Designing an academic electronic identity management system for student mobility using eIDAS eID and Self-Sovereign Identity technologies

1st Antonios Stasis[1], 2nd Nikos Triantafyllou[4,] 3rd Panagiotis Georgakopoulos[2], 4th Ross Little Armitt[3], 5th Petros Kavassalis[5]

1st University of Aegean, Chios, Greece, a.stasis.ydmed@gmail.com,

2nd University of the Aegean, Chios, Greece, triantafyllou.ni@aegean.gr,

3rd Athens University of Economy and Business, Athens, Greece, panosgeorgak@gmail.com,

4th ARI - ATOS Research & Innovation, Madrid, Spain, ross.little@atos.net,

5th University of the Aegean, Chios, Greece, pkavassalis@aegean.gr

(*) Contact Person : Petros Kavassalis, pkavassalis@aegean.gr

Keywords
Academic networks, academic eID, eIDAS eID, Identity Management, Self-Sovereign Identities, Mobile Identity, Multi-Factor Authentication

ABSTRACT

European Universities are currently entering a phase of inter-university alliances to face the challenge of student mobility across Europe, and the European Commission is planning to fully digitize ERASMUS+ program operations by 2025. One of the main features of the emerging European Education Area is the flexible and seamless provision of cross-university and cross-border electronic services to students and academic personnel moving to another institution, inside or outside of their country, for studying, teaching or research purposes. The concept of a well-defined and user-centric European academic identity is a critical element for the successful deployment of an inter-HEI (inter-Higher Education Institutions) digital services infrastructure and enables the delivery of a consistent digital "customer experience" to the user.

This paper investigates an innovative approach for creating such a European academic identity through a service that essentially links eIDAS eID with sectorial "official" academic attributes (obtained from local academic providers and via eduGAIN). The proposed framework explores the potential of Self-Sovereign identity technologies to support the process of creation and management of linked decentralized trusted identities. The new proposed forms of identity management are under the complete control of the user and enable students to easily prove their academic and citizen identities when accessing cross-border online academic services. In this context, W3C Verifiable Credentials, stored in a secure mobile wallet, play a vital role.

1. INTRODUCTION

European Universities are currently entering a phase of active networking and inter-university alliances to face the challenge of student mobility across Europe in the context of a future cross-

border university organizational model (Klobučar, 2019). Furthermore, universities increasingly collaborate with the private sector, in international research and innovation projects, and the public sector on professional qualifications that depend on academic diplomas. Digital technologies are crucial in establishing and broadening the scope of a common European Education and Research Area that promotes peer collaboration and best-practice exchange between the different education, training and research systems and institutions. However, the digital trajectory only unleashes its full potential when interoperability is ensured at both levels, the technology infrastructure, and the service level. In this perspective, several European policies and initiatives such as European Student Card Initiative[1], Erasmus Without Paper Network[2], Erasmus+ Mobile App[3], Online Learning Agreement[4] and others, design and promote the automated exchange of academic data among the Higher Education Institutions (HEIs). The above projects were sponsored by DG EAC while EC CEF Telecom Programme is funding student mobility projects aiming at providing a student identity system that facilitates student mobility based on their academic and eIDAS identities. CEF also supports the implementation of a Core Service Platform[5] to promote student mobility integrated with the eIDAS identification services.

When starting implementing a framework for digital cooperation between Higher Education Institutions (HEI) and systematically providing cross-border collaborative learning and academic services, and these services need to be accessed online (at a distance or in situ), the question of a cross-border, consistent academic identity becomes a priority. Nowadays, academic identity systems may be effective at the local level but fragmented at a European level, and integrated only through eduGAIN (Torroglosa et al, 2018), a federated identity management system (Birrell and Schneider, 2013) mostly tailored to the needs of online authentication. Other, more recent, initiatives such as the European Student Card (ibid.) and different forms of inter-campus cards[6] also claim a position in the emerging academic digital identity value net. However, the existing systems of academic identities cannot still provide a systematic mechanism for recognizing national credentials and identification means abroad. As a result, a whole class of services (especially, services requiring data transfer between two HEIs) cannot fully mature and go beyond pilot applications because they are not able to verify online, and in a trusted manner, the identities of students and academic personnel on the basis of the credentials of the country and academic institution of origin.

Yet, the application of the assurance levels for electronic identification, as defined by the eIDAS regulation (EU/910/2014), (EU/1502/2015), and the development of a secure link between eIDAS eID[7] and the academic identity systems, may have multiple benefits, ease the mobility of students abroad; increase and improve the available cross-institution and cross-border academic and supporting services. It is also expected to have a positive impact on the reduction of administrative complexity, paperwork and front-desk attention at the level of collaborating HEIs. As a result, the combined and secure use of eIDAS eID and academic credentials becomes a cornerstone of EU policy-making, and the direction of technical change for developing a European interoperability framework which

[1] https://europeanstudentcard.eu/
[2] https://www.erasmuswithoutpaper.eu/ewp-network
[3] https://erasmusapp.eu/
[4] https://www.learning-agreement.eu/start/
[5] https://ec.europa.eu/inea/sites/inea/files/eu_student_ecard_call_for_a_core_service_platform_final-v1.0.pdf
[6] Such as the products proposed by the European Campus Card Association (https://ecca.eu/)
[7] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

supports a mutually recognized academic digital identity. We expect this new form of "linked identity" to make possible an identification process for academic purposes with higher level of assurance and referred to the isers' eID schemes backed by their home Member State (notified under eIDAS Regulation)[8].

This paper aims at presenting a flexible and scalable approach for the integration of HEIs' identity systems towards eIDAS, which does not imply the creation of a central "linked identity" database and considerably improves user experience (notable when it is compared with the current eIDAS eID-based authentication process). We have designed and developed a self-sovereign and user-centric academic identity management framework capable of linking academic and PII (Personal Identification Information) data with user consent, in a secure and privacy-protecting manner, leveraging eIDAS eID. Our construct creates an ad hoc secure digital identification environment (a common identity layer on top of the existing academic SP/Service Provider and IdP/Identity Provider systems[9]), where: a) the participants in an online service (delivered either over the web or the mobile Internet) are reliably authenticated and identified, and b) personal data protection is enforced and embedded (by design and by default) in the interoperability support system which flexibly combines academic and Member State citizen identities. More specifically, the paper addresses the following issues:

a) The policy imperative and opportunities, and difficulties, to converge and further integrate the eIDAS Network and the academic identity management frameworks
b) The adoption of the perspective of Self-Sovereign Identities (Wang and De Filippi 2020), (van Bokkem et al, 2019) and Verifiable Credentials to implement the design of a decentralized academic identity management framework as a Linking Service (Chadwick and Inman 2009), which transforms federated identities into trusted linked identities with the blockchain.

The structure of the paper has as follows:

Section 2 briefly presents the policy framework which encourages the progressive unfold of a pan-european academic digital identity. Section 3 describes the core principles of the proposed framework for HEIs integration towards eIDAS, which leverages the potential of the emerging Self Sovereign Identity (SSI) technological trajectory and incorporates other related technologies. Section 4 discusses the legal implications and constraints that arise from the combination of the eIDAS regulation with SSI architectures. Finally, Section 5 concludes the paper.

2. POLICIES FOR AN EU EDUCATION AREA AND DIGITAL INDENTITY

The European "learning mobility" policy, i.e., the policy promoting "transnational mobility for the purpose of acquiring new knowledge, skills and competences", derives from the recommendation of the Council of the European Union to Member States to "create a positive environment to support learning mobility", in the context of the "Youth on the move" policy of 2011 (European Council, 2011). After years of successful implementation of the ERASMUS Programme for students, the concept

[8] In application of the EU regulation, the Members States have agreed upon a process of mutual recognition of eID schemes, known as "notification process"; see: https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[9] A federated identity system consists of Service Providers (or Relying Parties), i.e., web/mobile entities and services that depend on a third-party Identity Provider (IdPs) to identify and authenticate a user who is requesting access to a digital resource

of mobility has been extended to include academic staff mobility projects, collaboration projects between HEIs, scholarships, internships and cultural activities. All these forms of partnership should form the core part of the European Education Area Policy, defined by the European Council (European Council, 2019) on the basis of the proposition from the European Commission (European Commission, 2018), as the strategic framework for cooperation in education and training and as a common space "in which learning, studying and doing research would not be hampered by borders". In this context, Eurydice[10], a network of 43 national units based in all 38 countries of the Erasmus+ Programme, has been charged with conducting research and reporting on how national education systems work and evolve, and making comparative studies to facilitate HEI's transnational mobility among EU countries, EEA countries, potential candidate and accession EU countries. Eurydice has recently published the Higher Education Mobility scoreboard[11] identifying among others, as core mobility topics: a) the information and guidance to students and academic personnel, b) the portability of grants and loan, including credit mobility for short-term studies and full-degree studies, c) the recognition of learning outcomes through the European Credit Transfer and Accumulation System (ECTS) and d) the recognition of Qualifications[12].

All the above mentioned policy priorities require the automated and authoritative transfer of academic data among HEIs, in order to avoid paperwork and obtain gains from lower transaction costs (administration time and processing costs), and unique identification of the students and academic staff across countries and institutions. In practice, what is required is: a) the interconnection of HEIs information systems to allow for a secure exchange and verification of student data and academic records, b) the provision of seamless access to host HEI's online academic services and facilities (including registration) for students and academic personnel who participate in a mobility project and, c) the possibility for students and academic personnel for identifying with the services of the Host HEI by using their national credentials, in a trusted manner and in line with the Once-Only Principle[13].

Within this frame of reference, several initiatives have been formed to develop pilot service and applications that implement basic digital functionalities for inter-HEI collaboration. Among them, the ERASMUS Without Paper (EWP)[14] and EMREX[15], projects. The first one aimed at creating, with some success, a free public infrastructure that will replace the usual, related to mobility projects, paper-based workflow, with a digital one. The platform developed is expected to facilitate HEIs in exchanging students data (including HEI bilateral agreements, Learning Agreements. Arrival/Departure Certificates etc.), using the interoperability and security of the EWP Network. The second, EMREX a more mature and self-sustained project, provides an infrastructure and services for transferring large datasets, thus allowing students to provide, through the EMREX network, their academic credentials (including academic records and grades) across the borders, to HEIs and employers where they apply for a position.

---

[10] https://eacea.ec.europa.eu/national-policies/eurydice/home_en

[11] https://eacea.ec.europa.eu/nationalpolicies/eurydice/sites/eurydice/files/mobilityscoreboard_2018_19.pdf

[12] https://eacea.ec.europa.eu/national-policies/eurydice/sites/eurydice/files/mobilityscoreboard_2018_19.pdf

[13] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle

[14] https://www.erasmuswithoutpaper.eu/ewp-network

[15] https://emrex.eu/

The current and short-term policies and initiatives for promoting learning and research mobility need however, to be complement with a digital pan-european identity, in application of the EC Action Plan of 2018 (European Commission, 2018): "by 2025 all students in Erasmus+ mobility should be able to have their national identity and student status recognized automatically across EU Member States, including access to campus services when arriving abroad". The combination of the two identities, the national and the student identity, requires the creation of a trusted and secure link between them, possibly by using the possibilities and the safeguards provided by modern cryptography. The "linked identity" should, of course, aggregate attributes from both the eIDAS eID and the eduGAIN federated identity. While this implies non-trivial semantic and security issues, it may also require several re-directions from one system to another, which makes the user experience questionable and the users possibly reluctant to adopt the service. During the last years, important effort has been invested at several occasions (within STORK 2.0 project but also from recent projects such as the ID4U, ESMO[16] and MyAcedmeicID[17]) to address the most important aspects of the problem (semantic and operational), but a commonly adopted solution has not emerged yet. Other initiatives such as the European Student Card (ESC)[18], an older concept that is now re-designed to integrate with the eIDAS identification rules, and novel forms of inter-campus cards (such as the student card proposed by the European Campus Card Association[19]), promise a better user experience.

Albeit the progress made and the policy-push towards a eIDAS eID-compliant ESC, several questions remain open and will have to be decided soon. How is it possible to upgrade, reform and adapt the existing academic IT infrastructures to the challenge of a European digital academic identity? Which new technologies should be adopted in order to accelerate the digitization path in the domain of academic identity services, to effectively support the provision of a new generation of cross-organization and cross-border learning and academic online services? This paper addresses these questions under the a Seld-Sovereign Identity approach to "linked identities".

3. A SELF-SOVEREIGN IDENTITY APPROACH TO "LINKED IDENTITIES"

As mentioned in the previous sections, one of the main problems of building a cross border linked academic identity (especially with respect to student mobility) is that it is fragmented. Attributes about students exist in siloed Identity and Attribute Providers which do not necessarily integrate with each other. The situation becomes worse, because each such system uses different local identifiers for the same student, which for the most part are not correlatable. Also, in the cases where a degree of correlation is possible (for example by combining the first, last name and date of birth of a student in different universities) a natural question arises as to the level of assurance for this assembled identity. eIDAS eID has been envisioned as being the glue that would stick all those fragments together, however uptake has been slow in the Academic sector. This is mostly due to the fact that existing IT infrastructures need to be updated in order to associate university ids with eIDAS identifiers which is not a trivial task.

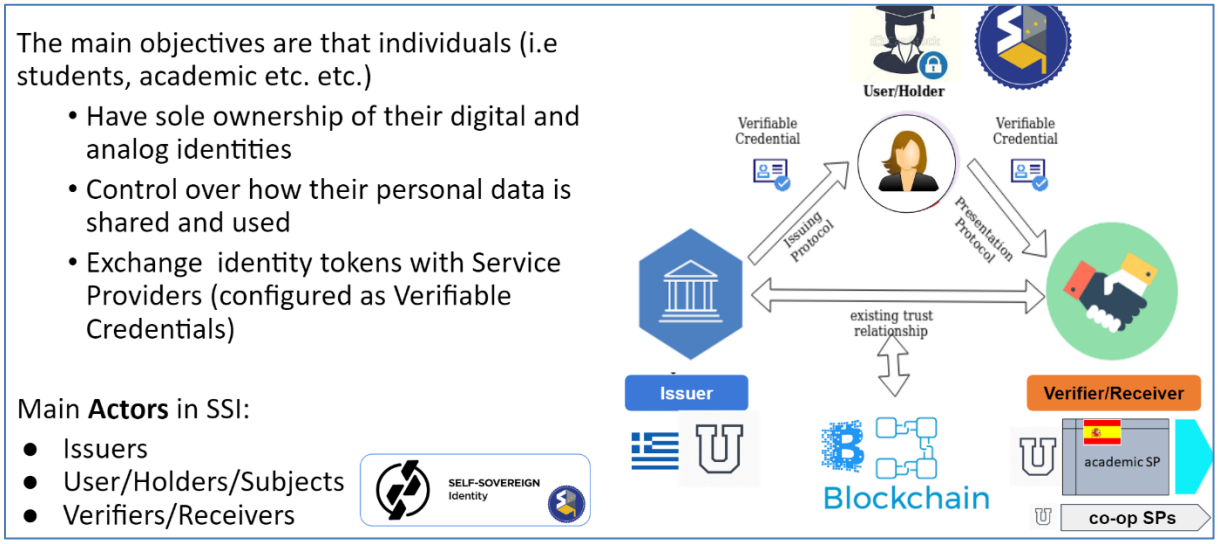
A simplistic solution would be to build a centralized system where the students would be able to aggregate their attributes and allow SPs to authenticate users over that system. However, it is well

[16] http://www.esmo-project.eu/
[17] https://uni-foundation.eu/project/myacademicid/
[18] Ibid.
[19] Ibid.

known that such systems pose huge honey pots for identity theft attacks. Another approach would be to allow users to authenticate over various Identity Providers and "on the fly" aggregate the required attributes. Again though, our experience has shown that this leads to very poor user experience and high service drop-out rates.

The system we propose in this paper attempts to address these issues by adopting eIDAS anchored Self Sovereign Identity (SSI) (Allen, 2016) as the means of generating linked student identities suitable and recognizable across borders and institutions. Specifically, it uses Verifiable Credentials (VCs), as those are standardized by W3C[20], as the means enabling Identity Linking. VCs are tamper-evident credentials that have provable authorship, ownership and integrity (i.e. cryptographically verifiable). They are always under the users control, require no centralized repository and are significantly expressible (in other words they can be used to represent an extended Student Identity). By adapting this emerging data model the need for interoperability between the existing data sources is removed.

In a nutshell, the proposed system enables students to generate their private space with eID information and academic records from HEIs. This allows the users to securely store their identity attributes, as those are gathered by the various authoritative sources, encoded as Verifiable Credentials and link them together. Thus, the students can create a linked identity by combining the various identity fragments each identity provider offers. Additionally, HEIs services or third party service providers are able to verify the authenticity of identification and academic attributes presented by the students with no need to contact a centralized service that would act as a single point of failure for the system or connect and integrate with multiple IdPs/APs. The following figure captures the high-level design of the proposed architecture.



The proposed architecture's key features are: a) the transformation of digital (federated) identity into trusted linked identities and b) the implementation of new forms of identity management, under the complete control of the user, capable to hold and manage links between a user's different

[20] https://www.w3.org/TR/vc-data-model/

identities, hosted by different IdPs and delivered through different networks (for example eIDAS, eduGAIN) without compromising the privacy of the user.

In this context, the user (i.e) Data Subject "holds" a wallet of Verifiable Credentials (VC); each Credential is composed of a number of identity claims (a VC is a piece of information that is cryptographically trustworthy).

3.1. Main Concepts

In more details, the main technical concepts of the architecture are: Decentralized Identifiers (DIDs), Verifiable Credentials (VCs) and Verifiable Presentations (VP). DIDs[21] are URIs that relate a user i.e. a specific subject with the means for trustable interactions. They are fully under the control of the user, who owns them, and are independent from any centralized registry (like for example an identity provider, or a University's records). VCs are non-reputable sets of statements made by an entity about another entity. These claims are cryptographically generated[22]. In the context of this paper, a verifiable claim could be issued by a University, which affirms that a related person is holding a degree from this University. VPs are tamper-evident presentations encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. They are similar to VCs with their main difference being that VPs usually contain data that is synthesized from VCs, but do not contain the original VCs. In this way VPs can be presented as proof of owning claims issued by different Issuers. A VP can express data from one or more VCs.

3.2. Main Actors and Trust Anchoring

The main actors of the system are the User/Subject, the Holder, the SSI Issuers, SSI Wallets/Agent, and finally the SSI Consumers (or Service Providers). The Subjects are the entities that a given VC is about or relates to. The Holder denotes the individual or entity in control of the digital wallet or agent that stores and controls the use of a given Credential. The Holder may or may not be the Subject. An SSI Issuer is an entity that is capable of generating Verifiable Credentials about users e.g. the university of origin or the identity provider. These claims express a piece of information the issuer is in possession of the user. Thus, the trust of a consumer to such a claim is directly related to the trust of the consumer to the issuer. SSI wallets are digital wallets that enable users to authenticate using the Verifiable Claims they have been issued, and store these VCs. They are usually implemented as applications to a mobile device. The PII information is stored in the SSI wallet. A consumer denotes an entity that is capable of receiving and validating VCs from user wallets e.g. destination university.

In the proposed architecture trust is decentralized. Consumers of verifiable claims decide which issuers to trust. To facilitate the trust building relationship between Issuers and Consumers, we leverage the existing eIDAS network for the discovery and verification of the identities of the Issuers in the system23. Additionally, Consumers are capable of independently: a) verifying the issuers identity, b) validate the claim itself, and c) validate ownership of the user on the VC.

3.3. Main Functionalities

---

[21] https://www.w3.org/TR/did-core/
[22] https://w3c.github.io/webpayments-ig/VCTF/charter/faq.html
[23] https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/about

The main functionalities of the framework are related with the management of the VC life cycle. It is really worth to mention the following:

Issuer Initiation: The Issuers of a VC generate a public DID Document. A DID document contains information about who the issuer is, the endpoints they use and the cryptographic keys they use (these documents are usually stored in a distributed ledger). In the proposed architecture Issuers include in this DID document public keys derived from an eIDAS qualified seal. In this way the legal entity behind an Issuer is anchored to the eIDAS network and thus is easily discoverable and verifiable.

VC Issuance: The user accesses an Issuer service and proves ownership over a DID. Next, the user fetches attributes from authoritative resources (e.g. eIDAS, eduGAIN etc.) connected to the Issuer. Finally, the Issuer creates VCs about the user containing some information that they attest to (based on the attributes available), includes the user's DID as the subject of the VC and transmits the VCs to the user's wallet. A VC basically is a statement, saying that the Subject of this token has some attributes that the issuer attests to. So, the issuer is the trust anchor-entity in the framework not the user. In the academia case the issuer can be either a HEI or an eduGAIN proxy service. This functionality is compliant with a predefined Policy Linking Architecture that sets the high-level requirements and enablers for managing and providing an efficient Linking Service. VCs are shared as proof of a set of identity attributes (obtained by authoritative resources, eIDAS eID, eduGAIN etc.), and are anchored using Decentralized PKI (DPKI) to a Distributed Ledger, by a public Decentralized ID (DID) written by the Issuer of the Credential.

VC Storage: The VCs are securely stored in the users' wallet, assuming that the user is in possession of an SSI wallet capable of proving ownership on Decentralized Identifiers (DIDs). VCs are transferred encrypted and signed to the user's Wallet (a secure application, usually stored on the user's mobile device).

VC Consumption: The users want to present attributes from a (set of) VCs to a Service Provider (e.g. a destination HEI). The users interact (using their wallet) with the HEI, by generating, in most cases, a Verifiable Presentation (VP) containing the requested attributes based on the VCs stored on their wallet (or in some cases might even transfer the VCs themselves). Next, the Service Provider receives the transmitted data and verifies their validity, authenticity and user ownership over them and grants access accordingly to the user. The authenticity of a VC can be verified by a public key associated with the Issuer's DID through a Service Interface provided to academic Service Providers (HEIs) and beyond. Ownership of a VC can also be verified cryptographically, in a similar manner.

3.4. Use Case Example

For example, assume that a student needs to book a room at a hotel offering special prices to Erasmus students with one of its partner universities. To enable this special price:

1. The student accesses their visiting University VC issuer service, connects their SSI wallet, authenticates using their university credentials and gets issued a Verifiable Credential attesting to their Erasmus status (this might be an atomic credential or contain additional data).
2. The student accesses the hotel booking page. There she selects to enable the special discount and is required to present a VP proving her Erasmus status
3. The student unlocks and connects their wallet with the SP service. Next, the wallet generates an appropriate VP and transmits it to the SP service

4. The SP service the VP, validates it and verifies that corresponding Issuer DID resolves to one of the partner universities
5. The SP service grants the discount to the student accordingly

4. LEGAL OPERATIONAL PREREQUISITES

Currently the level of assurance that characterises an eIDAS identification schemes should be extended to assess the quality of the linking service in the context of the SSI environment and verifiable credentials. It is important to mention that the assurance level of the academic attributes should also be revisited and defined, otherwise only trust based on a bilateral agreement among HEIs could be applicable. This is what is actually being done by EWP project services, and ESC services. In the context of eIDAS the role of the identity provider is crucial and is responsible for the management of the users' credentials. Verifiable Credentials should be recognized as a new instance of electronic identification considering both technical issues and a set of rules to allow for the use of them. This will require to revisit the Commission Implementing Regulations EU/2015/1501, EU/2015/1502, EU/2015/1984.

Moreover, complementary legal provisions should be required at national level, since National eIDs are issued according to the national legislation.

The use of Verifiable Credentials should also be expanded beyond eIDAS legal scope, especially when it comes to private sector HEIs. HEIs in the context of eIDAS should become Qualified Trust Services Providers issuing Verifiable claims (SSI issuers) linked with identity information, anchored in Qualified Certificates.

GDPR requirements will be easily applied in this proposed framework since the user is the holder of the data and only with his consent the data will be revealed to the service provider i.e. the destination HEI. The verifiable claims and credentials issued by a HEI should be considered as personal data since they are linked with the identity of a person although it is not possible to do this link without the consent of the User (European Commission, 2020).

5. CONCLUSIONS - FUTURE WORK

Given the fact that mandatory identification data (i.e. natural person minimum data set) are obtained automatically through the eIDAS SAML- based assertions with Member State guaranteed provenance of the data and with mechanisms ensuring its integrity and confidentiality combined with academic (eduGAIN), ESC and EMREX attributes, enables the safe use of this data to automatically complete web-based forms (for example in the context of Erasmus procedures), avoiding manual entry of data and thus minimizing the risk of errors in the input of personal information into HEI Identity and Access Management and/or Student Information Systems and minimising the burden and risks of in-person identity verification, especially for foreign students with their own national ID cards.

The proposed design will provide solutions, which bring concrete benefits and real improvements by addressing the need of and effectively facilitating the (physical and virtual) mobility of European students across the European Higher Education Area, based on paperless procedures enabled by the widespread cross-sector use of eIDAS-compliant electronic identification and authentication schemes (that minimizes the risks of identity theft/impersonation), the ability to exchange academic attributes in a manner which is consistent with and complementary with eIDAS Network exchange of minimum natural persona data set information and leveraging the enormous potential of eduGAIN

inter-federated identity and European Student Card harmonized identifier approach by offering identity linking and bootstrapping mechanisms as a basis for their interoperability. Huge savings in time and travel for students and for administrative staff by achieving noteworthy simplification of several administrative procedures and significant reductions of time to process the data when compared to the same procedures based on non-on-line cross-border workflows are expected.

The proposed architecture allows the user to manage his wallet of identities (through a web and a mobile interface), by linking existing ones and deriving others (like a opaque unique identifier, that could be used as European Student Identity), also controlling which information can be delivered and whom can it be delivered to, deleting links and creating sub-profiles. The impact of the linking academic attributes to CEF eID can be used to bootstrap a single European Student Identity (as well as to derive other identities, temporary or persistent, like orcID24) and establish links with all the other identities belonging to the student.

Considering this framework to an ubiquitous pan-European recognition of students' status and identity and once-only principle, a new CEF DSI should be developed to address the need for a single identity at least virtually through identity reconciliation, while still preserving the rights of the user over his data by enabling linking national eIDs and academic identifiers, as per the needs of HEIs/Ministries/students in their Member State. This will contribute to realise the strategic goal to electronically apply to and enroll in any accredited HEI in Europe when moving abroad for studies and traineeships and for Higher Education and to reduce the administrative procedures for students in mobility.

(*) Part of this research is funded by CEF Telecom Programme, and more specifically by INEA actions no (SEAL project, Grant Agreement No INEA/CEF/ICT/A2018/1633170) and no (eSig eID project, Grant Agreement No INEA/CEF/ICT/A2017/1558304)

REFERENCES

- T. Klobučar (2019), "Facilitating Access to Cross-Border Learning Services and Environments with eIDAS", Learning and Collaboration Technologies. Ubiquitous and Virtual Environments for Learning and Collaboration, International Conference on Human-Computer Interaction pp 329-342, June 2019
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- European Commission (2018), CEF eID Building Block for Banking and Educational Domains, Architectural Solution Document (eStudent) with recommendations, Deliverable March 2018

[24] https://orcid.org/

- E. Torroglosa, J. Ortiz, A. Skarmeta (2018), "Matching federation identities, the eduGAIN and STORK approach", in Future Generation Computer Systems Volume 80, pp. 126-138, March 2018
- E. Birrell and F. B. Schneider (2013), "Federated Identity Management Systems: A Privacy-Based Characterization", in IEEE Security & Privacy, vol. 11, no. 5, pp. 36-48, Sept.-Oct. 2013
- D. van Bokkem et al (2019), "Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology", available at https://arxiv.org/pdf/1904.12816.pdf
- A. Mühle et al (2018), "A survey on essential components of a self-sovereign identity", available at https://arxiv.org/pdf/1807.06346.pdf
- F. Wang and P. De Filippi (2020), "Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion", available at https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full
- P. Coelho et al (2018), "Federation of Attribute Providers for User Self-Sovereign Identity", in Journal of Information Systems Engineering & Management, vol. 3 (4), pp.32, 2018
- S. Pal et al (2019), "On the Integration of Blockchain to the Internet of Things for Enabling Access Right Delegation", in IEEE Internet of Things Journal, pp.1-1
- S. Jung (2017). Personal OAuth authorization server and push OAuth for Internet of Things, in International Journal of Distributed Sensor Networks, 13(6), p.155014771771262
- Q. Stokkink and J. Pouwelse (2018), "Deployment of a Blockchain-Based Self-Sovereign Identity", in IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1336-1342
- D. W. Chadwick and G. Inman (2009), "Attribute Aggregation in Federated Identity Management", in Computer, vol. 42, no. 5, pp. 33-40, May
- M. S. Ferdous et al (2019), "In Search of Self-Sovereign Identity Leveraging Blockchain Technology", in IEEE Access, vol. 7, pp. 103059-103079
- J.S. Hammudoglu et al (2017), "Portable Trust: biometric-based authentication and blockchain storage for self-sovereign identity systems", available at https://arxiv.org/abs/1706.03744
- D. Lagutin et al. (2019), "Enabling Decentralised Identifiers and Verifiable Credentials for Constrained Internet-of-Things Devices using OAuth-based Delegation", in Workshop on Decentralized IoT Systems and Security (DISS), San Diego, CA, available at: https://www.ndss-symposium.org/wp-content/uploads/DISS2019-proceedings-front-matter.pdf
- Self-ssi.com (2020), "esatus SeLF - Enables Self-Sovereign Identities (SSI) and empowers legacy & SSI-native IT systems", available at: https://self-ssi.com/en/#aboutus
- Z. Diebold (2017), «Self-Sovereign Identity using Smart Contracts on the Ethereum Blockchain», Master in Computer Science. University of Dublin, Trinity College
- A. Palomares (2019), "The next Identity Management evolution: Self Sovereign Identity", Atos, aailable at https://atos.net/en/blog/the-next-identity-management-evolution-self-sovereign-identity
- J. Wang (2018), "Single Sign-on using OAuth2 and JWT for Distributed Architecture", available at https://insready.com/en/blog/single-sign-using-oauth2-and-jwt-distributed-architecture
- C. Allen (2016), "Self-Sovereign Identity Principles", available at https://github.com/ChristopherA/self-sovereign-identity/blob/master/self-sovereign-Identity-principles.md

- European Commission (2020), “SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market”, Dr. Ignacio Alamillo Domingo