure of student identities with a modular design to permit a scalable set of identity registration, identity linking, and authentication mechanisms**. The aim is to provide the technical means to deploy this infrastructure at a larger scale after the end of the pilot and identify the barriers and pitfalls of the actual implementation process and provide insight on how to overcome them before the outcomes are adopted and promoted at a larger scale.

To pilot this infrastructure and achieve the necessary mass of users and foster future adoption and sustainability, the most popular services identified during the interviews should be adapted for the pilot. Having in mind the convergence with GÉANT, all of the proposed services should be actual production eduGAIN services. The most promising one would be the in Academia service that allows online stores to check the existence of an affiliation of the principal with a HEI to offer special discounts. This service that currently consumes attributes from eduGAIN, would as well be able to consume them from the central student identity server. Besides this, the HEIs participating in the pilot should propose other services they already have (or that they will be able to build after reaching agreement with local third parties) that would greatly benefit students in mobility, like accommodation, transport cards or other different amenities.

The most important amenity for students in mobility is the **Internet access**, successfully covered by the Eduroam initiative, and also actually the most popular service among students on mobility. To achieve a deep convergence and guarantee

the user mass, the pilot must offer a service in this field, which should be the possibility of deriving a temporary or permanent identity and credentials from the European student identity to be used on eduroam. This offers an added value to the end user as it will allow him to access the service even before registering on the HEI on its first year, or to use stronger credentials usually incompatible with eduroam to gain access to it (for example, an eIDAS identity using a smartcard could derive a temporary identity and password credential to use the Eduroam service). This approach is also beneficial as it would allow reducing the impact of the currently well-known eduroam security weaknesses[4] that expose every user to identity theft through rogue access points. This model provides a good scalability factor that could allow extending the usage of eduroam to other collectives like former students and potentially to all the European citizenry through the eIDAS identities.

The pilot will adopt a progressive strategy at all levels. On the technical design, for an enhanced flexibility, it must allow for additional methods to be plugged-in at all operations: identity registration, authentication and identity linking. All these methods will have an established assurance level so the quality assurance level of each identity will be inferred from the assurance value of the registration/linking and the authentication processes, also allowing these values to escalate in case user is able to provide further proof of linking/identity or a stronger authentication credential (or combination of them). This way, the system can be used to authenticate at different levels of assurance, permitting that eIDAS compliant identities coexist with non-eIDAS compliant ones, and allowing querying only identities of a certain level. This way, the adoption of this system also becomes progressive, as each institution can connect using whichever methods, from all the available ones, fit their needs or their budget at a certain moment. This progressive adoption approach will encourage HEIs to converge towards eIDAS compliant identities and generalise their use.

Finally, despite the focus of this pilot is the higher-education sector, its results will be designed with the clear aim of allowing their extension to other education sectors, like professional training or secondary education; and even to different business sectors that may benefit from the learning and from the technical developments to build similar infrastructures on their own scope. Also, its centralised status, independent from MS management and legislation will set the grounds for a possible extension to non-MS countries, like eduGAIN currently does.

[4] It would provide a well secured RADIUS server, as eduroam's worst security issues are poorly configured institution servers. Also, as they would be credentials for eduroam only, it would overcome the other issue: prevent identity theft, as there exist badly implemented clients (Android systems prior to 7.1, for example, are the worst case, users tend not to do a secure configuration) that would expose the credentials to rogue radius servers.

5.2. Scenario Description

First, we will give an overview of the functionality of the proposed architecture to support the scenarios that will be described at the end. Below, a diagram showing the technical representation of the proposed student identity service can be found. As it can be seen, it includes 5 major modules, representing the main functions of the system: European student Identity registration and credential management, authentication, identity linking, identity management and delegation. Each of them allows the modular connection of a series of interfaces, which can be increased in the future. These interfaces will perform the tasks of service offering, communication with the federated entities and internal module communication, covering different protocols and protocol profiles (like, for example, SAML2-int and SAML2-eIDAS).

The Registration module will allow different methods of registering the European Student Identity with a high level of trust on it representing the citizen requesting it, granting its uniqueness and the citizen's condition as student. The two initially envisioned methods are a method to support the in-person work of registration officials at institutions and a method to allow online registration based on eIDAS authentication and domain specific attributes.

The authentication module will have interfaces supporting different authentication federation protocols (initially, SAML2-int and SAML2-eIDAS, but will be designed in order to easily connect more methods). Internally, the module will support different authentication methods. Some internal (username and password, software certificate) and some delegated ones (eIDAS authentication, eduGAIN authentication). The requesting user will be able to choose the desired identity provider, internal or external.

The delegation module will be in charge of communicating with all the federated sources of identity or academic information, as well as to implement the identity provider interfaces for internal use and the interfaces for external services or federations to use the local authentication methods. This will allow the interoperation with federations like eduGAIN or eIDAS, or with individually connected institutions.

The identity linking module will offer several interfaces and a workflow to allow and manage the request of two identities being considered linked (requested through in-person or online methods and verified by manual or automated means), and also to check if two identities are considered linked and with which assurance level.

The identity management module will implement all the mechanisms to ensure the uniqueness of the identities and to create, delete or alter the identity and credential information with the required level of trust. The inclusion of auditing processes and quality assurance mechanisms in this module could make it possible for the ESI to be compliant and become a notified eIDAS identity. This module will also manage the lower level identities, including the possibility to derive temporal or permanent identities based on the ESI. As an additional feature, this module will be able to mark some derived identities and their credentials as usable by Eduroam, and be synchronized with a Radius server connected to the Eduroam network.

Although the displayed architecture shows a centralised ESI Service, on the design phase it could be turned into a distributed system, by replicating this component on each node of the distributed system, managed by a MS, and implementing identity synchronization and uniqueness mechanisms over the network. The service, attribute and identity providers could be connected to a single node or many of them, depending on the service entry point.

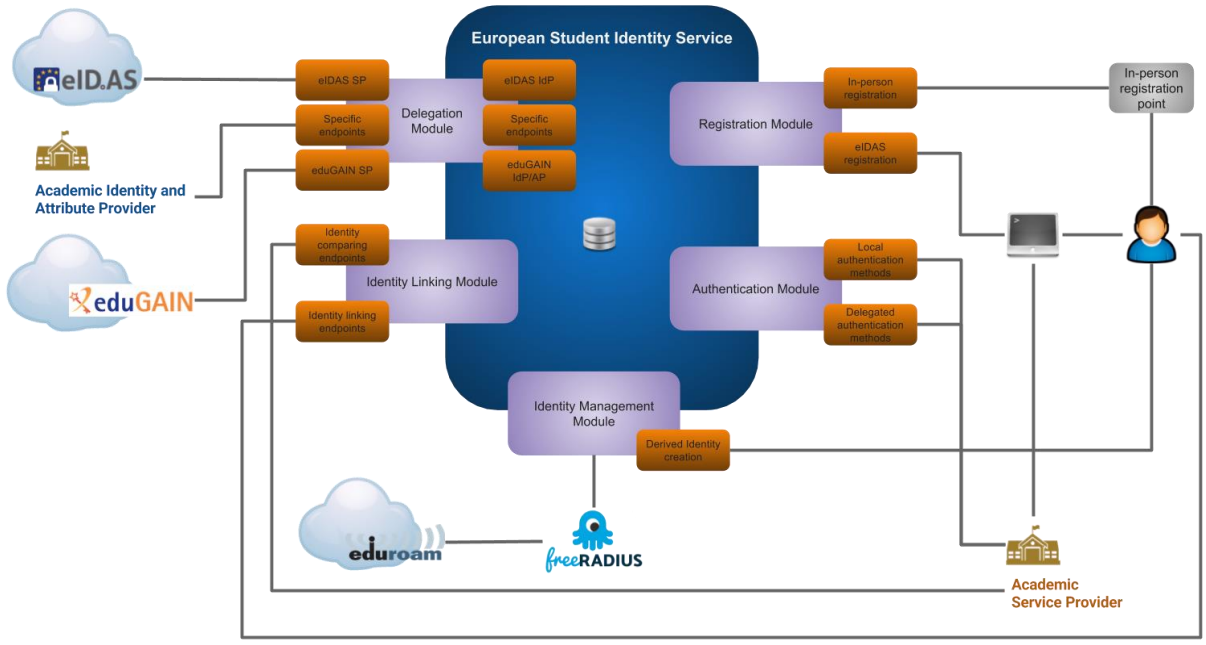

Figure 1: Architecture for a centralised ESI Service

To effectively test the feasibility of deploying a centralised student identity system with authentication and identity linking capabilities and to achieve an effective level of interoperability with GÉANT, the pilot contemplates the following major scenarios:

1. **Identity registration and credential generation with the validation of a trusted third party.**

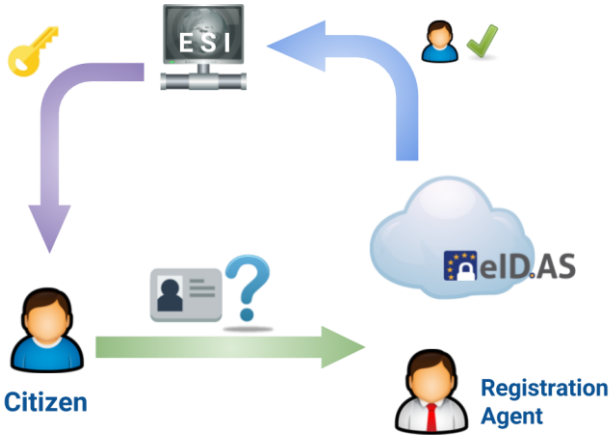

Figure 2: Scenario 1- Identity registration and credential generation with the validation of a trusted third party

In this scenario, an individual who is a student at a participating HEI, will be able to generate his own European student identity, identified by his own and unique European Student Number (ESN). To this purpose, regarding the individual, the central service will need to

- **Acknowledge his own identity.** This can be achieved through different means and designed procedures, which the central system should support in a modular pluggable way. Each method will be awarded a different level of quality assurance, based on the eIDAS requirements, and an individual will be able to perform different acknowledgement methods as soon as they become available to raise the quality assurance level of his own identity, thus, gaining access to services more demanding in terms of identity assurance. This means that, for example, an identity registered through an online method, like the attributes received from an authentication through eIDAS, should have a lesser level than an identity registered through a in-person official ID validation process on an official registering point. And the first identity could promote its quality level if, after registration, it performs the second acknowledgement process.

- **Check if the identity has been registered previously**. As stated above, the individual can go through different registration methods to raise his QAA, thus, different must not be created for the same individual. Automated methods based on the comparison of a subset of personal data (like the name and surname, date of birth, place of birth, etc.) should exist for online registration methods, but an interface for the in-person registration officials to check should exist, with facilities to check suspiciously similar identities and mechanisms to avoid identity duplicity.

- **Acknowledge his condition as student**. On a first phase, this step may not be necessary, as some of the identity acknowledgement methods may not have access to this information. The system would simply not be able to provide the attributes that proof this affiliation for this identity on a HEI. On later steps, after in-person registration is deployed at universities, they will be able to acknowledge such information for their own students. As an alternative method, the connection to academic attribute providers can provide this information on demand in a federated way.

- **Receive his new credentials**. To this end, different means can be used, which can be deployed and performed incrementally to provide different alternative authentication methods, with different levels of strength, to the convenience of the end user (OTP, user and password, mobile identity, software certificate). He will be able to receive any number of credentials of his choice if undergoing the proper registration method (to obtain a mobile identity, he will need to register a device or phone number where the identity will be securely checked). Also, combinations of the credentials can be used to achieve multi-factor authentication and raise the level of quality of the authentication.

Below, you will find an activity diagram representing the described scenario. A practical example of the scenario is provided after it.

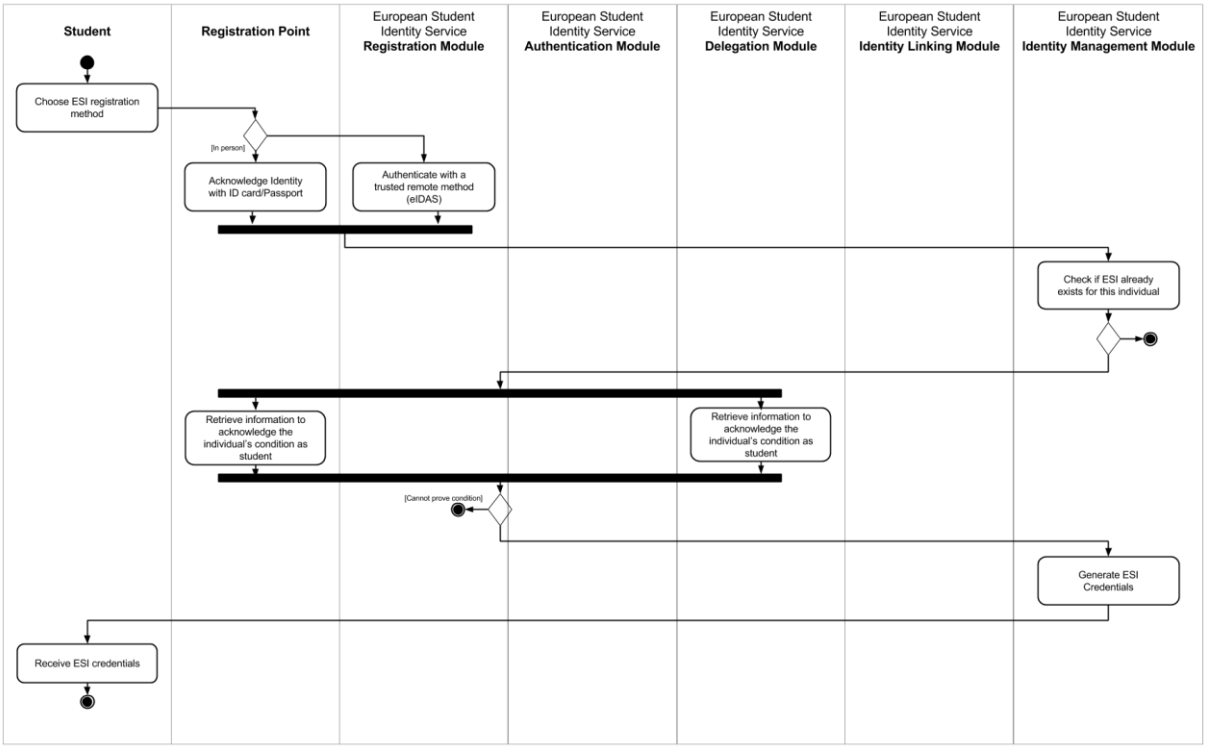

Figure 3: Practical representation of the scenario 1

A Spanish student enrolling for a course in a Swedish university wants to create his European Student Identity so he can access services in his Spanish university and the Swedish university with the same credential. On the university offices, as he is formalising the enrolment and given the university local credentials (he has already proven his identity with his national ID), the official can also generate the ESI and a set of credentials for it (a password or a software certificate) and provide the student with them. Alternatively, the student could have used his Spanish DNIe (electronic ID cryptographic card) to access the ESI service, authenticate on it via eIDAS and request the creation of his ESI.

2. Identity linking with the validation of a trusted third party.

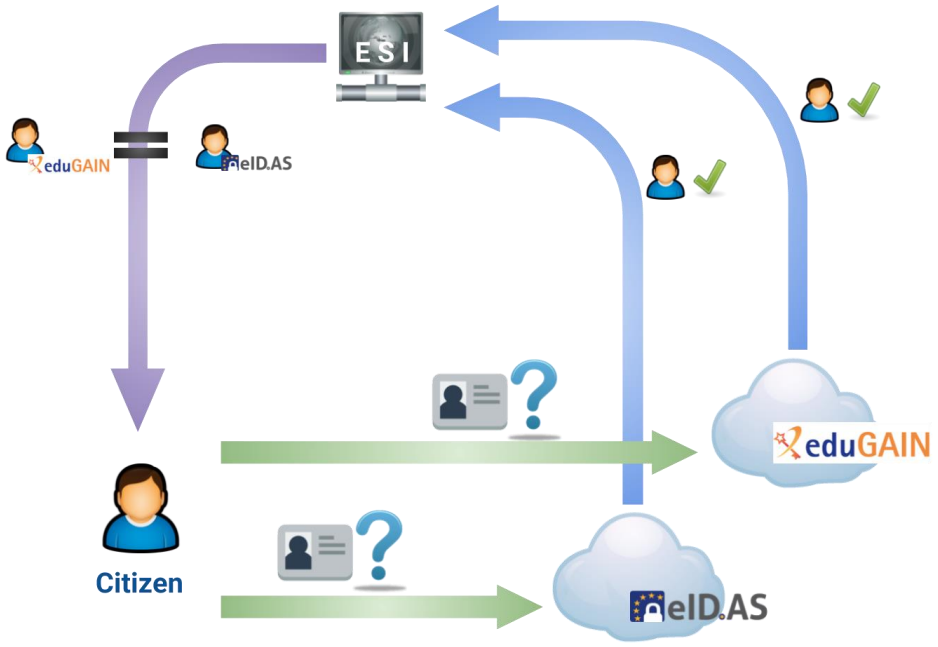

Figure 4: Scenario 2 - Identity linking with the validation of a trusted third party

In this scenario, the individual who registered his European student identity will be able to establish a permanent link with any other identity he may have, like its own MS eIDAS identity, or the local identity at any HEI where the student may be enrolled or had been enrolled in the past. Of course, this link needs to be reviewable and correctable if any errors may had happened, on request by the student on the exercise of his own data protection rights, or by the registrars or the authority auditors, but this process should not be a common one and the user shouldn't be able to easily unlink his identities to minimise fraud or impersonation risk. To this purpose, regarding the individual, the central service will need to

- **Acknowledge the possession of the identity**. The individual will need to authenticate with or acknowledge the identity to be linked in some way trusted by the central service: using a federated authentication through eduGAIN if the HEI is an IdP, on the physical registry point of the involved HEI, where both the identity and its link to the local identity can be checked, etcetera.
- **Acknowledge his own European student identity**. The individual will need to authenticate with or acknowledge the European student identity which the other identity is going to be linked with.
- **Validate that both identities belong to a same individual**. The linking of both identities will only be performed if there is enough proof that they were both issued for the same individual. This can be performed through an in-person verification process at the registry point of the involved HEI, through a semi-automated process, where the individual will electronically or personally provide enough proof of his identity (paper documents, etc.) at a registry point, to be checked by another person on the involved HEI, or through a fully automated process, where a sub-set of his personal data (probably including provided national identifiers, name, family name, date and place of birth, and possibly the parents' names) will be compared with string-comparison algorithms to validate their similarity to an acceptable degree.
- **Register the unique identifier of the linked identity**. Once both identities have been proved belonging to the same individual, the unique persistent identifier (or identifiers) of the identity to be linked will be registered on the central system, along with an institution identifier (that will act as a domain identifier to avoid data collisions), associated to the individual's ESN. Any further association (by this individual or any other) will necessarily have to check that the provided unique persistent identifiers and their domains do not match any other ones already registered in the system. Any mishap will need to be addressed by the authority auditing team.

Below, you will find an activity diagram representing the described scenario. A practical example of the scenario is provided after it.

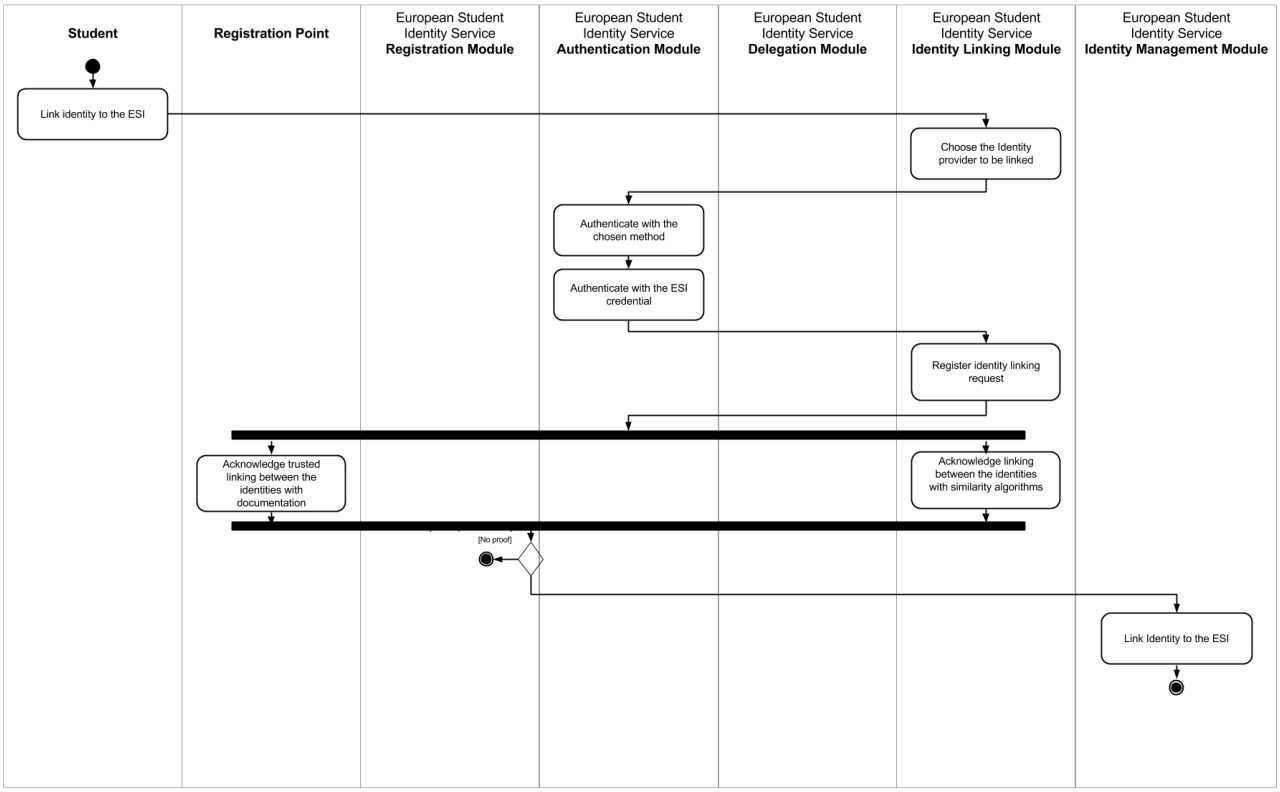

Figure 5: Practical representation of the scenario 2

A Spanish student on a course abroad in a Swedish university wants to link the Swedish university local credentials and the Spanish university local credentials to his ESI. He will go to the registration desk at the Swedish office and, after proving his identity with his Spanish ID and being requested to authenticate on the terminal with the ESI credential, the official will use his privileged interface to link the local university identity with the authenticated ESI credential, not before comparing the provided ID card with the claimed ESI credential information (in fact, as in the previous scenario the user registered his ESI on the desk while being given the university credentials, the official would have performed the linking then by default).

Now, the student wants to link his Spanish university identity to the ESI. As the Spanish university allows remote linking, the student will authenticate on the ESI Service and request to link a credential from the Spanish university. He will be asked to authenticate there and the request will be filed. A set of personal attributes from the ESI and from the university identity will be included on the request to be compared. This set of data will be enough to proof that both identities belong to the same individual. An automated string similarity algorithm will give an approximate estimation of the identity matching, but as the university aspires to a higher link assurance, the filed request is examined online by an official, who will approve or deny it. Once this is done, the Student will be able to access a service with any of the

allowed credentials and, if the identifier is unknown to the service, the service will be able to query the ESI Service to check if the provided identifier matches another one known by the service, like it could be the ESI, to avoid an individual having multiple profiles on the service using different identifiers.

3. Delegated authentication.

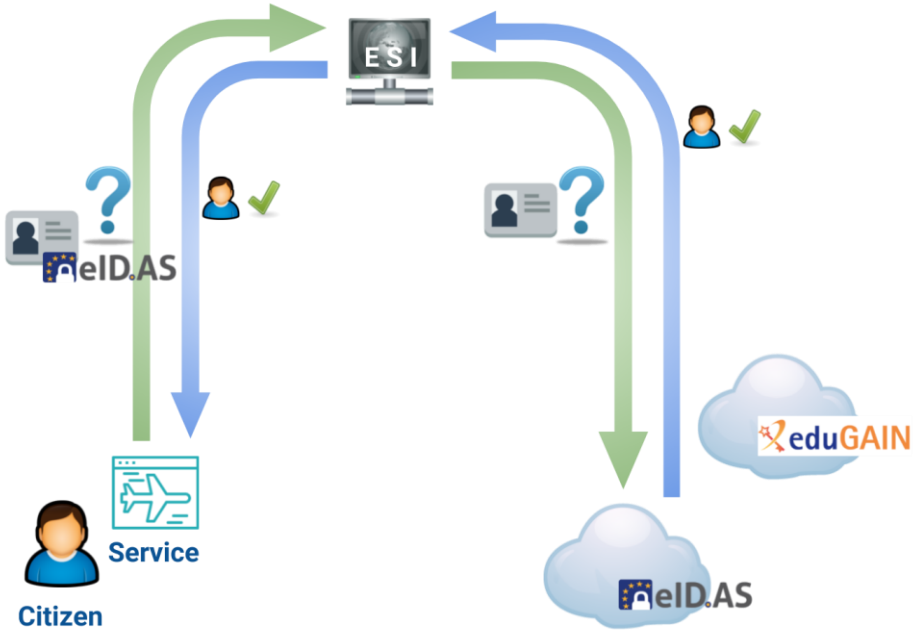

Figure 6: Scenario 3 - Delegated authentication

The individual will be able to connect to different services using to this end the identity and authentication methods registered on the central identity service. To this end, the central identity service will act as a federated identity provider. Different interfaces will be supported, as before, in a modular way. At least a SAML interface to connect with eduGAIN and another SAML interface to connect with eIDAS will be provided. This authentication can be achieved either accessing said networks or a direct connection between the service and the interface can be performed. That is, the ESI Service can act both as a hub between a service and the federations like eIDAS or eduGAIN, or it can act as a IdP for eduGAIN or eIDAS (in the case, the system was able to implement the requirements for its identities to be notified through eIDAS).

- The individual will **access the desired service**. The service will require authentication, offering as one of the possibilities the European student identity central service authenticator (either directly or to be reached through eduGAIN or eIDAS).
- The authentication service will **present all the available authentication methods**, the individual will choose one of them among those he has available.

- The individual will be **challenged to proof his identity**. The challenge will depend on the selected method (which can consist of a combination of methods), say provide his ESN and password, the ownership of a software certificate, a challenge OTP to a registered device or telephone number, etc.
- If the individual succeeds at providing the proof of identity, the central identity service will **generate the corresponding assertion** containing the requested attributes, usually the name, surname, ESN and if available, the attribute marking the affiliation of the individual (student at the beginning, but can be extended to represent former students and other collectives). Many other personal or academic attributes can be retrieved, depending on the needs of the services proposed by the pilot.
- The **authentication assertion will be marked with a quality assurance level**, which will depend on the quality of the registration and the authentication. This way, the service can make an informed decision on whether the identity can be trusted enough.
- The **assertion is returned to the service**, which can decide whether the individual is authenticated or not with the required level of trust.

Below, you will find an activity diagram representing the described scenario. A practical example of the scenario is provided after it.

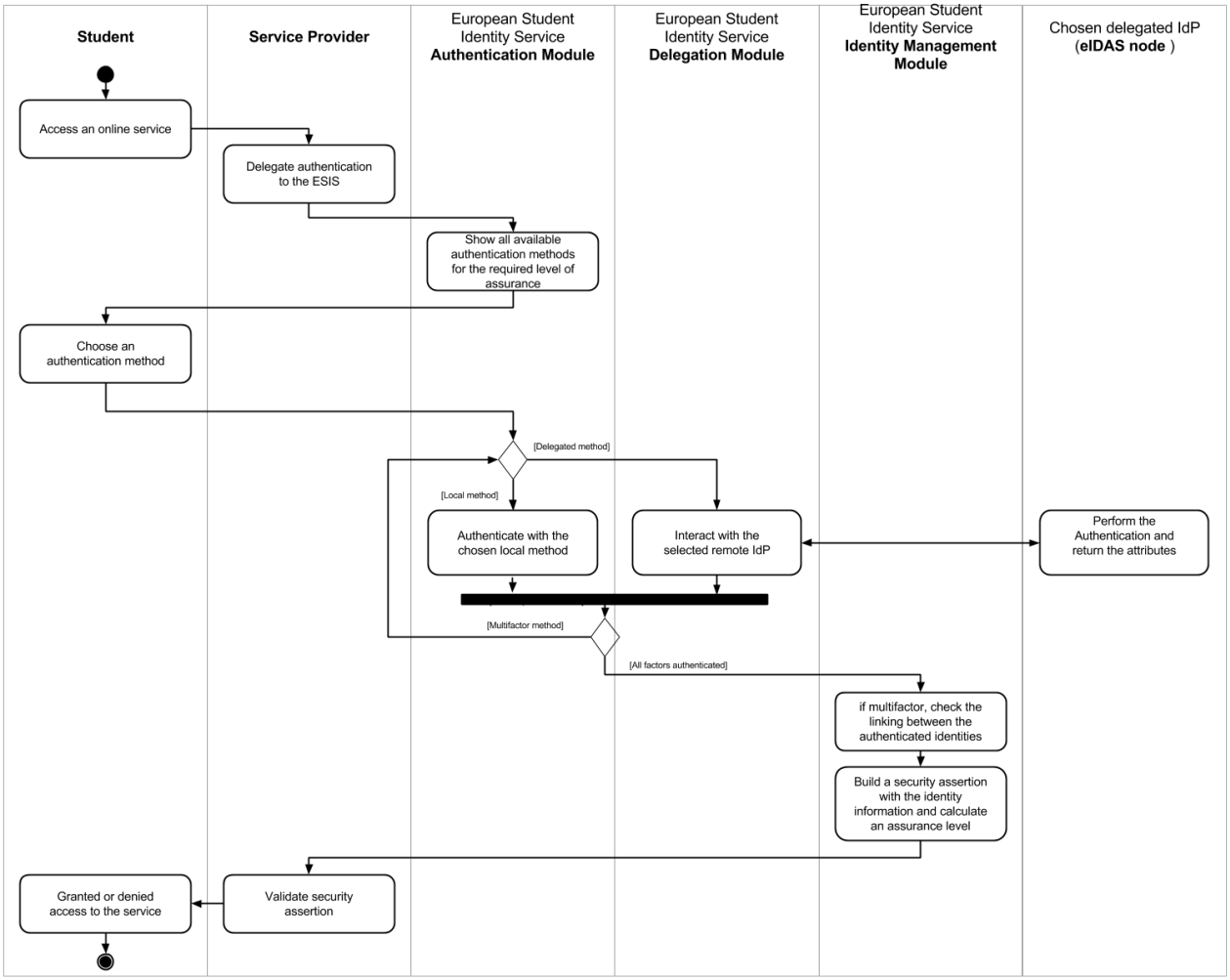

Figure 7: Practical representation of the scenario 3

A Spanish student in a Swedish university wants to access the library resources of a French university using his eIDAS credentials. The French service uses ESI as a gateway to eIDAS, so the French service will ask the ESI authentication service, which will present the user with all the available sources of identity. He will choose eIDAS and a request will be issued. The user will authenticate on the Spanish eIDAS node and the assertion will reach the ESI service, which will then send the authentication information to the French Service which will use it to grant or deny access to the user. On another occasion, the user can't use his eIDAS credential to access the same service, but the university credential is not enough. He can choose to perform a multi-factor authentication at the ESI authentication service, authenticating consecutively with the ESI password credential and the university local credential. This double authentication with two linked identities raises the assurance level of the authentication enough for the French service to allow access to the user.

4. Authorisation through additional academic attributes.

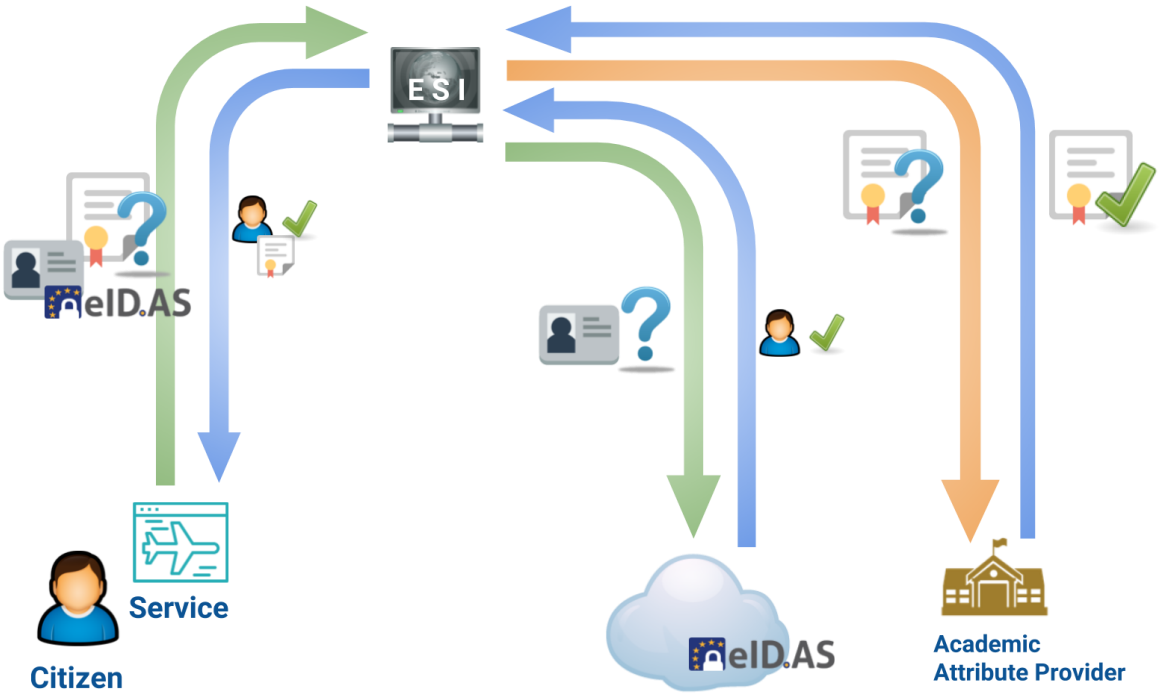

Figure 8: Scenario 4 - Authorisation through additional academic attributes

This scenario is similar to the authentication scenario above. The individual will be able to connect to different services using to this end the identity and authentication methods registered on the central identity service. The end service will also perform an authorisation decision based on the received information. To this end, the central identity service will act as a federated identity provider. Different interfaces will be supported, as before, in a modular way. At least a SAML interface to connect with eduGAIN and another SAML interface to connect with eIDAS will be provided. This authentication can be achieved either accessing said networks or a direct connection between the service and the interface can be performed. The additional academic attributes that will be used for the authorisation process can be retrieved from the central service if registered there, but more likely will be accessed in different attribute providers, which are the real and trusted source of this information and is properly maintained there. It must be noted that when acting as a hub for different attribute providers and being connected through eIDAS, the central service can be used as a sectorial hub for education attribute providers and act as a single attribute provider towards eIDAS.

- The individual will **access the desired service**. The service will require authentication, offering as one of the possibilities the European student identity central service authenticator (either directly or to be reached through eduGAIN or eIDAS).

- The authentication service will **present all available authentication methods**, the individual will choose one of them among those he has available.
- The individual will be **challenged to proof his identity**. The challenge will depend on the selected method (which can consist of a combination of methods), say provide his ESN and password, the ownership of a software certificate, a challenge OTP to a registered device or telephone number, etc.
- If the individual succeeds at providing the proof of identity, the **central identity service will then proceed to ask for the source of the additional attributes** among all those registered attribute providers, using a selector.
- the individual will be **redirected to the attribute provider** where he will authenticate and retrieve the attributes. Depending on the used interface, the attribute provider can also use the central identity service information to authenticate the individual, or will otherwise be required to provide some additional data to proof that both identities are the same (for example, if the identity has been linked, the linked identifier).
- The **identity of the retrieved data will be automatically checked** to prevent impersonation; not in the sense of identity theft, but as one identity transferring some of its attributes to a different identity for the last identity's benefit.
- The central identity service will **generate the corresponding assertion** containing the requested attributes, both the ones from the central identity service and the ones from the attribute provider. This will be delivered to the service to make his decision.
- The attributes will be marked with a piece of metadata indicating **the level of assurance for the data individually**, based on the quality of the identity linking and the quality the same attribute provider awards to each data.
- The **assertion is returned to the service**, which can decide whether the individual is authenticated or not with the required level of trust, as to decide whether each attribute is accepted or not based on its individual quality assurance level.

Below, you will find an activity diagram representing the described scenario. A practical example of the scenario is provided after it.

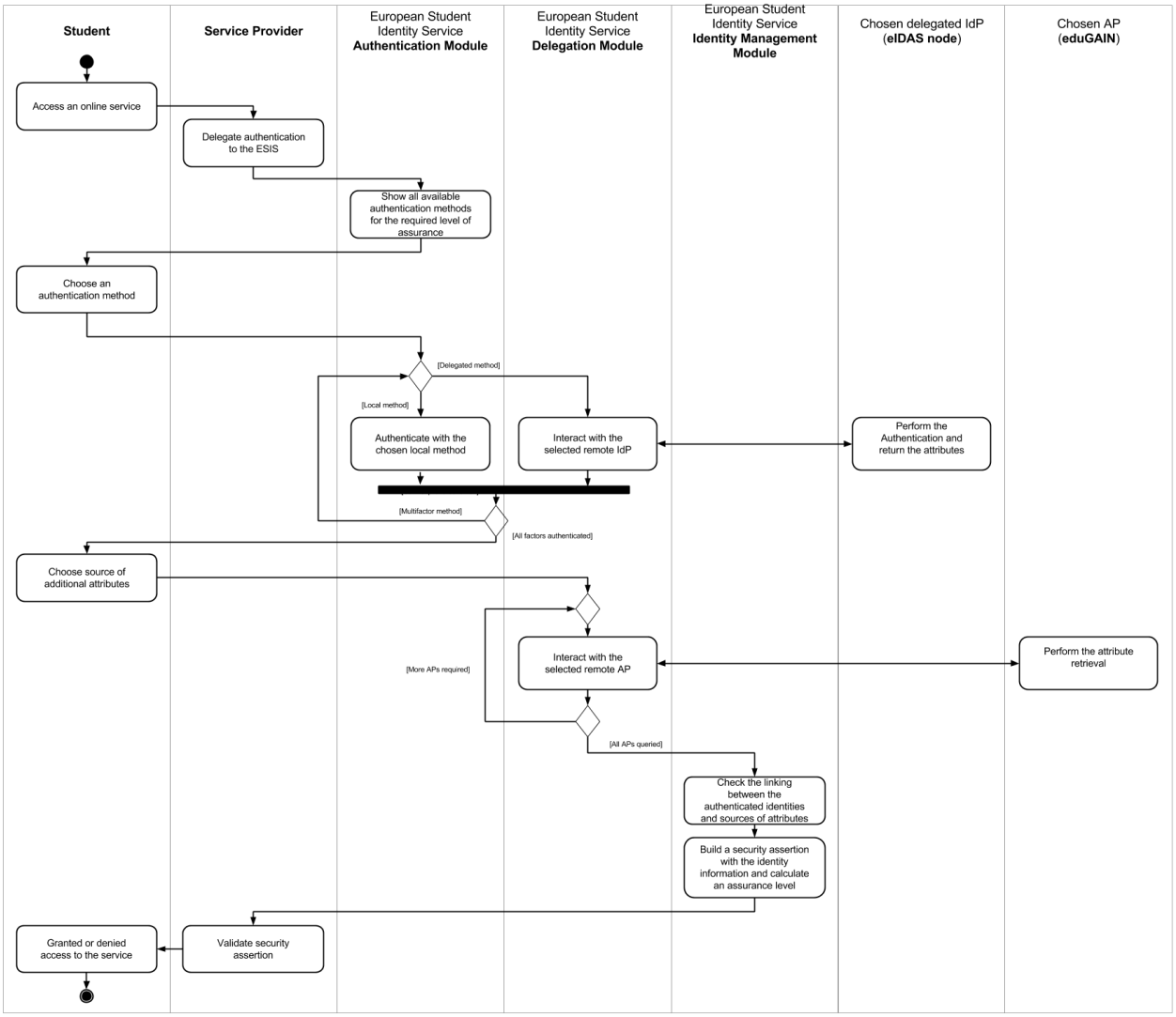

Figure 9: Practical representation of the scenario 4

A Spanish student in a Swedish university wants to access research resources of a French university using his eIDAS credentials, but these resources are only available to those who can proof being students of a university. The French service is connected to ESI, so the French service will ask the ESI authentication service, which will present the user with all the available sources of identity. He will choose eIDAS and a request will be issued. The user will authenticate on the Spanish eIDAS node and the assertion will reach the ESI service. Now, as the French service is requiring additional data (the proof of being a student), the ESI authentication service will prompt the user to choose a source for that information among all the available ones. The user chooses to get that information from his Spanish university through eduGAIN, so a request is issued. The user will authenticate on the Spanish university IdP and the assertion will reach the ESI service. As both eIDAS and Spanish university identities are linked, the ESI service accepts claiming with a reasonable level of assurance that the two

assertions belong to the same individual and the combined information is then sent to the French Service which will use it to grant or deny access to the user.

5. Identity derivation for eduroam access.

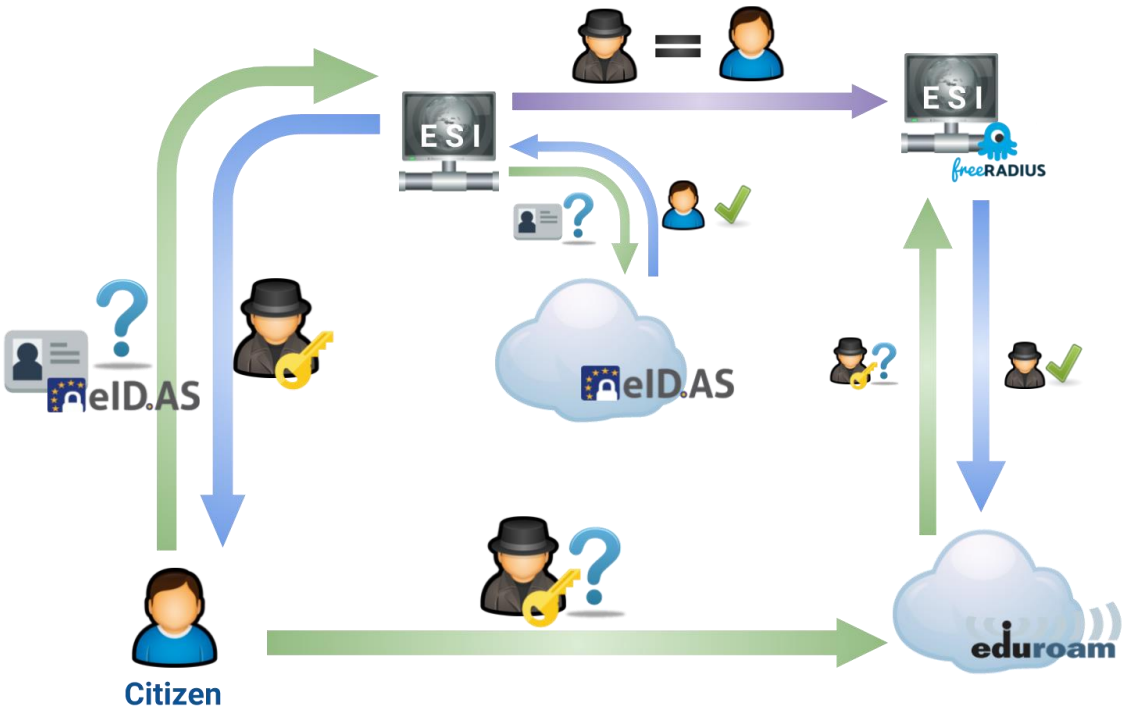

Figure 10: Scenario 5 - Identity derivation for eduroam access

The individual will be able to create a temporary or permanent persistent and opaque identifier with a new set of low-assurance credentials linked to the European student identity. This identity can be used to access services that require lower levels of assurance, need some identity dissociation from the user's side or are less reliable and could be prone to credential theft. Although many potential applications could use this feature, in the context of the pilot it will be used to generate identities and credentials to connect to the eduroam network. To this purpose, regarding the individual, the central service will need to:

- **Authenticate on the central system.** The individual will authenticate using any of the available credentials on the central identity service.
- **Generate the derived identity**. The user will set the lifespan of the identity and an opaque identifier derived from his ESN will be generated and stored in the system.
- **Set the new credentials**. The user will set his password for this new identity.

- **Export credentials on the radius server**. The identifier and the password will be exported by the system to the radius server connected to the eduroam network.
- **Connect to eduroam**. The identifier and its domain will be configured by the individual on the wireless access client, along with the password. The client will check the radius server hierarchy and the authentication challenge will be launched against the European student identity radius server. After validation, the client will be granted connection access with a trusted identity.

Below, you will find an activity diagram representing the described scenario. A practical example of the scenario is provided after it.

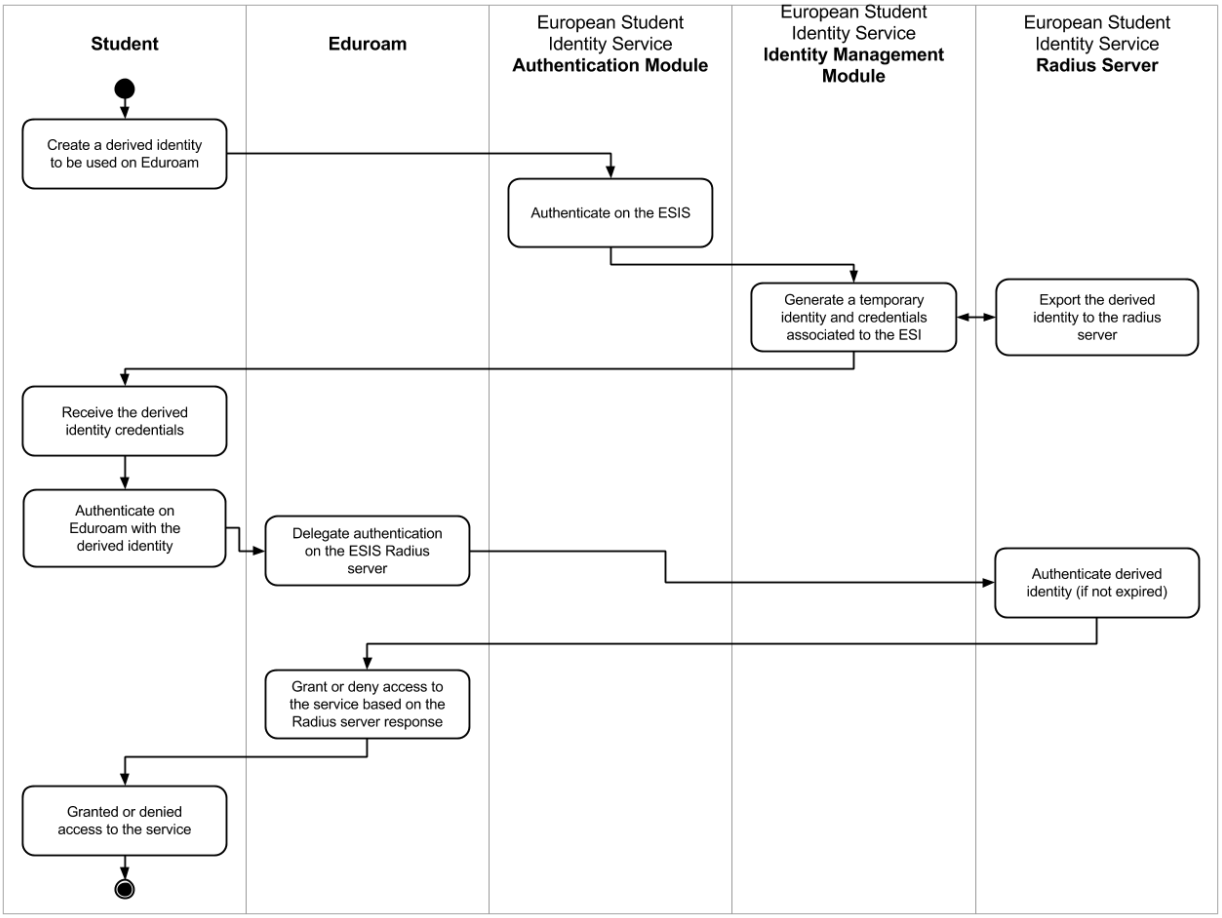

Figure 11: Practical representation of the scenario 5

A Spanish student from a university not connected to Eduroam is visiting a Belgian university which actually offers Eduroam service. As the student owns an eIDAS credential, he can register his own ESI and then access to the Identity derivation module of the ESI service. There, he will create a temporary identifier, with a password credential, and mark it to be used on Eduroam. Then, he will be able to

configure the derived identifier and credential on his terminal and access the Eduroam Service. Internally, this means that on connection of the terminal, the hotspot will send the provided identifier and password to his local Radius server, which will be forwarded to the ESI Radius server and successfully authenticated; after the successful response, the terminal will be granted Internet access.

This same scenario is useful for a student concerned with the security issues of Eduroam, especially over the Android implementation of the wireless connection client, and who fears having his university credentials stolen and being impersonated. To this end, this student will create a derived identity with specific credentials, a limited lifespan, and exclusively for Eduroam use. So, the impact of a credential theft gets minimised to the lifetime of the credential and only for access to the eduroam service.

5.3. Expected Outcomes and Success Criteria

From the implementation of the scenarios described above, several beneficial outcomes are expected for all the stakeholders:

Students will have a **convenient and trusted method of authentication** available, a secure and easy-to-use eID solution for citizens at such a relevant sector as the higher education sector. They will be able to access it quick and easily on the entry levels and on further steps, they will be able to upgrade it to a level of trust which will enable them to access advanced services, using it as a main or as a secondary authentication method in multifactor-authentication demanding services. This identity will also allow them to relate all their existing identities in different institutions, also with their MS eIDAS identity, with the additional trust it provides for procedures involving more than one different institution. This will also enable them to access a wide variety of existing and potential services that will be developed under the trust conditions of this infrastructure. One of the most important one will be the generation of derived identities that will also grant them access to eduroam, solving several trust and security issues and allowing first-time students to acquire eduroam credentials before getting the local credentials at their destination HEI in Europe or elsewhere in the world where an institution supports eduroam.

Former students will also benefit from this pilot, as they will be able to use services which are enabled for their role and especially, achieve the **linking of their identities**. Also, eduroam access could be enabled for users in this profile, which could become a great sustainability measure to achieve a critical mass of users. Also, these kind of users will have the potential access to services like trusted online job qualification verification, job selection with trusted student records as a proof to

register as job seeker, diploma checking and transfer between institutions for credit or diploma recognition.

HEIs will benefit from the possibility of having trusted identities for their students, the possibility to implement stronger authentication and reliable multifactor authentication. Also, the identity linking will allow for more trusted services that will help reduce the over the desk procedures and paperwork, especially for mobility students, and provide a higher level of trust on identity recognition, thus reducing fraud, and human resources needs.

Member states will benefit from the fact that this infrastructure will **open the way for HEIs to become progressively eIDAS compliant**, and will provide a trusted and standardised way of exporting academic information with a considerable trust level, instead of having to develop MS specific solutions which are not interoperable. Multiplicity of identities issues will drop and thus the impersonation risks. This way, the pilot will contribute to accelerating the deployment of eID for cross-border student services, while ensuring coordination between national and EC initiatives in the field and support federated eID management schemes across Europe based on open standard definitions where appropriate, thus allowing for more advanced services to be deployed and converge towards a harmonised and fully interoperable Europe on the higher education sector.

So, after settling on the expected outcomes for the involved stakeholders, we will establish a set of criteria that will indicate whether the execution of the pilot can be considered successful.

First of all, the most important criterion would be that the pilot was executed by a representative set of HEIs from a varied set of Member States. A large number of Member States participating to the pilot is a clear indication of the consensus that could be built as result and of the corresponding interoperability. The selection of universities from different Member States should take into account the different national regulations on students and different eID deployments, to provide a diverse sample enough to face the majority of deployment issues and provide expertise on how to overcome them in the context of the pilot and its future adoption, generating a set of learnt lessons valuable to the European roadmap on eID and freely accessible for any interested stakeholder.

Another criterion will be the impact of the pilot, which can be measured through the number of effective users the service pilot attracts. But it must not be reduced to these numbers, also a qualitative estimation of the number of students in the society

potentially affected by the changes in a positive way, and the frequency of occurrence of the described scenarios in current or potential services will be a good indicator of the adoption potentials. To this end, the services selected to be adapted for the pilot should have a high demand for students in the short and medium term, as are eduroam and inAcademia, the ones we propose as must-haves.

A quick implementation leading to a quick benefit is fundamental for the success of the pilot. That is why we propose a **modular and incremental design** on all the scenarios: simpler methods can be developed and deployed quickly, especially the online methods. These methods also are the ones easier to access and to use by the end user, providing a quick user base that can later escalate when new and more complex methods become available.

But the piloting of services in the proposed scenario is not the only focus for success. The development of a solid and modular infrastructure, based on open source and popular tools to sustain the central service, with a focus on future maintainability and extension of the functionalities is essential. The pilot will be considered successful if the central authority is able to adopt the results and operate them as more institutions attach and create the required service and data provider base. This is not limited to the development, but to the documentation and the development of useful modules and adaptations for common software to facilitate the adoption by these institutions as attribute and service providers.

Finally, the pilot will have to contribute valuable elements on sustainability based on the piloting experience for addressing the **longer-term challenges** around the proposed pan-European governance of an student eID interoperability infrastructure. The pilot will have to provide insights on the approach for visibility and support to encourage institutions to attach, propose a unified member state strategy and involve pan-European actors like GÉANT or TERENA as brokers for the MS acceptance and coordination.

5.4. Challenges to address and pilot requirements

After establishing the goals and the scenarios to be piloted, we must identify which will be the foremost challenges that the pilot will face on the implementation and deployment of the proposed solution, and which requirements, especially at a technical level, this solution should fulfil to achieve the success criteria established earlier.

As described earlier, the European student identity server **must be centralised** to **allow for multiple identity linking**, as it will need to check all the identity creation and linking request and avoid duplicates. This could also be technically achieved with a distributed system, but such architecture would present several issues: from governance issues between the different entities, different deployment and maintenance states with the increased costs and interaction issues, different procedure definition and application given the lack of a central governance authority, but most of all, the operation would be hindered by legal constraints, both involving local legislations and the European General Data Protection Regulation. For example, eIDAS needed to deploy a specific infrastructure to overcome legal constraints in some MS, where they are legally unauthorised to transfer citizen data, internally called middleware countries. This specific infrastructure greatly raises deployment and maintenance costs, as it is needed in each one of the MS (regardless of being middleware countries or not, as they must attend middleware countries' citizens requests). The central design of the European student identity allows avoiding this constraint as the citizen of such countries would voluntarily register his information on this central system, not bound by his MS legislation. Besides, to assure that an identity is not duplicated in a distributed system, the validation of all the nodes should be granted, but as that process needs the transferring of some of the personal information of the citizen, that data transfer should be authorised to each of the involved MS by the end user, giving him the power to duplicate the identity. Another reason for this model emanates from what has been observed on the previous study, as most HEIs won't be able to fulfil the eIDAS requirements for 'substantial' or 'high' assurance level on their eID systems, at least at a shot or medium term. The existence of this centralised and compliant eID system will help overcome this limitation and the modular and incremental design will help institutions move toward eIDAS compliance at upper levels.

As observed in STORK and STORK 2.0, the main challenge of these pilots is to achieve a **critical mass of users and services** that can guarantee the sustainability and expansion of the deployment of the infrastructure on the targeted sector. To this, it is essential to offer services with a quick and easy gain for the end user and then add incremental layers to offer more complex and less-demanded services that wouldn't sustain for themselves but offer a valuable gain when required, and can compensate the deployment costs with the quick-gain services and benefit from the attracted user base that they wouldn't attract initially for themselves. Also, as observed in the interim study, most used eID solutions are considerably weak and can't be eIDAS compatible, whereas more secure solutions have low acceptance and use due to the

knowledge gap, both on the institution and the user, and the effort required for deployment, maintenance and use of said solutions, also for the end user who usually perceives them negatively. That is why all the business processes supported by the central server must be designed modularly and with an incremental trust model. Deploying a eIDAS compliant European student identity infrastructure alone by itself would be pointless, as it would not be able to compete with the existing solutions as each of them currently solves a part of the end user needs, and wouldn't create enough interest to implement the new potential services that would benefit from it. Instead, the pilot needs to create synergies between the existing solutions and try to give solutions for the holes between them, so it can be inserted in the current market and offer an attractive alternative, being these holes mainly the problem of identity linking at different data sources and the increased effort of registering and configuring some of the more reliable authentication methods.

The central server must be designed in a way **multiple authentication methods** can be supported, and new ones added if the demand requires so. One time passwords, mobile identity, user and password, software certificates issuing, federated authentication from any of the linked identities that allow federation... the goal is to offer the user a wide array of authentication methods he can choose, and also to offer the service provider to choose which are the accepted methods and demand a combination of them, in a multi factor authentication schema. Given the user's means and needs at a certain moment, the user must be able to achieve what he needs through the European student identity server at any time. For example, he might only be able to obtain a one-time password credential online at a moment, but use it to access a low-assurance level service, and later be able to obtain a software certificate in person to have access to more demanding services. If the system was simply eIDAS compliant, all the entry level needs would be fulfilled using different existing mechanisms, like eduGAIN or the local credentials at a HEI, and the user base would never acquire the critical mass. This multiplicity of available methods will also help reduce the knowledge gap on end users and encourage them to progress towards upper levels of complexity on their own demand.

For the same reasons as above, the central server must also be designed to allow for **modular and incremental methods of registration and identity linking** (eduGAIN identities, eIDAS identities, in-person registration, in-person registration with remote humane validation). This way, a simple remote credential may be created, based on low assurance methods, to access some entry services, and later other methods can be used to verify the identity of the individual and raise the assurance level of the identity. This entry level design presents an issue: if remote

non-highly trusted identification methods can be used to create an identity and its associated ESN, a same individual may create multiple identities with multiple ESN. Although later validation methods would ensure to take care of this multiplicity, the ESN could have already been used as a single identifier in some systems, damaging the purpose of a single identifier. The pilot must analyse how to address this issue and decide which constraints should be set to achieve equilibrium between user accessibility to the service and multiplicity risk and mitigation needs. For example, it could be decided that the ESN be created only starting from a certain level of assurance and temporary identifiers be issued on lower levels (and later linked to the ESN once it is created). This way, ESN function wouldn't be tainted and low assurance access services could still benefit from the central service. This solution would also link with the tolls that are necessary for the scenario where temporary identities are created for specific purposes like eduroam access.

As explained, ESN identity could be registered only with certain methods (eIDAS, in-person), but a temporary identity could be created with the others (eduGAIN, other HEI specific methods, even social network registration). This process would be the same for identity linking, but in this case, the ESN identity should previously have been created an the linking process will set a unique and permanent relationship between the ESN and the linked identity identifier, in a fashion that an identity will not be able to become linked to two different ESN. The pilot must define which **control and audit mechanisms** should be established to avoid this and to manage possible incidences of foul identity linking, intentional or accidental.

The previously explained **incremental assurance system** will require a mechanism to track this escalation process and define security levels with enough detail, to easily transmit which is the actual assurance level. To this, the pilot will have to define a set of rules to tag each one of the registration, linking and authentication methods, as well as an algorithm to determine the eIDAS compatible QAA level based on the method of registering/validation and the method of authentication used at a certain moment.

The central server will also need to implement an **attribute provider access gateway**. A set of flexible and sector-agnostic services needs to be developed in order to deploy an interoperability infrastructure for HEIs as Attribute Providers. In particular, a common reference implementation, open source-based, of a Where-Are-You-From service for the discovery of academic attribute providers with configurable attribute vocabulary translation and visualization of the academic attributes to obtain consent by the user before their cross-border exchange through eIDAS-Network in

compliance with high data protection standards, can be envisaged. We envisage a model (apt to be replicated in other sectors/domains) focused on scalability towards eIDAS and sectorial governance of trust that hides national complexities enabling to centralize at national level (by means of an academic Hub or gateway eventually managed by the NREN) the discovery of attribute and service providers, the display of sector-specific information to users, multi-protocol interfaces for Service and Attribute Providers and mechanisms for the translation of attribute vocabularies and protocol adaptation; features that the Gateway will implement with the goal of maximising adoption through minimising the integration and interoperability costs of existing services and attribute sources. Given the variety of supported service provider interfaces, this gateway will have the need to present several ways of functioning. The first and most important should be the stateless-hub mode, where the central server will act as a metadata service and discovery service and direct the request to the selected attribute provider, but won't act as a broker for the requests and responses between the SP and the AP, simply redirecting them unchanged. The second mode should be the bridge-hub mode, where besides acting as metadata provider and discovery service, it will provide trust-abstraction by accepting requests and responses and issuing them to the counterpart, but emitted from the bridge (this way, each part only needs to trust the hub). The third mode that should be supported is the eIDAS domain specific interface mode, where besides acting as a bridge, the central server will be able to transmit identity information to the AP so it can authenticate the principal based on this data and its trust to the central server, avoiding double authentication to prevent identity sharing and impersonation. This process should also offer the possibility to selected and query multiple APs in a single flow and return a combined response to the SP. To support these and help detect and prevent impersonations and identity sharing, a similarity of strings comparison service should be developed, to be offered to the service providers, and even integrated on the returned response in the third operation mode. Finally, the pilot should also study the possibility to include a standard interface to query data sources through a backchannel. This way, non-federated data sources could provide attributes based on the individual who authenticated. This last interface should be carefully examined and develop a mechanism on how to overcome the legal implications that this way of transferring personal information presents.

As with the registration and authentication, this versatile but complex system of attribute provision needs a way to tag the quality assurance of every piece of information, given the **increasing number of student mobility scenarios** that will entail the automated exchange of attributes between HEIs and across-borders as well,

in order to establish confidence in the quality and trustworthiness of the information being exchanged. To this end, the **AQAA model developed on the STORK 2.0 project** is key. At a technical level, some improvements should be discussed in order to make it closer to standards and conventions on the field and reduce implementation, integration and maintenance costs, but potentially, every attribute coming from an external AP should be marked with this value for the SP consideration. The value should depend on the quality of the authentication at the AP and the quality of its link with the authenticated individual, besides a base qualification derived from the level of assurance in the acquisition and maintenance of the information (for example, a university issuing a degree is expected to be a trusted source for it). A STORK 2.0 deliverable provided a comprehensive guide to perform this data qualification process and should be used. Deploying this model across the Higher Education community and promoting its adoption will require time and concerted approaches between education authorities at different levels, but this centralised service and the operating entity can act as a mediator and organiser of the process and prevent deviations and lockouts.

From an organisational point of view, the pilot needs to address several important challenges. First of all, the **trust**: all involved HEIs, both as service, attribute or identity providers, or identity registrars, need to have mutual trust. The governance is another challenge, as the sustainability of the pilot will greatly depend on its visibility and expansion strategy, combined with a good and reliable service offering. STORK and STORK 2.0 projects showed the complexities of distributed management of trust and governance. This centralised model is expected to provide lower humane and monetary costs for deployment and maintenance, with lower learning needed, thus reducing the knowledge gap both for the central infrastructure maintainers and for the service providers. Also, better and more efficient governance and sustainability strategies will emerge from a centralised authority. One of the main concerns in the academia sector towards a centralised system would be the trust on the authority running it, but no concerns should be expected if the entity operating the identity server is a renowned organisation excelling on the involved sector and trusted by all HEIs, and the best candidate would be GÉANT itself. As the central authority, it will be tasked with developing and executing the required assurance and auditory procedures, a code of conduct for all involved institution and user roles. The authority will have to determine the procedures involved on, the requirements and the level of assurance for each of the registration, credential issuing and authentication methods implemented on the central server, as well as the related management and organisational procedures associated to keep the level of assurance of the stored identities.

Finally, one of the biggest challenges will be the **economic costs** of generalising this model. The pilot plans to develop a system of registration points. All the administrative work, procedure definition processes and personnel training associated to it can be achieved during the pilot, given its small scale, but the later expansion needs to be carefully considered in order to be successful. That's the main reason to be of the modular and incremental design of the system, and the need for a centralised governance. The central authority will need to design the plan to reach the institutions and the amenities to be provided to foster adoption: training plans, materials and personnel, administrative procedures, economic help, tech and administrative remote support, paid training, provide out-of-the-box workstations for registration points, etc. These measures must be carefully planned and executed based on the available budget. The incremental and modular design will help attract institutions that will connect at the lower levels with the minimal costs and, once they acknowledge the usefulness and convenience of the centralised identity service will develop further engagement and invest in deploying the most advanced features, such as the registration point.

5.5. Selection criteria

We have exposed what the pilot should execute, to which extent and how to determine its success, but among different proposals fulfilling the above mentioned, we must provide some insight on how to choose the proposal with the highest probability of success and learning generation. The pilot should fulfil a number of very important criteria with regard to demonstrating the positive impact of the introduction of this eIDAS-compatible solution into the cross-border student scenario.

First and most important factor would be the **participation of academic institutions from as many different MS as possible**. A large number of Member States participating to the pilot is a clear indication of the consensus that could be built as result and of the corresponding interoperability, as more pitfalls derived from each MS legislation and organisation regarding higher education would arise during the execution and could be tackled at this small scale, with greater flexibility, providing solutions and preparing the way for an easier and simpler large scale deployment afterwards. The selection of universities from different Member States should take into account the input from the previous report regarding the different use of eID solutions for accessing student services in the different Member States, to try to provide the richest and adapted solution for all. Proposals with participating HEIs involved in EduGAIN, other federations, or with identity federation specialists involved in the project (Groningen declaration members, REFEDS members, STORK

participants), should be better considered. In general terms, the applying consortium should not include many ministries or big administrative institutions whose internal organisation could interfere with the development of the pilot. The great majority of it should be composed of research and education institutions, public or private, NRENs, especially if they have an important influence inside GÉANT

The proposal shall specify which **services will be piloted**. High impact services in terms of the number of students potentially affected by the changes in a positive way, and the frequency of occurrence of the scenario should be used to weight the proposal. These "killer applications", as reported in the previous study, should be selected as the purpose of their inclusion is to maximize the benefits of the application of the eID solution in the academic sector. The selected services should be, of course, cross-border services or those with a cross-border potential, and have a high demand for students in the short and medium term. Services must have the need to be accessed with an eID and they should be common services, existent in different institutions across different MS. In previous sections we proposed the integration with eduroam service for this reasons, as well as the integration with inAcademia service. Other proposed services with this same success profile will likely be in the areas of enrolment, application and registration, access to discounts, or amenities like public transport or housing. The best candidates should be quick to implement and preferably provide a quick win, by being not too complex to implement and possibly lead to a series of other quick wins, by extension of their scope.

This same approach should be taken when considering the proposal for the **design and implementation of the central identity service**. Functional coverage should be broad, involving interesting aspects of identity, authentication, authorization, data protection, etc. The proposed authentication, registration and identity linking methods and their design and implementation order are key to determine the success of the system and the connected services from an early stage. The proposal should take into account the input from the previous report regarding the maturity of the eID solutions currently in use in tertiary education in the EU, their recognition for cross-border usage and the main issues found when adopting the solution in the sector. All proposals must include eIDAS integration, both for authentication and for registering, as it is the best entry point in terms of complexity, cost and usability. Also, all the proposals should propose the development and deployment at a limited scale of in-person registration and identity linking methods, along with the sustainability guidelines for its future expansion. The proposal should include a list of the methods that will be implemented to grant the uniqueness of the link between a ESN and an external identity, and to prevent multiplicity in ESN registration for a same individual.

Besides, although the main focus are the European students, proposals exposing how this model could be extended to facilitate the inclusion and access to services to non-European and former students, should be better considered. Another strong point would be if the proposal includes the development of an app for mobile identity, as it is one of the main observed trends on the former report and opens the door to further functionalities.

Finally, the proposal should explain how it plans to contribute **valuable elements to the vision on sustainability for addressing the longer-term challenges around permanent pan-European governance** of this eID infrastructure interoperability and the eID interoperability scenario in Europe in general, beyond the technical hurdles and with an insight into the business perspectives to cross-border eID potentials and adoption and their associated long-standing barriers, with a focus on expansion strategy and governance.

5.6. Work packages

Although the proposals will include their own work distribution structures, we will provide some guidelines on what should be expected for a proper and efficient execution.

A **coordination** work package is essential, as there is a permanent need for supervision of the tasks being executed and a dedicated and expert guidance on the non-technical or design aspects of the project. It will also contribute to create synergies between the different work groups and facilitate communication among them. It will also help in keeping the internal organisation of each of the work packages.

Another work package should be devoted to studying the **legal, technical and administrative implications of the proposed design**, to ensure eIDAS compliance, pilot requirement compliance and thus ensure the viability of building and operating this centralised eID system. The design of the procedures and measures for deploying and maintaining in-person registration spots in HEIs, and ensuring the eIDAS compliance of the issued identities should be a task for this work package too, including how to keep the security standards on the verification of the identity, registration of data and its maintenance on the server; define the required personnel training standards, the measures to secure the workstation deployment, the model to issue registrar high level identities, and all the related work specific to this end. Also, the model of deployment on each MS should be discussed and determined (either if there should be country specific structures or just a centralised coordination and point

of application for all HEIs). Guides on the qualification of data assurance level and with recommendations on procedures and security measures for granting the quality of identities and determining the levels based on the previously described parameters should be developed and submitted for discussion by the eIDAS technical subgroup. This would allow a better alignment of HEIs with eIDAS.

A work package should be dedicated to the **design and implementation of the central identity server building blocks**, taking into account the requirements of the procedures and roles defined in the previous work package. The proposed authentication, registration and identity linking methods should be implemented along all the operational tools needed to run, maintain and audit the identity service. The Attribute Provider management module and interfaces should also be a task of this work package, as well as the derived identity module. Generated software should be based on open source popular and common use tools, with a focus on maintainability.

A different work package from the one above should be devoted to the development of the building blocks needed to provide the **interoperability layer between the central identity service and GÉANT services**, **eduGAIN and eduroam**, namely an integrated radius server and a bridge to eduGAIN, able to act as a service provider and identity provider on the eduGAIN side and as attribute provider, identity provider and service provider towards the central identity service. Several initiatives have been working on this direction, so the pilot should try to reuse as many results as possible to develop this interoperability layer, and design the integration with the building blocks from the previous work package.

Another work package should be devoted to the **adaptation and interoperability piloting in production of the selected user services**. This work package will probably be the one involving the most institutions and the most difficult to coordinate and execute, given the dependencies of the work package towards the previous ones.

Another work package must take the task of overseeing the pilot with a different optic , focusing on **ensuring the quality of the developments**, making sure that the proper results are collected, the requirements are met and the general guidelines are being followed, especially regarding the sustainability. This work package will also have to define this sustainability strategy and provide the necessary insight given the project results to foster its adoption and achieve enough impact to extend the success into the future. This work package will also have to study the **feasibility of implanting the registration points at the HEIs**, and propose the needed actions to facilitate the expansion of this infrastructure.

Finally, a work package devoted to the **communication and dissemination** of the pilot and its results is necessary generate impact among the stakeholders and disseminate the knowledge, in order to attract HEIs to adopt the results and secure the user base necessary to provide the critical mass for the sustainability of the project results.

5.7. Feasibility and proposed planning

The pilot will have duration of **2 years and a half**, dedicating the first half of the year to the design and initial coordination and governance tasks, followed by a year mainly focusing on development of the central service building blocks and integration testing of the services to be adapted, while the last year will showcase the solution being operated in a real life environment with real life production services.

M1-M6:

During this period, the pilot Technical Business Objectives & Specifications will be properly detailed and documented, including:

- **Pilot-specific Scope Definition** (including pilot main objective and specific pilot goals suitable to be transformed into pilot success criteria)
- **Technical & Business Objectives** (to be satisfied by the corresponding use cases)
- **Use Cases Identification**: for the central service and for each participating institution, usually will present MS similarities in case more than one HEI from the same MS participates. In consideration of existing infrastructures, resources (i.e. eID credentials, commercial software partially implementing some of the required modules, GÉANT results) and services to be used across borders. A preliminary identification of required and available attributes and interface definitions and of any necessary trust mappings or legal questions will be provided in the context of major interactions. Procedures and roles for the central service must be established in this phase.
- From the results of the use-case definition, specifications for the central server **building blocks** must be generated, especially the interface definition.

Detailed pilot planning is also to be done during this period, covering all the activities required to successfully implement and bring the central identity service and pilot services into cross-border operational status in the production environment (i.e. pilot test strategy, test scripts to conduct cross-border testing based on test cases, pre-production testing planning, planning of steps for the connection of the services to the

central identity service, planning the deployment of the in-person registry points, planning the communications strategy, etc.).

M7-M18

- **Execution of Pre-Running activities**: The building blocks for the central identity service and the gateway to eIDAS will be developed and put in pre-production state. In parallel, service and attribute providers, among others, will implement the activities planned in the pilot planning phase required to connect their infrastructures to the central identity service for interoperability.
- **Running phase planning**: This detailed planning (focuses on all activities required to ensure a smooth running of the services and to gather all necessary results both for the pilot evaluation and for public reporting of progress and benefits.

M19-M30

Running phase: All activities planned in the running phased planning will be carried out and evaluated according to plans seeking maximum impact at the level of the pilot. This includes:

- Operation of the adapted services in a production environment.
- Gather information from the execution for learning.
- Engage in activities to attract the required user base for the pilot services.
- Disseminate the pilot in all relevant forums and reach all the potential stakeholders, both MS ministries of education and HEIs.
- Propose a sustainability plan, including the transfer of the building blocks to the authority designed to run the central server after the pilot's end

Although it might be considered ambitious, this pilot can successfully be executed with the proper disposition by all the members of the consortium if special care is paid to the technical specification design phase for the central identity service and an efficient governance procedure is established.

5.8. Risk assessment

The potential risks for the success of the pilot must be considered at different levels. There are technological risks, linked to the technical implementation of the solution

foreseen, legal constraints or organizational challenges. The following table identifies the main risks foreseen for the pilot proposed.

Type	Description of possible risk	Impact	% occurrence	Remedial actions
Technological	Development of a centralised identification service	Redesign, Delay, Inaccuracy	Low	Monitoring of the development. Fluid communication between the stakeholders involved in the project to work together solving any possible issue. Clear roadmap.
Legal	MS regulation might prevent the adhesion to the identity system.	Redesign, Operational feasibility	Low	Close attention to national regulation. Study the feasibility of alternative scenarios.
Organizational	Low number of users	Delay	Medium	Develop engagement activities.
Organizational	Low number of participating institutions in production	Delay	Medium	Disseminate the project within academic institutions taking advantage of existing forum. Facilitate and simplify integration procedures.
Organizational	Low amount of eduGAIN institutions accepting the integration (either as SP, IdP, AP)	Cost	Low	Disseminate the project within academic institutions taking advantage of existing forum

Table 1: Risk assessment

5.9. Pilot communication and engagement guidelines

Experience shows that presenting the benefits of such initiatives to the potential stakeholders is an enormous and non-rewarding task, as the full benefits often depend on a large-scale adoption and must be expected on the long run. That is why elaborating and providing guidelines for the preparation of specific dissemination and marketing plans to promote adoption and participation in the pilot is a major challenge. Plans must be tailored to fulfil specificities and needs of the different stakeholders (users, academic institutions…).

In order to promote pilot's objectives and vision; to raise awareness and enhance the visibility of the initiative; to win stakeholder acceptance, trust and commitment; to encourage participation for improved take-up, and to foster their sustainability beyond the project's end, the pilots must be supported by a consistent marketing plan. Participants should commit to deliver the tasks included in this plan.

In the context of the plan some elements may be considered:

Project web site.

The World Wide Web has become a major information channel. A pilot dedicated website will therefore serve as an information channel to promote the objectives and activities of the initiative.

Dissemination and communication strategy.

In order to ensure coherence and sustainability in the outreach activities, a common strategy must be developed.

Dissemination materials.

Online and offline support will be crucial to raise awareness about the initiative. Specific material (brochures, posters and factsheets) should be created accordingly.

The following table identify the target groups per level of engagement: "Informing", "Consulting and Involving" and "Empowering".

Stakeholder Type	Department	Job Title
Universities		
Universities and other academic institutions	International Relations Department	Director
	Departments in charge of registration of students Departments in charge of ICT-related services	Director
	Management Team	Rector
Students	Participating in the delivery of the pilot	n/a

Stakeholder Type	Department	Job Title
Generic and Specialized Media	Departments in charge of the news from the EC Departments in charge of ICT Related news or eGovernment	Director Director
Students associations	Institutional Relations department	Director
Similar initiatives	WP in charge of dissemination and promotion	WP or project leaders

Table 2: Target groups per level of engagement

Dissemination and engagement plans must send clear key messages through the adequate channels. These messages should reflect the benefits of the project and it is of great importance that these messages are carefully sent and not misleading.

5.10. Pilot sustainability guidelines

The pilot, during its execution, will provide a **significant amount of learnt lessons** that will help in modelling a more accurate plan to foster the adoption of the pilot results and help achieve sustainability through more concrete recommendations addressed to policy makers, academia sector institutions and ministries, researchers and related industry representatives and maximise its impact, but we will provide some preliminary insights.

It is of particular importance to sustainability the centralised approach we present. Of course, this central component of the identity system could be designed as a distributed component operated by MS entities with no harm to the technical description or goals, it can be completely abstracted at a technical level, but it presents a set of difficulties and barriers that we must examine closely.

Any distributed approach would require data synchronization mechanisms at each of the component nodes, in order to guarantee the singularity of the generated identities and avoid duplicities and data inconsistencies for citizens operating at different nodes at the same time (accidentally, maliciously or legitimately). This synchronization process would imply personal data transfer among different member states, which could carry legal issues due to specific MS legislation on implementation. If this data transfer process needs the active approval of the user, then the user experience will suffer and the synchronization will be more complex and prone to failure.

Due to this and the fact that a distributed approach would require replication of the deployments, both development, deployment and maintenance costs will rise, which is an important drawback for sustainability.

Governance is another important factor: establishing an homogeneous image, procedures and system maturity and stability is key to gain the confidence of sector stakeholders, attract services and thus, end users. With a distributed governance system, with a high level of autonomy of each component, it is extremely difficult to achieve this desired status, putting adoption at a serious risk, especially by private sector. This is especially important in the Higher Education sector, where the traditional level of independence of academic institutions reduces their eagerness to adopt state-promoted initiatives. Especially when talking about the identity federation ecosystem, where entities like GÉANT are reference models and eduGAIN is a mature, earlier in time and competing initiative to eIDAS. EduGAIN is more prone to be accepted as an initiative born inside the sector and developed in common, through a central entity constructed by all the stakeholders.

That is why an initiative in this sector needs to try to converge the needs and requirements of both sides: MS and HEIs, and thus a flexible and progressive approach is the best strategy.

As explained earlier, **attracting a significant user base** is key for the sustainability, as it will encourage new institutions to join, which at the same time will encourage more users to access and services to be deployed. This process should be started at the institutions, as they can invest more effort to provide attribute and service providers, attracting them to offer cross border services which will attract mobility users attention. To achieve this, it is essential to inform institutions properly about the benefits, requirements and procedures to join the European student identity service, including the compatibility it provides with eIDAS, showing a solid image of commitment and ensuring adequate technical support and production environment stability. The central authority running the identity service will be tasked with coordinating and organising these greatly needed engagement and visibility activities. Also, with the aim of fostering adoption and reducing the knowledge gap, seminars, workshops and audio-visual materials such as walkthroughs should be developed and offered to potential implementers. In order to minimize adoption and maintenance costs for adopters, popular software with modular design should be used for the common parts. Also, the multi-protocol design of the central service interfaces should be aimed to easily integrate the existing institutions, with the minimum development and maintenance costs, and in case some building block must be developed for the

service provider or attribute provider side, out of the box software adaptations, with proper documentation and support, should be developed for the most popular tools.

It is not particularly difficult for HEIs to put in place eID solutions that meet the eIDAS Enrolment and Authentication Mechanism elements of the eIDAS LoA mappings, while Organisation and Management element requirements are much more demanding, as they are designed for IdPs issuing government accepted official eIDs. That is the role the central service will play, generating a mutual benefit with the institutions by providing the required eIDAS compliance for identity management while the institutions will facilitate the deployment of a registration point infrastructure. To maximise the willingness to adopt, HEIs should be aware of the benefits of following the eIDAS recommendation to use a greater number of authentication factors, in order to gradually reduce the dependency of the vast majority of services on low assurance authentication, such as the username and password. The institutions should also be informed that when assessing the complexity and costs of adopting multi-factor authentication, HEIs should also factor-in the reputational damage to the HEI and costs associated to identity fraud, especially if new and more sensible services are made cross-border available. The fact that this central identity service can be used to provide multi-factor authentication at a reduced cost and with a higher level of trust, should also be informed. These institutions are unlikely to become Identity Providers of eID that would be notified through eIDAS for mutual recognition, but the identity linking system and the alternative authentication methods will allow to relate these identities with the eIDAS identity and will ease the path for mappings with eIDAS when deploying or upgrading their eID solutions to seek to the extent possible compliance with the Regulation. Also, HEIs need to be aware of the guidance on eIDAS LoA (Levels of Assurance) to interpret correctly the received information for students authenticating in the future with these types of credentials, and also for the attributes retrieved from other APs, also to mark the emitted attributes if the institution is connected as an AP. The development of applicability guides by the central authority will facilitate maximizing interoperability scenarios, trust and willingness while minimising costs and incidences in the prospect of an increased number of cross-border exchanges and long-lasting implementation of student mobility procedures based on IT systems and automation.

GÉANT, as suggested earlier, is the most likely candidate to operate this service after the end of the pilot and act as the central authority, being a renowned institution in the higher education sector, both at EU level and internationally, with a great impact and influence on the education sector and the identity federation field. A wide dialogue must be established with Higher Education sector stakeholders (States education

ministries, regions with education competences, university coordination bodies at national level, and universities) to discuss sustainable models that also consider the specific demands of sector service and attribute providers (i.e. service levels, liability, usability, security, support aspects) which are key for scaling up adoption, together with identification of funding sources at different levels to make the ecosystem economically sustainable in the longer term (e.g. considering funding and real revenue sources in the market and at national and European level for modernisation and use of ICT in higher education). It is necessary to incorporate relevant inputs and the participation of international associations such as EUNIS or EUA (European Universities Association), and national Research and Education Networks, and national academic associations such as CRUE-TIC (ES), UCISA (UK), ZKI (DE), Comité numérique de la CPU (FR) will also help to increase the possibilities of interaction with the EC and other Member States to foster academic sector uptake of eID. This dialog needs to be extended to plan the adoption of standards not only on interoperability interface specifications, but to data transfer formats and data semantics, to move towards a interoperability scenario where new automated services can be made available. GÉANT, even if not acting as the central authority of the service, and its related entities NRENS and HEIs, could benefit from the exchange of best practices on eID through the eIDAS Cooperation Network, especially at policy-making levels and/or coordination on HEIs modernisation in alignment with strategic goals of the Bologna process and the EHEA and work together to advance more in the convergence path opened by the pilot.

There is a tendency proposing that some mobility procedures should be initiated by the students themselves so it is of particular relevance that the confidence in the identity of the user is quite high. The proposed incremental model allows attracting users and institutions at an entry level and increasing their trust level while keeping compatibility and interoperability. The infrastructure resulting from this pilot is an important asset to produce the environment required to foster this tendency and so must be properly publicised among all the potential adopters. Also, as a result of the implantation and consolidation of the results of the pilot, new applications for the institutions can be envisaged using the resultant infrastructure, such as security application lock systems from the mobile identity, or credential recovery services.

Despite the importance of engaging institutions, the sustainability measures regarding the users must not be left aside. The main focus are the current and new students, but in order to popularise the service and reduce the knowledge gap on the average user, it is also important to extend the influence to users outside these circle, and that's why former students should be the following target group. Once an student

loses this status, it shouldn't stop being a user of the identity service, and also students in the past should also be able to join with the former student status to gain access to services potentially addressed to them. To attract this population group, some attractive service offering should be envisaged, and one of the most obvious and quick-gain options is the eduroam service. Offering the eduroam service to former students would suppose a good visibility and interest boost, as it would enable them to have instant internet access on a huge set of academic institutions and other public infrastructures, like airports and stations across the world. This would also open the possibility to extend funding to cover more public infrastructures and possibly extend the service offering to all of the citizens of the EU through eIDAS.

6. CONCLUSIONS AND NEXT STEPS

The pilot drafted on the present document is an ambitious project, but with the proper focus on the technical and procedural aspects it will be a successful vehicle to accelerate the adoption of eIDAS compliant eID solutions for cross-border access to student access and maximise its impact, renovating academic services and offering to EU students better, more efficient, friendly and useful services. It also helps filling some long-running gaps in the identity federation scenario by boosting the long-time pursued eIDAS and GÉANT convergence.

A lot of attention must be paid to analyse how different stakeholders (policy makers : (EU, Member States education ministries, university coordination bodies at national level), universities, as well as industry representatives) should take action, and with what kind of instruments. Recommendations, based on the prior analysis, must be issued for all significant stakeholders.

Sustainability is a crucial part of the project. Stakeholders demand certainty on the fact that their efforts will be sustained in time and that services provided are guaranteed not only in the short term, but also in the medium and long one as has been addressed in the previous section of this document.

It is also especially relevant to point out the importance of eIDAS enhanced sectorial attribute profile and the generalisation of APs. If the profile becomes a standard, only the existence of a vast number of Aps will ensure the usefulness of the solution.

European Commission

Feasibility Study on Cross-border Use of eID and Authentication Services (eIDAS compliant) to support Student Mobility and Access to Student Services in Europe

Luxembourg, Publications Office of the European Union

2018 – 78 pages

ISBN 978-92-79-80164-8
doi:10.2759/735197

KK-01-18-156-EN-N

doi:10.2759/735197 ISBN 978-92-79-80164-8