innovalor

The impact of EU Digital Identity Wallets on NRENs

Colophon

DATE	2021-12-28
VERSION	1.0
PROJECT REFERENCE	
CONFIDENTIALITY	Public
STATUS	Final
COMPANY	Innovalor Advies
AUTHOR (S)	Jurjen Braakhekke, Koen de Jong, Bob Hulsebosch

Table of contents

Management summary

In early June 2021, the European Commission announced their plans to introduce a framework for a European Digital Identity as an amendment to the eIDAS regulation. The framework creates a new qualified trust service for attestation of attributes concerning information related to, amongst others, educational qualifications and credentials. With so-called EU Digital Identity Wallets (eWallets), such information can be offered, shared and exchanged across borders, in full security, with data protection and legal recognition across borders, all under full control of the end user. eWallets have the potential to empower students and workers in proving their skills across the EU and to improve identity-related processes and services in the research and education sector.

This research helps NRENs to gain a better understanding of the potential and limitations of the EU Digital Identity Wallet concept and how it may impact their digital identity initiatives. It answers three research questions:

1. How does the EU Digital Identity Wallet impact the roles of NRENs and providers of credentials?
2. How can existing NREN initiatives be leveraged to support the EU Digital Identity Wallets?
3. Is there a coordinating or supporting role to be played by GÉANT in this development?

The research was done by desk research, interviews with NREN and identity experts, and a plenary session with NREN and identity experts to discuss and review the answers to the research questions.

European Digital Identity Wallets

Although eIDAS does not say anything about the form of the eWallets, in practice this will often come down to a mobile application, published by public or private parties, that can be used as a national eID, both online and offline, for both public and private services. The core functionality of eWallets concerns the identification and authentication of users, the exchange of attributes and credentials, and the provisioning of digital signatures. The identification/authentication is performed with Personal Identification Data (PID) including a unique and persistent identifier (this can be considered an ‘EU ID’).

eWallets receive their contents (IDs, attributes, attestations, credentials) from certified authentic sources and attribute providers. Relying parties must be registered, so eWallets can verify their authenticity. All actors in the eWallet ecosystem must comply with the technical architecture, standards, references and guidelines for implementing eWallets. These are being defined in the so-called Toolbox, which will be published by the end of October 2022. At least one eWallet must be available in each of the Member States by 30 June 2024.

How does the EU Digital Identity Wallet impact the roles of NRENs and providers of credentials?

The proposed eIDAS amendment requires private relying parties that provide services that are required by national or Union law to use strong user authentication for online identification to accept the use of eWallets[1]. This means EU educational institutes must accept certified eWallets for electronic identification purposes during student registration at the institute. Acceptance of eWallets for other use cases is not required by eIDAS but optional. Also, eIDAS requires all parties relying on eWallets (Relying Party, RP) to be registered as such by their Member States. This may involve a certain assessment to ensure institutes comply with the technical architecture, standards, references, guidelines and best practices for eWallets.

Institutes may delegate the implementation and execution of the eWallet RP infrastructure and processes to their NRENs, much like they delegate trust and identity infrastructure and processes to NRENs today. NRENs are well positioned to take up the role of RP, although certain NRENs may be challenged to provide the required resources to do so.

[1] eIDAS amendment Art. 12

Some concerns exist regarding institutes delegating their RP role to their NREN because this introduces a single point of failure in the eWallet processes and increases the risk of NRENs snooping on the information exchanged via eWallets. However, NRENs are expected to be able to leverage their strong trust capabilities and assets to manage these risks reliably and transparently and thus become highly trusted RPs.

In addition to becoming RPs, NRENs may act as a so-called eWallet Proxy, enabling institutes to issue eduIDs to eWallets. This would allow eWallets to be used to access services within the existing research and education identity frameworks, facilitating the integration of eWallets in these ecosystems. However, the use of eWallets may not be enforced when there is no legal basis for strong user authentication. This implies that there must remain another means for end users to identify themselves, for example the existing identity federations such as eduID. Also, it is not yet clear if the eWallet proxy concept will be included in the Toolbox, and if the concept will be allowed for bootstrapping sectoral identity frameworks to the eWallet.

For institutes, alternative implementations of eWallet ecosystem roles (i.e., by themselves or by (new) third parties) seem less viable, at least in the short to mid-term. This may change as the eWallet ecosystem develops and if users want to solely rely on eWallets for all kinds of identity related use cases. This development would change the ‘trust and identity’ market significantly, forcing institutes and service providers to reconsider their existing identity frameworks.

The amendment of the eIDAS legislation creates a uniform European market of approximately 450 million users for eWallet providers. It is not inconceivable that tech giants such as Apple and Google will enter this market with certified eWallets. Aside from the tech giants, existing wallet providers are likely to develop into eWallet providers. But even if tech giants and wallet providers do not bring a single eWallet solution to the market, Member States must provide an eWallet for all inhabitants. Due to this expected availability of eWallets in the market, a scenario of NRENs developing and providing eWallets is not considered viable or relevant.

How can existing NREN initiatives be leveraged to support the EU Digital Identity Wallets?

As mentioned in the previous section, eWallets must be supported as identification means during the registration of new students. In addition, the following use cases are expected to benefit from the application of eWallets:

- eWallets can carry verifiable credentials, such as diplomas, micro-credentials and other education and skills related documents (CVs, language passports, copies of degrees, work certificates, etc.). Promising candidates to issue to eWallets are diplomas and EduBadges. However, institutes and NRENS must deal with national differences in their legal responsibilities and options for issuing such credentials.

- eWallets provide opportunities to solve several issues and challenges related to (international) student and staff mobility. This would improve student registration at foreign institutes, handing out grades and exchanging these between institutes, handling multiple accounts at different institutes.

- For staff and researchers working for several institutions at the same time or taking up temporary (guest) roles at various institutions, eWallets can be applied to simplify identification and onboarding processes.

- For lifelong learning, eWallets can be used to carry and present identification attributes and knowledge and skill credentials when returning to institutes for further education, again simplifying onboarding and attestation processes.

In the international research domain, the role and value of eWallets is still unclear. Here, eWallets bring many questions to the table that require further research and/or may be answered as the eWallet Toolbox is being developed. For instance, how can eWallets be used outside of the EU? Even in countries that are not officially recognised by the EU? And how to use eWallets to grant access to research resources that typically have non-interactive interfaces and command line interfaces? How to deal with the lack of standardisation in research resource user authentication mechanisms?

Applying eWallets to the use cases requires they implement more complex eWallet processes and infrastructures to issue and consume attributes, attestations and credentials. Again, NRENs are well positioned to take up these roles for their member institutes.

However, international standards for eWallet research and education specific attributes, attestations and credentials are still lacking. NRENs can drive the development of such standards and, through GÉANT, act as a sectoral governance body for these standards.

Is there a coordinating or supporting role to be played by GÉANT in this development?

We advise both institutes and NRENs to actively assess eWallet developments, not only in the research and education domain but in the market in general, and adapt the strategies for their trust and identity frameworks accordingly. GÉANT is well positioned to facilitate this through market research, eWallet technology assessments, market consultations for eWallet solutions and services, and providing a strong liaison with EC identity initiatives such as the Toolbox development.

Depending on the ambitions of institutes and NRENs to apply eWallets for use cases around (international) student mobility and Lifelong Learning, GÉANT can support and harmonise the development of the required eWallet research and educational content standards and act as a sectoral governance body for these standards.

1 Introduction

1.1 CONTEXT

In early June 2021, the European Commission announced their plans to introduce a framework for a European Digital Identity. This should enable citizens to prove their identity and share credentials via EU Digital Identity Wallets (eWallets). The framework creates a new qualified trust service for attestation of attributes concerning information related to, amongst others, educational qualifications and credentials. With so-called EU Digital Identity Wallets such information can be offered, shared and exchanged across borders, in full security, data protection and with legal effect across borders. In this way, the EU Identity Wallets have the potential to play a role in empowering students and workers in proving their skills across the EU, however it is not yet clear how the framework and wallets will work in practice.

This research helps all NRENs to gain a better understanding of the potential and limitations of the EU Digital Identity Wallet and how it may impact their digital identity initiatives. It does so by researching the strengths, weaknesses, opportunities and threats for possible roles NRENs can play with respect to the European Digital Identity framework, and assessing the high-level architectural implications and possible leverage of current NREN initiatives for implementation of these roles.

1.2 OBJECTIVE

This project aims to help NRENs gain a better understanding of the potential and limitations of their roles with respect to the EU Digital Identity Wallet, and how these may impact their initiatives. The project aims to reach this goal by answering the following questions:

1. How does the EU Digital Identity Wallet impact the roles of NRENs and providers of credentials?
2. How can existing NREN initiatives be leveraged to support the EU Digital Identity Wallets?
3. Is there a coordinating or supporting role to be played by GÉANT in this development?

The project is to identify the strengths, weaknesses, opportunities and threats for the NRENs in each of the identified roles, and to assess if and how existing NREN initiatives can be leveraged to accomplish these roles.

1.3 PROJECT APPROACH

The main activities conducted are as follows:

1. An initial analysis of the European Digital Identity Wallet was prepared, based on desk research. This was used to determine interview questions for the NREN experts and stakeholders.
2. The team conducted interviews with representatives from four NRENs, GÉANT, Euroteq and NIKHEF[1] to discuss identity related initiatives and challenges and their relationship with the eWallet concept.
3. Based on the interviews, four possible NREN roles in the eWallet ecosystem were identified. For each role, the strengths, weaknesses, opportunities and threats for the NRENs were assessed.
4. The roles and SWOTs were reviewed with GÉANT and SURF and refined through further desk research. This resulted in the identification of a fifth NREN role, for which strengths, weaknesses, opportunities and threats for the NRENs were assessed.
5. An expert session[2] was held to present a high-level overview of the EU ID wallet concept and ecosystem as well as an overview of the digital identity initiatives and challenges in the research and education domain, and to review the various roles NRENs may play within the ecosystem, including a SWOT-analysis for each role.
6. The outcomes of the interviews and the expert session were applied to answer the research questions and provide recommendations for further steps in this report.

[2] Please refer to Appendix 1 for an overview of interview and expert session participants.

2 EU Digital Identity Framework

This chapter attempts to clarify the concept of wallets as proposed in the revised eIDAS regulation. At the time of writing, various aspects of the eWallet are being elaborated and established by the eIDAS Expert Group. Various ambiguities and contradictions will be resolved over the coming months. For the most up-to-date description of the structure and operation of the eWallet ecosystem we refer to the most recent publications of the eIDAS Expert Group[3].

2.1 EUROPEAN DIGITAL IDENTITY WALLET

The revised eIDAS legislation aims, among other things, to provide a European Digital Identity solution in the form of an eWallet that must be recognized by public and private service providers who need a certain degree of identity assurance for their services. Although eIDAS does not say anything about the form of the eWallet, in practice this will often come down to a mobile application, published by public or private parties, that can be used as a national eID, both online and offline, for both public and private services.

With this eWallet the user can:

- Safely request and obtain, store, select, combine and share identification data and the electronic attestation of attributes, in order to authenticate online and offline, in a manner that is transparent and traceable to the user;
- Sign by means of qualified electronic signatures and seals.

The identification/authentication is performed with Personal Identification Data (PID) including a unique and persistent identifier (this can be considered an ‘EU ID’). Pseudonymous or anonymous authentication is supported by providing a privacy preserving proof of possession.

Article 6a of the amendment refers to the services for which an eWallet can be used:

- Issuing of qualified and unqualified[4] electronic attestations of attributes or other qualified and unqualified certificates by qualified and unqualified trust services to the European Digital Identity Wallet;
- Requesting and validating personal identification data and electronic certificates of attributes by relying parties;
- The presentation to relying parties of personal identification data, electronic attestation of attributes or other data such as login details, in local mode that does not require internet access for the wallet.

The core functionality of eWallets concerns the identification and authentication of users, the exchange of attributes and credentials, and the provisioning of digital signatures. In addition to the basic functionality, various eWallet use cases have been identified, some of which have been designated a priority in the further elaboration of the eWallet concept into the so-called Toolbox (see also paragraph 2.2). One of these priorities are education use cases.

Providing documents for qualification recognition processes can be costly and time consuming for end users, businesses, and educational and academic institutions. Using eWallets, authentication and attestation processes for students and employees can be facilitated. For example, digital attestations for diplomas can be shared in a verifiable, trusted format with another educational or training institution or a third party (f.i. an employer), in a Member State other than the Member State that issued the diploma. This use case enables pan-European exchange of educational attestations (and possibly other educational and vocational certificates) with third parties such as universities or companies, significantly reducing verification costs and improving confidence in the authenticity and integrity of documents.

[3] https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupId=3032&fromMeetings=true&meetingId=32634

[4] https://ec.europa.eu/cefdigital/wiki/display/ESIGKB/What+is+the+difference+between+non-qualified+and+qualified+trust+service+providers

2.2 EDI FRAMEWORK TOOLBOX DEVELOPMENT

The European Digital Identity Framework Toolbox describes the technical architecture, standards, references, guidelines and best practices for implementing eWallets. These will be determined in the period up to April 2022 and then tested by executing pilots in the period up to April 2023. With regards to these pilots, it is not yet clear which aspects and use cases of eWallets will be tested, and to what extent Member States will coordinate their pilots. Also, it is still unclear how the private sector will be involved in these pilots.

The Toolbox will use as many open standards as possible for issuance and delivery of attributes, digital documents and verification protocols. The Toolbox will be published by the end of October 2022. At least one eWallet must be available in each of the Member States by 30 June 2024.

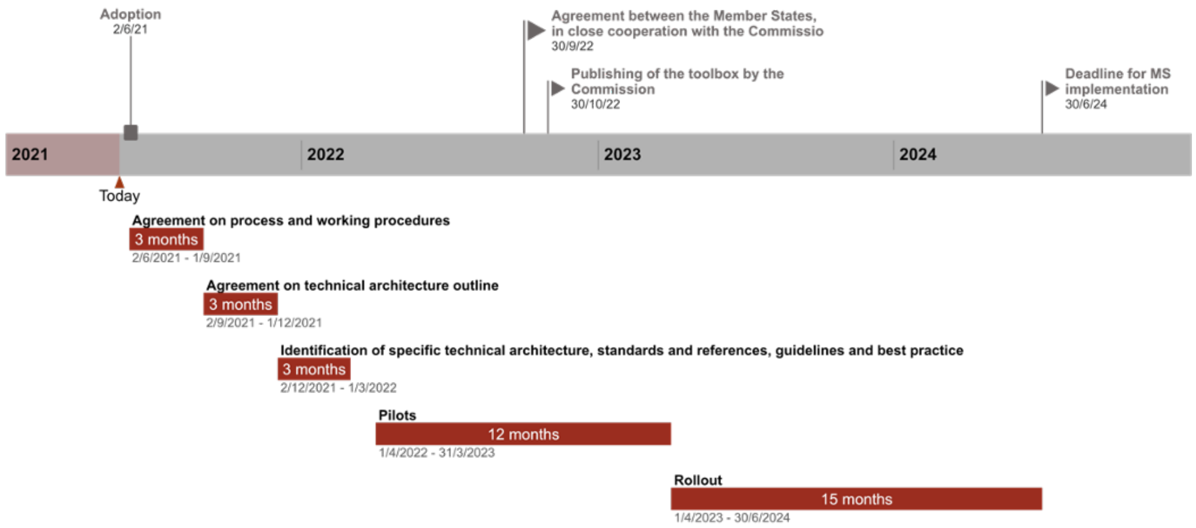


Figure 1: Planning of Toolbox development and eWallet rollout.

2.3 EUROPEAN DIGITAL IDENTITY WALLET ECOSYSTEM

The concept eWallet ecosystem is described by the EU Commission in the non-paper "European Digital Identity Architecture and Reference Framework" (version 20210930). This non-paper was used for the ecosystem description below. The roles and processes will be further elaborated and agreed upon by the eIDAS Expert Group in the coming months.

The operation of eWallets requires many actors who, in collaboration and interdependence, carry out the processes necessary for:

- The issuance of eWallets;
- Providing data to eWallets;
- Exchanging data between eWallets and relying parties;
- The verification of the data received by relying parties.

We first describe the most important roles and then discuss the processes.

2.3.1 Roles in the eWallet ecosystem

The diagram below shows a high-level overview of the eWallet ecosystem.

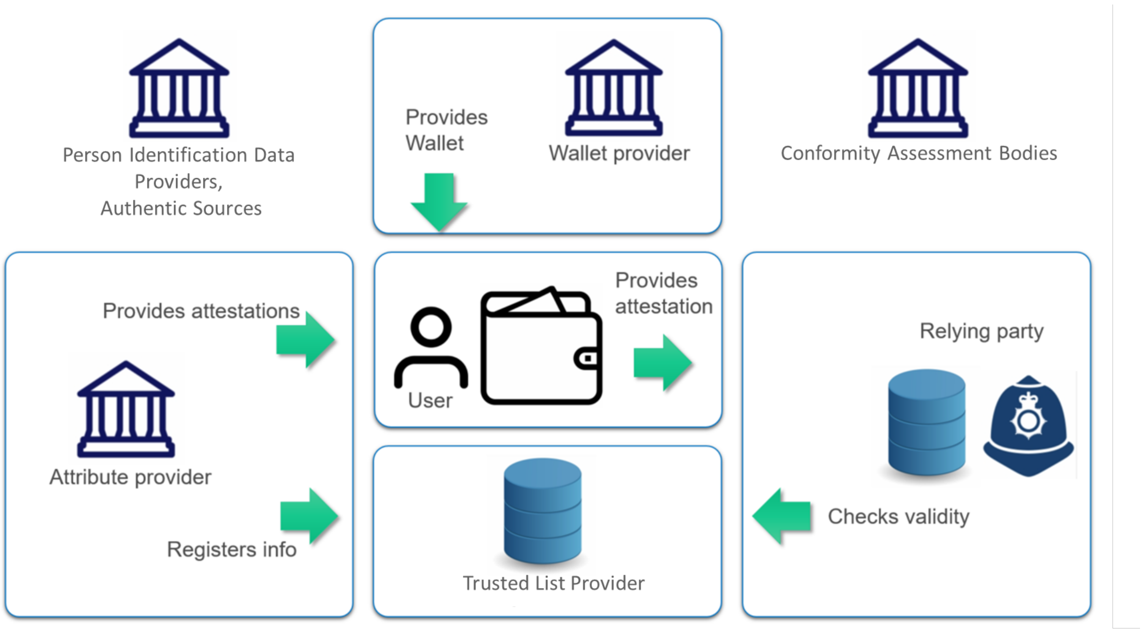


Figure 2: Simplified view of European Digital Identity Wallet ecosystem.

The following key roles can be distinguished in this ecosystem:

- End users of Wallets

  End users of Wallets are the natural or legal persons using a Wallet to receive, store and present attestations, including attributes to service providers proving their identity or a particular attribute. Wallets enable end-users to create and use qualified electronic signatures.

- Wallet Providers

  Wallet Providers are defined as Member States or other organisations either mandated or recognized by Member States making Wallets available for users.

- Person Identification Data Providers

  Person Identification Data (PID) Providers provide Person Identification Data securely to European Digital Identity Wallets (in a harmonized common format) and provide a mechanism to verify the validity of the data. They will typically be the same organisations that today issue official identity documents.

- Authentic Sources

  Authentic sources are those sources legally appointed to hold data on a defined set of attributes including for example address, age, gender, civil status, family composition, nationality, educational qualifications titles and licenses, professional qualifications titles and licenses, public permits and licenses, financial and company data.

- Electronic Attestation of Attributes (EAA) Providers

  Electronic Attestation of Attributes (EAA) Providers issue EAAs. As with other Trust Services, the EAAs can be qualified (QEAA), issued by qualified EAA providers (QEAAP), or non-qualified, issued by either qualified or non-qualified providers. The requirements applicable to all current eIDAS (Q)TSP and the (Q)TS they provide respectively apply to (Q)EAAP and the (Q)EAAs they provide.

- Relying Parties (RPs)

  Relying Parties request presentations of PIDs and attributes (including attestations and/or credentials) because they are required to do so by law, by contractual agreement or by their own corporate decision. RPs are responsible for authenticating the attributes they receive from the Wallet. RPs may be required to match the identity of Wallet users to existing ones.

- Trusted Lists Providers (TLP)

  The specific status of a service, entity or device may need to be verified in a trustworthy manner. The qualified status of QTSPs and the QTS they provide (including the issuance of QEAAs) can be recorded in trusted lists by Member States. Additional information may also need to be provided, such as verified identification data related to wallet providers, person identification data providers, relying parties or certified wallets. The provision of such additional information may take the form of trusted lists or be provided in an authenticated manner in other forms (e.g. databases, ledgers, PKI-based certificates, signed assertions, EAAs). In this report, these possible means are referred to a "trusted lists" irrespective of their actual implementation.

- Conformity Assessment Bodies (CAB)

  The Wallets and QTSPs will have to be certified. Conformity Assessment Bodies (CABs) will be accredited by Member States as responsible for carrying out assessments on which Member States will have to rely before issuing a European Digital Identity Wallet or providing the qualified status to a Trust Service Provider.

2.3.2 Process flows in the eWallet ecosystem

When using eWallets, the following processes can be distinguished:

- Issuance of the eWallet

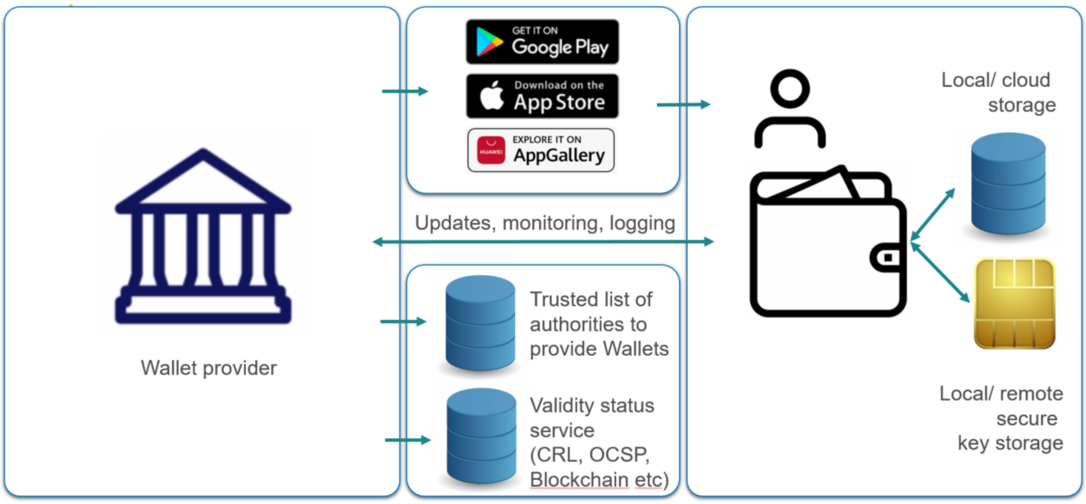

GET IT ON Google Play
Download on the App Store
EXPLORE IT ON AppGallery
Local/ cloud storage
Updates, monitoring, logging
Trusted list of authorities to provide Wallets
Wallet provider
Validity status service (CRL, OCSP, Blockchain etc)
Local/ remote secure key storage

Figure 1: Issuance of the Wallet

eWallets will typically be provided as mobile applications that are able to securely communicate with the relevant parties and components. They need to be provided as software for the major mobile platforms (e.g. iOS, Android). To be distributed through relevant App Stores, eWallets need to be developed in conformity with their rules.

All issuers of eWallets need to be authenticated, allowing the verification of their authority to maintain validity status services for the individual eWallet instances installed on user's hardware.

- Onboarding to the wallet

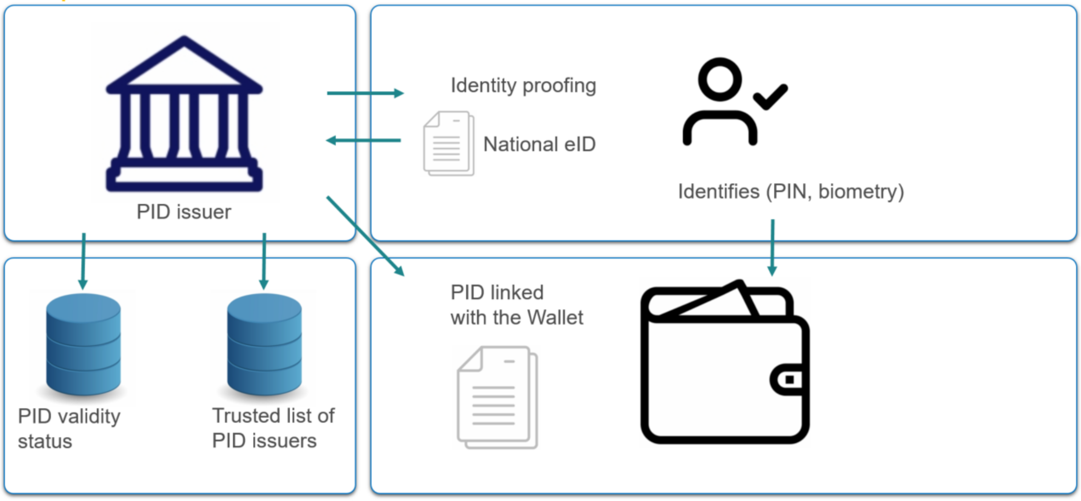

PID issuer
Identity proofing
National eID
Identifies (PIN, biometry)
PID validity status
Trusted list of PID issuers
PID linked with the Wallet

Figure 2: On-boarding to the Wallet

As part of the onboarding process, the eWallets is personalised through an identity proofing process that meets the requirements of Level of Assurance "high". Primarily, existing notified national electronic identity means at Level of Assurance "high" can be expected to be used for that purpose, while other methods may also be used, such as physical appearance or a remote verification method which is part of a certified national eID scheme. As a result of the onboarding process, Person Identification Data is linked to and issued to the eWallet. Personalisation enables eWallet issuers to keep a log of all personalised eWallets, which can be used to enable the invalidation of specific eWallet instances (e.g. in the case of theft).

- Issuance of attestations of attributes

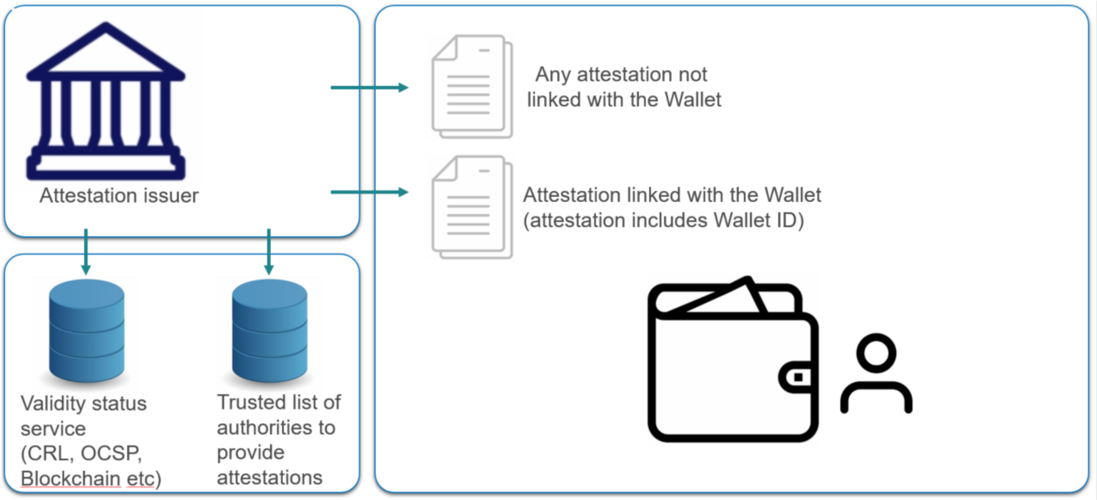

Attestation issuer
Any attestation not linked with the Wallet
Attestation linked with the Wallet (attestation includes Wallet ID)
Validity status service (CRL, OCSP, Blockchain etc)
Trusted list of authorities to provide attestations

Figure 3: Acquiring attestations

The eWallet application is to be able to discover and select, based on users' choice and consent, the issuers (e.g. (Q)EAAPs) of the requested (set of) attestations of attributes.

The user can request PIDs/EAAs from authorized issuers. These may be issued including a unique element (e.g. a public key or a reference to it) of the requesting eWallet (i.e. the user). This links the eWallet, and consequently its holder and other attestations, with the PID/EAA. Later – upon presentation – relying parties can verify that the subject of the attestation and the holder of the eWallet is the same person (e.g. by requesting a proof of possession for the responding private key, taking this as a proof that the presenting party is in fact the holder). Where there is no link between the EAA and the eWallet or other EAAs, additional identification means of the user are required.

- Providing / presenting attestations

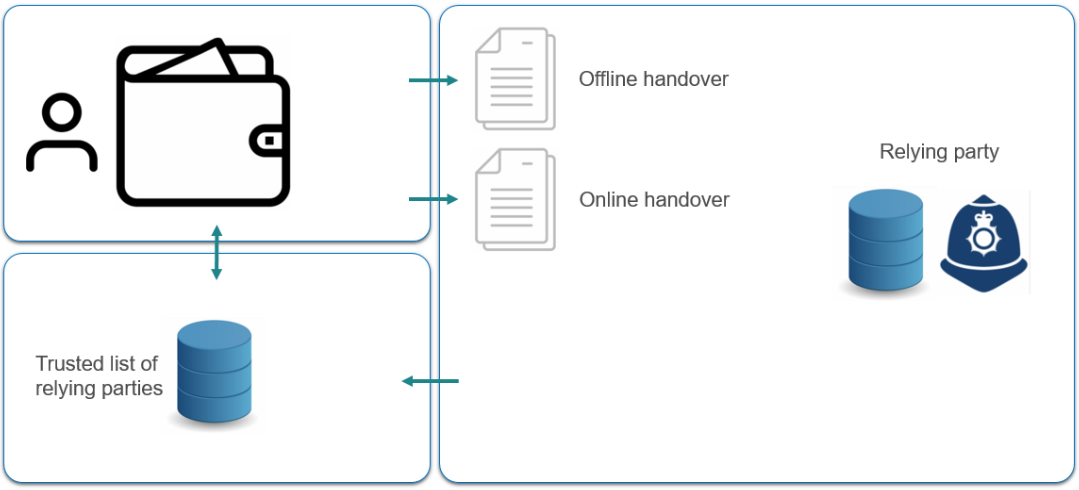


Figure 4: Providing / presenting attestations

Often, service providers make the delivery of a service or product dependent on a user account or on the existence of certain attributes. In many cases, they are legally required to do so. Users can present the relevant proofs by means of PIDs/EAAs stored on their eWallet.

Relying parties providing such services initiate the “handover” of the PIDs/EAAs, for instance by presenting a QR-Code, providing a deep-link or via other methods, prompting the eWallet to ask for the end user’s consent to share the attributes.

When the requested attributes do not exist in the eWallet, they can be discovered and selected with relevant issuers, based on the user’s choice and consent.

Online, the eWallet allows end users, through the PID and (Q)EAAs, to share PIDs/EAAs that are necessary for example for securely allowing access to accounts of authorized identities, or for one-off processes requiring secure user identification. Additionally, the identification process involving such sharing of attestations can be used to link a new authentication token to an existing account, provided that the account is connected to the identity (account recovery).

To protect users online, only requests originating from relying parties that are who they claim to be (and are listed as such) will be processed by the eWallet.

In an offline scenario, eWallets are asked by relying parties to present an attestation in a readable form accompanied by a machine-readable representation transmitted through a presentation protocol (e.g. QR code, Near Field Communication NFC or Bluetooth).

- Authentication of attestations

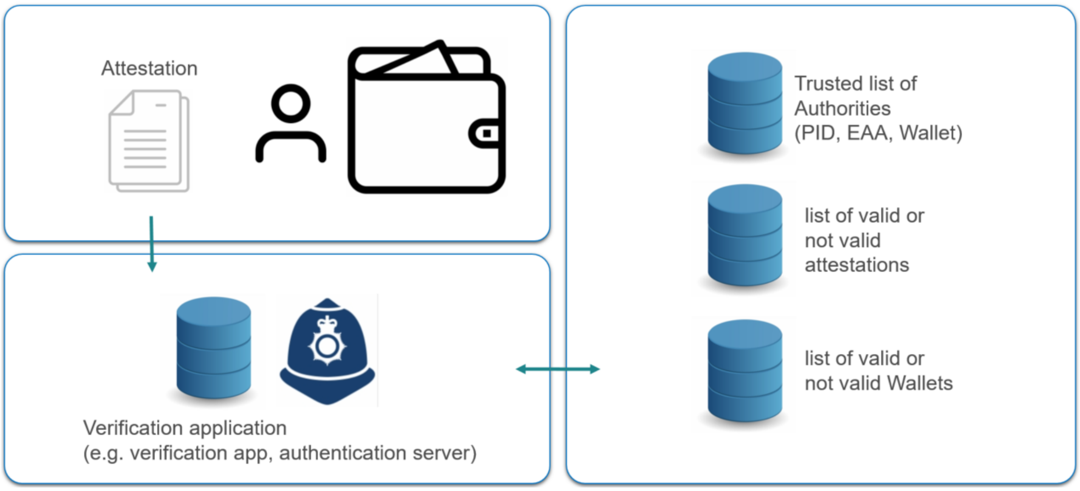


Figure 5: Authentication of attestations

Trust is ensured by the Member State who either issues Personal Identification Data and the Wallet or guarantees their issuance as trust anchor for the relying party. These trust anchors are recorded in trusted lists. Similarly, trust in (Q)EAAs is ensured by the trust in the (Q)EAAP provider and may be verified by means of Member States trusted lists pursuant to Art. 22 of the existing eIDAS Regulation.

QEAAs include cryptographic elements and information that allow the relying party to verify authenticity and authorship in several ways, such as:

- The advanced electronic signature/seal of the issuer of the QEAAs, which may be verified against the corresponding trusted list;
- Information about validity or the location of the validity status service that handles enquiries about validity;
- The public key of the wallet, which may be used to sign presentations of attested attributes from QEAAs, enabling the relying party to verify proof of possession of the corresponding private key and hence authenticate the presentation as originating from the eWallet user. This verification could be carried out directly or by reference.

Validity status services may rely on blacklists (blocklists, revocation lists) or (where possible) whitelists.

- Signing data by means of qualified electronic signatures

The eWallet enables the user to electronically sign data (e.g. files such as contracts) by means of qualified electronic signatures, issued by any qualified provider based on user choice. Third party web sites or apps may be provided with an interface to hand over documents to the eWallet for signing, and receiving back the signed documents in order to provide a seamless user experience.

Electronic signing may be enabled locally by means of private key(s) stored in the device, or remotely by means of activating, after authentication, a signature private key managed on behalf of the user in the context of a remotely managed QSCD. In case of a local QSCD, a qualified certificate for electronic signatures would be issued for the public key(s) used for signing. In case of a remote QSCD, the person identification data and QEAAs would be usable for authentication.

Recovery and restoration processes and functions in case of technical failure or loss of the device would equally be developed.

2.4 ARCHITECTURE FRAMEWORK

At the time of writing, the eIDAS Expert Group is working on the definition of the architecture framework for the eWallet. A first high-level framework was published in September 2021, as shown in the diagram below.

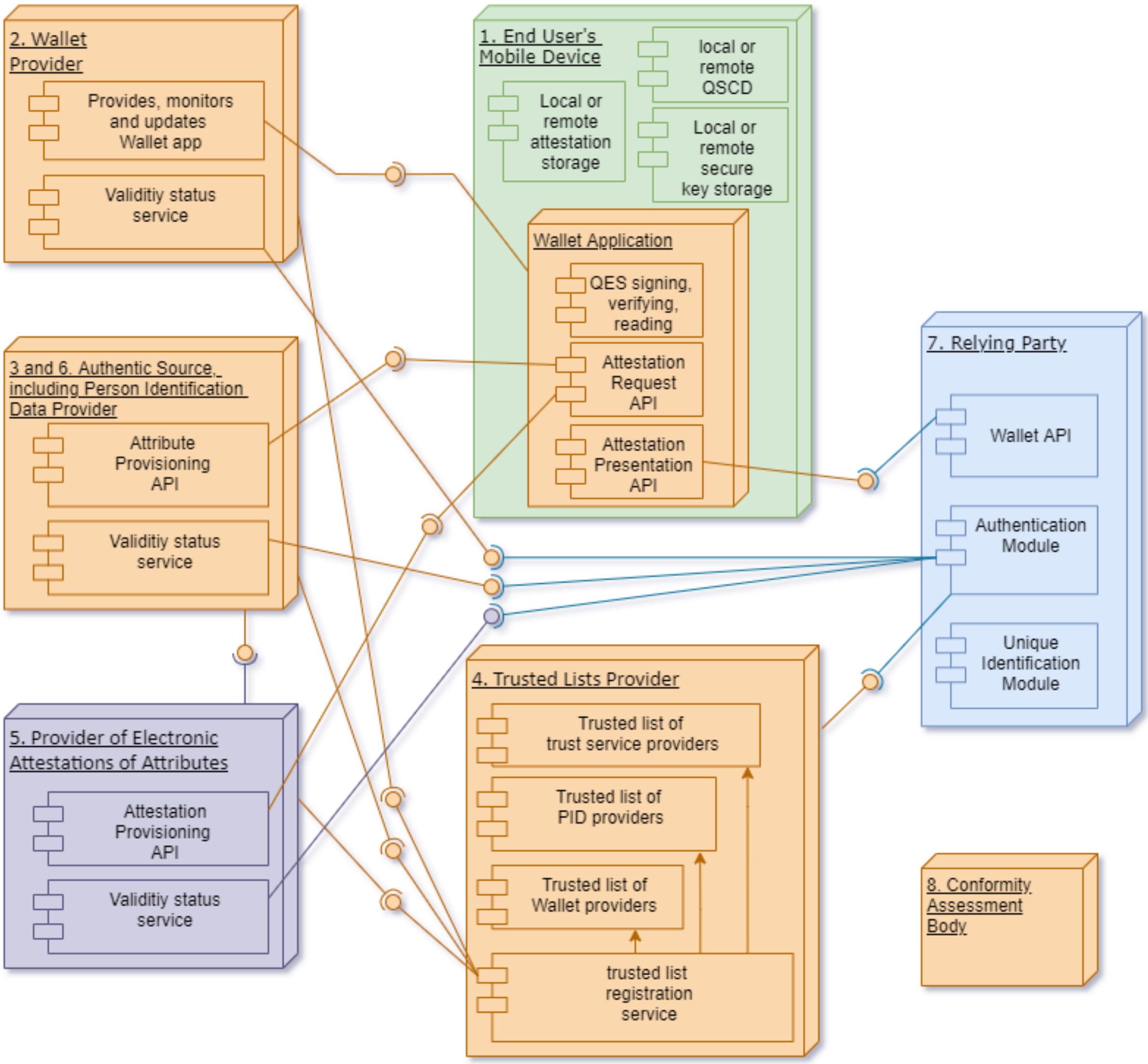

2. Wallet Provider
Provides, monitors and updates Wallet app
Validitiy status service
1. End User's Mobile Device
local or remote QSCD
Local or remote attestation storage
Local or remote secure key storage
Wallet Application
QES signing, verifying, reading
Attestation Request API
Attestation Presentation API
3 and 6. Authentic Source, including Person Identification Data Provider
Attribute Provisioning API
Validitiy status service
7. Relying Party
Wallet API
Authentication Module
Unique Identification Module
5. Provider of Electronic Attestations of Attributes
Attestation Provisioning API
Validitiy status service
4. Trusted Lists Provider
Trusted list of trust service providers
Trusted list of PID providers
Trusted list of Wallet providers
trusted list registration service
8. Conformity Assessment Body

Figure 8. High level architecture model for eWallet ecosystem

This model shows the main functional components and interfaces that actors in the eWallet ecosystem must implement. The technical standards for these components and interfaces are not yet defined by the eIDAS Expert Group. We expect these to become available in the first half of 2022. This implies that in this research we are unable to identify the architectural implications for NRENs in different eWallet roles in more detail.

3 NREN roles

3.1 INTRODUCTION

NRENs today provide identity broker and/or governance services for research and educational institutes and their service providers. Research and education service providers are relying parties for student and staff IDs, attestations and credentials, issued by the institutes as authentic sources and attestation providers. Typically, NRENs act as a broker and/or governance body for this exchange of IDs and attributes in their identity framework.

In this chapter we analyse the impact of eWallets on NRENs and institutes, by assessing six possible eWallet ecosystem roles for NRENs in the EU Digital Identity Wallet ecosystem. For each role, a high-level SWOT is presented.

Our analysis is based on the first drafts of the architecture, roles and processes in the eWallet ecosystem, and emerging concepts for governance of both the eWallet and the ecosystem. These are all still being developed by the eIDAS Expert Group, and therefore subject to change. Final definitions are expected to become available in the first half of 2022.

3.2 NREN AS EWALLET PROVIDER

It can be conceived that NRENs may develop and deploy eWallets for the research and education domain. However, because of eIDAS requirements, there already will be one if not more eWallets made available in each Member State[5]. The amendment of the eIDAS legislation creates a uniform European market of approximately 450 million users for eWallet providers. Therefore, we expect several existing wallet providers to develop into eWallet providers. In fact, some wallet providers are already expanding their footprint to new (geographical) markets today.

Furthermore, it is not inconceivable that tech giants such as Apple and Google will enter this market with certified eWallets. Even though eWallets must be offered for free, a revenue model can be found in the integration of eWallets with other, paid value-added services. These services can (with the user's consent) process data from the user’s eWallet and data from the use of the eWallet for numerous innovative applications. Here, the tech giants have a strong position in many respects. This is reflected in their identity and wallet related initiatives, like the recent agreement between eight US States and Apple to load and present State IDs and digital driver’s licences in the Apple Wallet app. Other recent examples are Google’s launch of the Android Ready SE Alliance, aimed to accelerate the development of secure digital keys (for cars and properties), driver's licences, national ID cards, ePassports and eMoney solutions, including wallets, and Microsoft's Azure AD Verifiable Credentials platform to develop eWallet solutions based on W3C standards.

Due to this guaranteed availability of eWallets in the market, and Member States having to provision at least one generic, standardised eWallet in their markets, a scenario of NRENs developing and providing eWallets was not considered viable or relevant, and thus not analysed in this research.

3.3 NREN AS RELYING PARTY

To comply with eIDAS, educational institutes only have to accept eWallets during student registration, for the verification of an applicant’s ID with Level of Assurance High, i.e. for authentication or electronic identification purposes. Optionally, if entities decide to issue educational attributes (e.g. educational qualifications, titles and licenses) to eWallets, institutes may want to consume and verify such attributes for other student and staff processes. In this scenario, the NREN may consume and verify attributes provided by eWallets on behalf of the receiving educational institutes.

[5] eIDAS amendment Art. 7

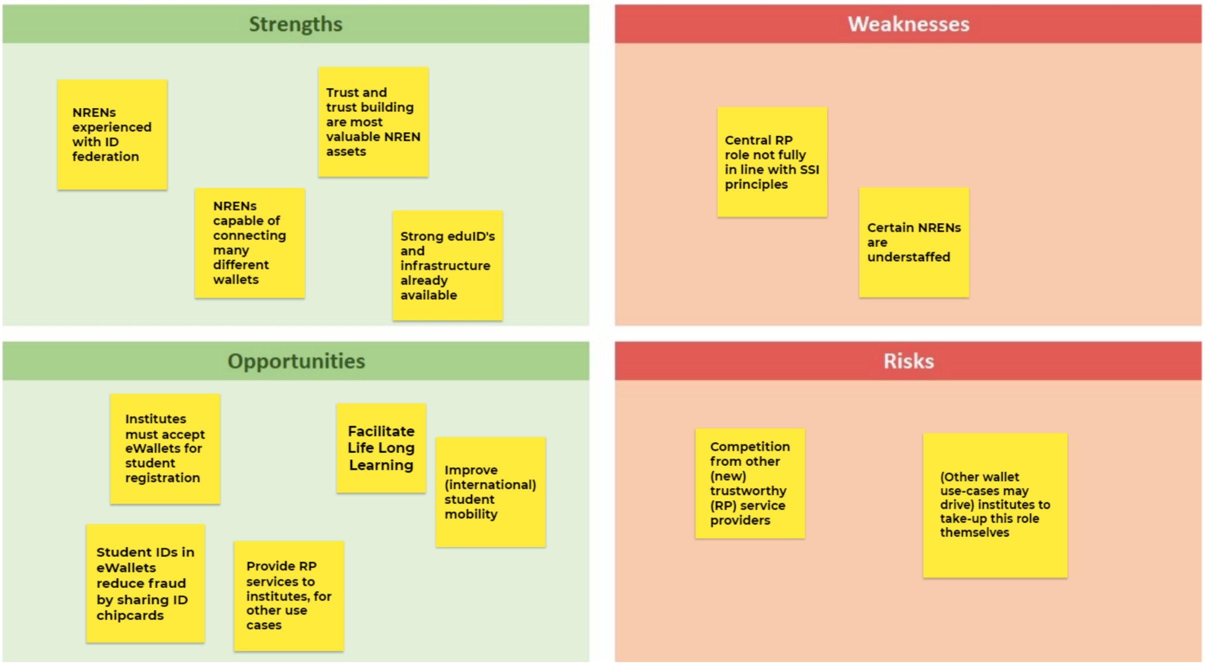

Strengths
NRENs experienced with ID federation
Trust and trust building are most valuable NREN assets
NRENs capable of connecting many different wallets
Strong eduID's and infrastructure already available
Weaknesses
Central RP role not fully in line with SSI principles
Certain NRENs are understaffed
Opportunities
Institutes must accept eWallets for student registration
Facilitate Life Long Learning
Improve (international) student mobility
Student IDs in eWallets reduce fraud by sharing ID chipcards
Provide RP services to institutes, for other use cases
Risks
Competition from other (new) trustworthy (RP) service providers
(Other wallet use-cases may drive) institutes to take-up this role themselves

Figure 9. SWOT for NREN as Relying Party

In this role, the NREN would leverage it's trusted position in the research and education identity framework and it's extensive experience, capabilities and infrastructure required to support the consumption of eWallets.

This enables the NREN to not only support it's member institutes to comply with eIDAS for student registration, but also provides the opportunity to improve identification processes related to (international) student mobility and Lifelong Learning (LLL). Moving student IDs from chipcards to eWallets (i.e. on smartphones) will reduce fraud by students 'sharing' IDs. And, if NREN members need or want to consume eWallets for use cases not specifically tied to student identification, the NREN would be able to provide them with RP services for those use cases.

Some NRENs may have challenges to take up a role as RP due to being understaffed. This is considered a significant weakness. Also, institutes or other stakeholders may consider NRENs in a 'delegated' RP role not fully in line with the SSI principles underlying the European Digital Identity Framework.

Although NRENs are better capable to provide RP services than their member institutes when eIDAS becomes effective, over time the institutes may want to take up this role themselves, driven by the need to consume eWallets for other use cases, for instance for administrative or HR business processes. Another threat for NRENs in an RP role may be competition from other (new) trustworthy RP service providers that may enter the market.

3.4 NREN AS AUTHENTIC SOURCE / ATTESTATION PROVIDER

In this role, the NREN provides educational attributes (educational qualifications, titles, credentials, badges, memberships, licenses etc.) to eWallets, on behalf of the issuing educational institutes. Also, the NREN provides attestations for such attributes to relying parties, for instance other institutes or employers. This role becomes relevant when institutes decide to issue educational attributes to eWallets, for instance to facilitate use cases like (international) student mobility and Lifelong Learning (see chapter 4).

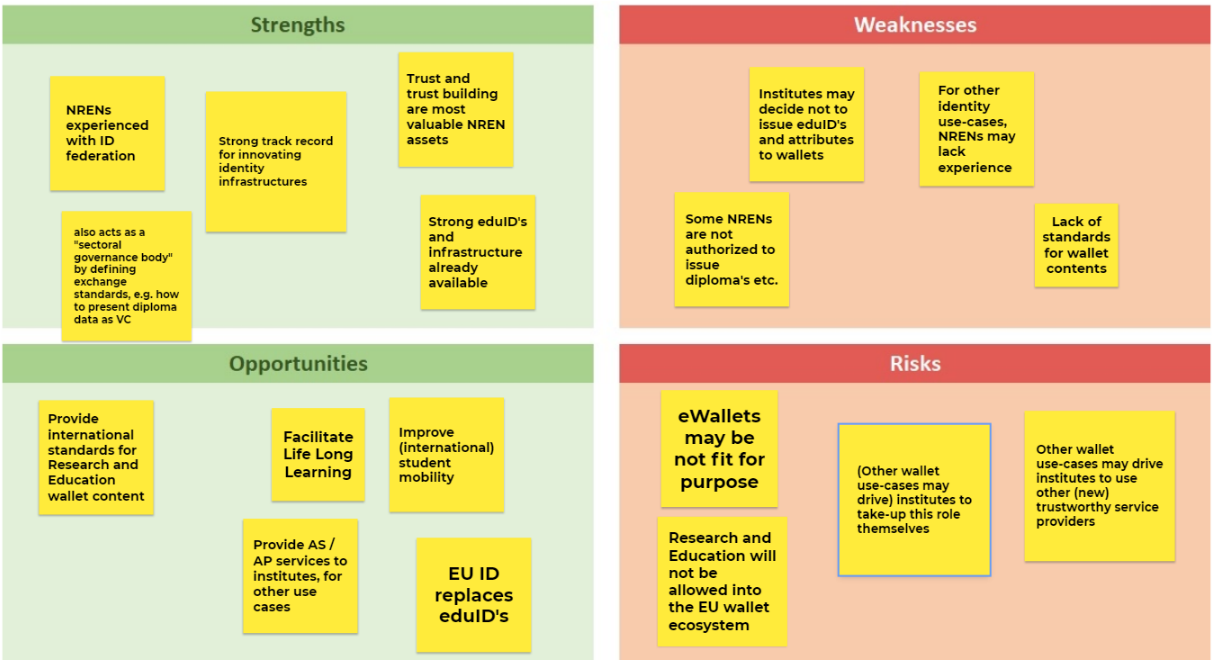

Strengths
NRENs experienced with ID federation
Strong track record for innovating identity infrastructures
Trust and trust building are most valuable NREN assets
also acts as a "sectoral governance body" by defining exchange standards, e.g. how to present diploma data as VC
Strong eduID's and infrastructure already available
Weaknesses
Institutes may decide not to issue eduID's and attributes to wallets
For other identity use-cases, NRENs may lack experience
Some NRENs are not authorized to issue diploma's etc.
Lack of standards for wallet contents
Opportunities
Provide international standards for Research and Education wallet content
Facilitate Life Long Learning
Improve (international) student mobility
Provide AS / AP services to institutes, for other use cases
EU ID replaces eduID's
Risks
eWallets may be not fit for purpose
(Other wallet use-cases may drive) institutes to take-up this role themselves
Other wallet use-cases may drive institutes to use other (new) trustworthy service providers
Research and Education will not be allowed into the EU wallet ecosystem

Figure 10. SWOT for NREN as Authentic Source / Attestation Provider

As (delegated) AS/EAAP, the NREN would leverage its trusted position in the research and education identity framework and its extensive experience, capabilities and infrastructure. Also, NRENs have a strong track record for innovating identity frameworks.

This enables the NREN to support its member institutes to improve identification and attestation processes, for instance related to (international) student mobility and Life Long Learning (LLL). Additionaly, the NREN would be able to provide AS / EAAP services for other use cases.

Weaknesses that may hinder NRENs taking up this role are a lack of staff and the fact that in several Member States NRENs are not formally authorized to issue credentials like diplomas. Also, the role is very much dependent on institutes' ambitions to use eWallets for improving identification and attestation processes, and the availability of standards for the related educational attributes.

Some NRENs raised concerns as to the eWallets 'fitness for use' in the research and education domain. Some mentioned the possibility that research and education are not allowed to use eWallets for various processes and applications. However, NRENs are well positioned to contribute to the development of international standards for educational attributes, for instance by mediating between W3C and the institutions on standardization of educational attribute semantics. Here, GÉANT could act as a collaboration and governance platform for such standardizations, thus ensuring the eWallets usability for all kinds of ID-related processes in research and education.

3.5 NREN AS WALLET PROXY

In this role, the NREN handles EU wallets for the educational and research institutes, to allow them to continue using their existing identity frameworks whilst supporting EU wallets. In fact, this role combines the roles of Relying Party and Authentic Source.

The diagram shows the steps that are taken when a user wants to use his eWallet to access a service in a Research and Education (R&E) Identity Framework that does not (yet) support eWallets.

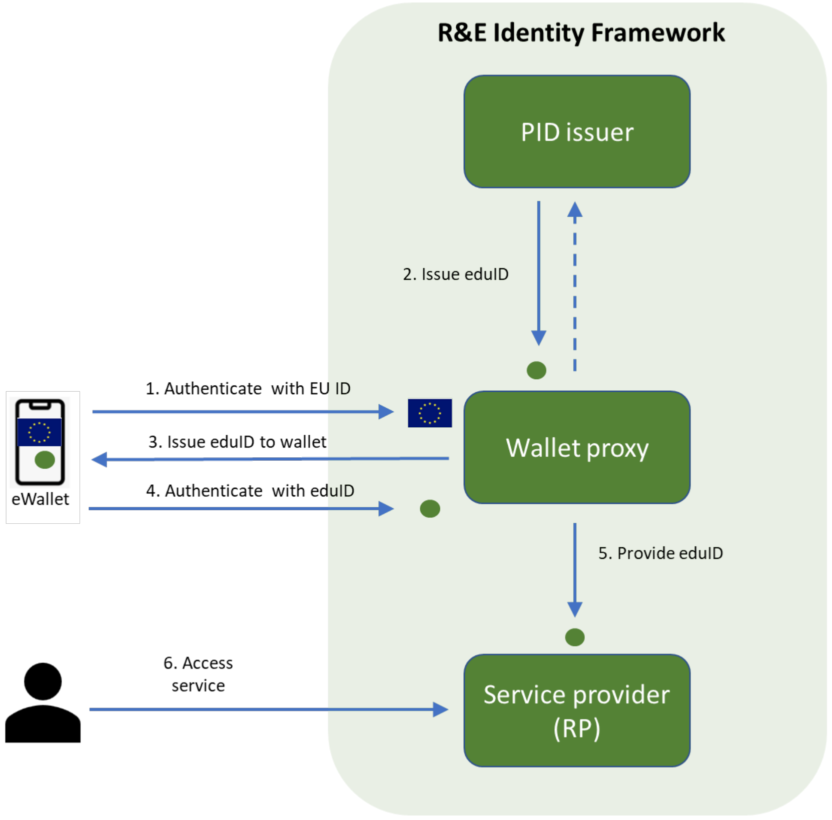


Figure 11. eWallet onboarding in R&E Identity Framework

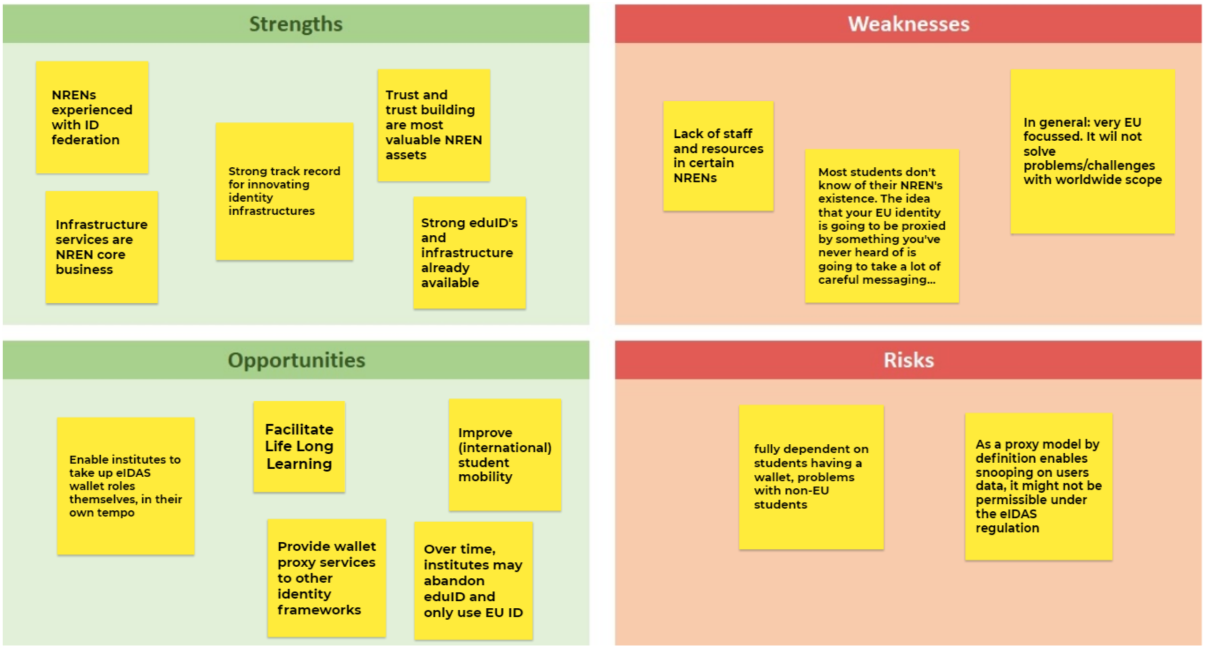
The first time the user logs in, he identifies himself with his EU ID at the Wallet Proxy of the R&E Identity Framework (1). The Wallet Proxy is included as RP (trusting party) in the eWallet ecosystem and authenticates the user using the EU ID. The Wallet Proxy then sends a signal to the PID issuer of the R&E Identity Framework, which causes the PID issuer to issue an eduID to the eWallet (2, 3), after which the eWallet provides this ID to the Wallet Proxy (4). The Wallet Proxy then passes on the eduID to the service provider (5) who, based on this ID, grants access to the user (6).

Every next time the user requests access, both his EU ID and eduID are provided to the Wallet Proxy. Over time, as service providers start supporting EU IDs themselves, the Wallet Proxy will only forward the EU ID to the receiving service provider. As service providers over time choose to support eWallets themselves, both the Wallet Proxy and PID Issuer roles may no longer be required. In due time the EU ID may replace the eduID entirely.

This eWallet bootstrap concept was presented to the eIDAS Expert Group for inclusion in the Toolbox[6], with the objective to facilitate the transition of existing national eIDs to the eWallet ecosystem. It is not yet clear if the eWallet proxy concept will be included in the Toolbox, and if the concept will be allowed for bootstrapping other (sectoral) identity frameworks to the eWallet.

[6] Bootstrapping identity wallet authentication with national eIDs, Agency for Digitisation, Denmark

Whilst providing an elegant mechanism to transition from existing national and sectoral Identity Frameworks and infrastructures to the eWallet ecosystem, allowing institutes to use eWallets to facilitate Lifelong Learning and to improve student and staff mobility, the proxy model requires further elaboration to overcome challenges regarding privacy and service availability issues.



Strengths

NRENs experienced with ID federation

Infrastructure services are NREN core business

Strong track record for innovating identity infrastructures

Trust and trust building are most valuable NREN assets

Strong eduID's and infrastructure already available

Weaknesses

Lack of staff and resources in certain NRENs

Most students don't know of their NREN's existence. The idea that your EU identity is going to be proxied by something you've never heard of is going to take a lot of careful messaging...

In general: very EU focussed. It wil not solve problems/challenges with worldwide scope

Opportunities

Enable institutes to take up eIDAS wallet roles themselves, in their own tempo

Facilitate Life Long Learning

Improve (international) student mobility

Provide wallet proxy services to other identity frameworks

Over time, institutes may abandon eduID and only use EU ID

Risks

fully dependent on students having a wallet, problems with non-EU students

As a proxy model by definition enables snooping on users data, it might not be permissible under the eIDAS regulation

Figure 12. SWOT for NREN as Wallet Proxy

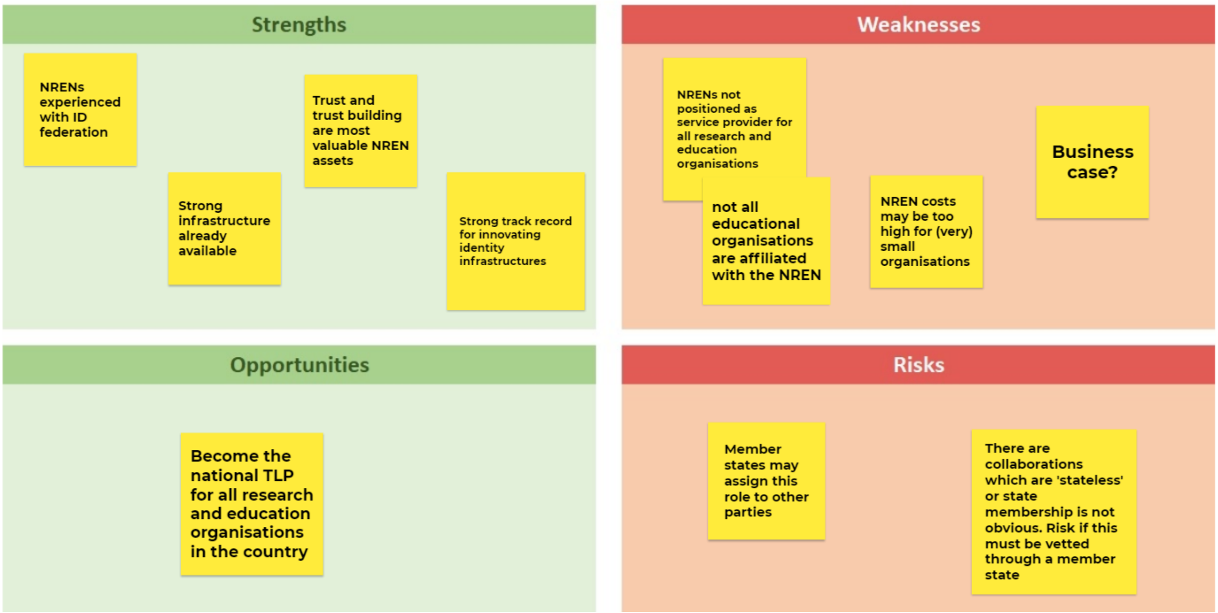
If Wallet Proxies are supported by eIDAS, NRENs would be able to leverage their strengths mentioned in the previous SWOTs to help their member institutes and partners to gracefully transition to eWallets, in line with user acceptance and market penetration of eWallets in general. Obviously, this will not solve identity related issues with non-EU students and institutions, which is considered a weakness of the concept by some.

The Wallet Proxy scenario touches upon the possible replacement over time of sectoral IDs by EU IDs as provided in eWallets. Even though eIDAS stipulates that in addition to eWallets, alternative means of identification and attestation must be supported by relying parties[7], eWallets and EU IDs may become the preferred identity solution for both users and organisations. This would mean the focus of institutions could shift from identity provisioning (IDP) to attribute and credential provisioning (f.i. micro-credentials such as EduBadges). As mentioned in the previous section, NRENs are well positioned to contribute to the development of international standards for such educational attributes. Also, they may find there is a role to play as a broker or aggregator for service providers (relying parties) that do not (yet) support new standards for research and educational attributes.

[7] eIDAS amendment Recital 28

3.6 NREN AS TRUSTED LISTS PROVIDER

In this role, the NREN provides trusted lists containing all entities that are verified Authentic Sources, Electronic Attestation of Attributes Providers and/or Relying Parties in the research and education domain.



Strengths

NRENs experienced with ID federation

Trust and trust building are most valuable NREN assets

Strong infrastructure already available

Strong track record for innovating identity infrastructures

Weaknesses

NRENs not positioned as service provider for all research and education organisations

not all educational organisations are affiliated with the NREN

NREN costs may be too high for (very) small organisations

Business case?

Opportunities

Become the national TLP for all research and education organisations in the country

Risks

Member states may assign this role to other parties

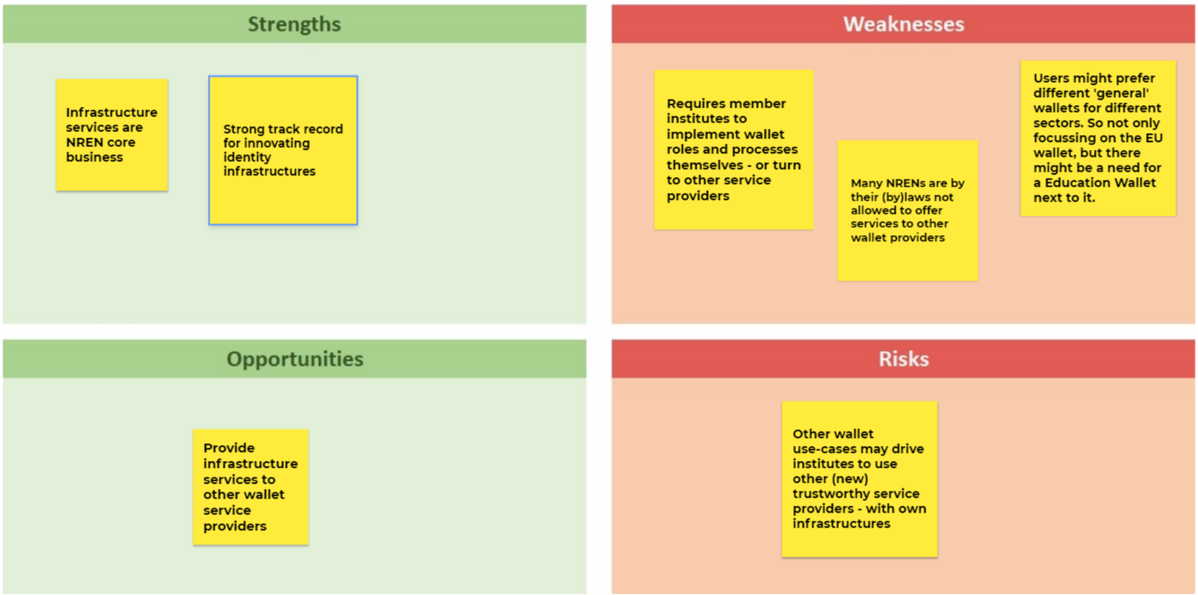
There are collaborations which are 'stateless' or state membership is not obvious. Risk if this must be vetted through a member state

Figure 13. SWOT for NREN as Trusted Lists Provider

This would allow NRENs to leverage their strengths to become the national TLP for all research and education organisations in a Member State. However, it is still very unclear what the business case would look like, and whether NRENs are able to provide TLP services at acceptable or even competitive costs to organisations large and (very) small. Another challenge may be the fact that today, not all national research and education organisations are member of a NREN. Finally, not every NREN is formally recognized by their national government; hence Member States may assign TLP roles to other (public) parties.

3.7 NREN AS INFRASTRUCTURE PROVIDER

In this role, the NREN provides eIDAS infrastructure services to educational and research institutes. This means the NREN has no eIDAS process role; these are taken up by the institutes and third parties.



Strengths

Infrastructure services are NREN core business

Strong track record for innovating identity infrastructures

Weaknesses

Requires member institutes to implement wallet roles and processes themselves - or turn to other service providers

Many NRENs are by their (by)laws not allowed to offer services to other wallet providers

Users might prefer different 'general' wallets for different sectors. So not only focussing on the EU wallet, but there might be a need for a Education Wallet next to it.

Opportunities

Provide infrastructure services to other wallet service providers

Risks

Other wallet use-cases may drive institutes to use other (new) trustworthy service providers - with own infrastructures

Figure 14. SWOT for NREN as infrastructure provider

Infrastructure services are NREN core business, and NRENs have a strong track record for innovating identity infrastructures. Providing such services to various wallet service providers in the research and education domain may allow NRENs to increase their economies-of-scale, effectively reducing costs for their members.

However, leaving member institutes to implement wallet roles and processes themselves – or turn to third parties to do this for them – may be considered undesirable. Also, other wallet use cases may drive institutes to use other (new) trustworthy wallet service providers – with own infrastructures. This could over time erode the added value trust and identity services NRENs provide today.

4 NREN identity initiatives

In this chapter we provide an overview of the main NREN initiatives with respect to digital identity. We look at the relationship with the eWallet and reflect on the potential impact of the eWallet on these initiatives.

4.1 IDENTITY MANAGEMENT

One of the main objectives of the eWallet is providing reliable digital identities for all citizens in the European Union. Historically NRENs have been very active in the field of identity and access management. Often by providing infrastructures and services for identity federation networks. Another important use case supported by NRENs is the registration of new students. The impact of the eWallet on these Identity and Access Management (IAM) initiatives is discussed below.

Identity federations

NREN have been managing and providing infrastructure for (national) identity federations for years. Classically each research and education institution would be an identity provider within these federations. Users would get an account for each institute where they are working or studying. Although identity federations allow for mutual recognitions between institutes of each other's identities, in practice this is often not well organised. This results in employers and students having to manage digital identities for each institute they are involved with. To tackle the challenges of managing multiple identities some NRENs introduced an eduID. Although implementations and maturity differ from country to country, the main objective is the same: a user-centric digital identity that can be used at all institutes in a country.

The concept of an eduID has clear similarities with the eWallet. A digital identity that is yours and that you can use anywhere anytime. It can easily be imagined that in the future the eduID would be incorporated into the eWallet. Instead of managing identities itself, institutions or NRENs could issue an eduID credential to the eWallet that can be used to access services of research and educations institutes. However, the use of eWallets may not be enforced when there is no legal basis for strong user authentication. As identity management at education and research institutes is often not based on such legal basis, the acceptance and use of the eWallet may only be optional for the end-user. The implication is that there must remain another means for end users to identify themselves, for example the already existing identity federations or initiatives such as eduID.

This means that the eWallet will not fully replace the current identity federations nor initiatives such as eduID. Moreover, when there is no legal obligation for strong user authentication, there is also no obligation for institutes to accept the eWallet. However, acceptance of eWallets will benefit the end-user, for instance in situations where he now needs to manage a digital identity for each institute he is related to. These use cases are also addressed in sections 4.3, 4.4 and 4.5.

Student registration

Another use case in the identity domain is the registration of new students. Although students sign up for a specific education at a specific institute, the registration of new students may be organised at national level. An example is Studielink, where students can sign up for studies within the Netherlands. These use cases often have a legal obligation for strong user authentication and so must accept the eWallet. On the other side the use of the eWallet may also simplify the registration of foreign students as there will be a reliable digital identity available for most of the students. Whether the acceptance of the eWallet for student registration will impact the NRENs and educational institutions will differ from country to country. In some countries NRENs are appointed to facilitate this process, in other countries there are other (government) organisations in place and in some cases universities themselves facilitate this process. Considering the legal basis for strong user-authentication when registering students, this means these organisations should prepare themselves to accept the wallet.

4.2 VERIFIABLE CREDENTIALS

Electronic attestations of attributes (EAAs) are sets of attributes regarding an individual or organisation. They are designed in such a way that the content and origin of the attributes can be verified by the relying party. Outside of the scope of eIDAS, EAAs are often referred to as verifiable credentials (VCs). There are already multiple projects focussing on the application of verifiable credentials within education. The most prominent ones are discussed below.

Diplomas

Multiple countries already provide digital versions of diplomas. Often these are handed out as digitally signed PDFs. Although easy to use for people, PDFs cannot easily be processed by machines and are unsuitable for the eWallet. Diplomas are mentioned as one of the important EAAs within the eWallet context. It makes it easier for both institutes and employers to check the authenticity and validity of diplomas through the whole European Union. Although the potential of this use case is recognised, there are no live implementations to issue diplomas as VCs yet. It would make sense to start issuing diplomas as EAAs. However, it is yet unclear who should be responsible. The role of the NREN in issuing diplomas as EAA will differ from country to country. Where the NREN is part of the ministry of education, the NREN might be appointed to hand out the EAAs. However, there are also countries where the NREN is not part of a governmental organisation. In this case the NREN is not in the natural position to hand out EAAs. Institutes might decide or be appointed to hand out the diplomas as EAAs themselves. In that case the NREN is in a natural position to provide infrastructure to support this process.

Micro-credentialing

A relatively new development is micro-credentialing. Instead of only handing out diplomas after finishing a complete study program, micro-credentialing focusses on recognising minor achievement such as finishing a course or acquiring a certain skill. Micro-credentials can support both the use case of student mobility where a student wants to follow courses at different institutes and lifelong learning, where a student wants to gain extra knowledge or skills, but has no need for following a complete study.

One of the examples of micro-credentialing is EduBadges[8], which is built on top of OpenBadges. In this case SURF provides the infrastructure for EduBadges. Institutes can connect to EduBadges and start issuing micro-credentials to students. Even more then with diplomas institutes are in the national position to issue micro-credentials. After that the EduBadges has been issued to the student, he can share it with his own institute or (future) employer. Right now the student collects all his EduBadges in a dedicated EduBadges account/wallet. However, it would make sense to also issue these to the eWallet. NRENs can take a role to support this process.

Europass

As of 2005, the Europass initiative provides a portal for users to create and maintain documents such as a curriculum vitae (with motivation letter), a language passport or any other document bringing evidence of skills and qualifications (copies of degrees, work certificates, etc.) or other types of certificates of learning achievements. They are multilingual and signed with a unique electronic seal. This allows education and training institutions to easily authenticate, validate and recognise credentials of any size, shape or form.

A problem is the difference in legal status of paper documents versus digital documents. As a result, a paper diploma is not easy to reproduce digitally (f.i. due to GDPR requirements). Also, since Europass uses electronic seals, institutions need a secure data center with special HW to process Europass documents. Or have users work with USB tokens – which is not scalable. For most if not all educational institutions the Europass solution is therefore too complex and expensive to be used.

Provisioning of Europass attributes and credentials via eWallets may be challenging because the Europass data model is very complex. And as the Toolbox is still under development, it is unclear if and how eWallet eSeal functionality can be used to support Europass seals.

[8] https://www.surf.nl/en/edubadges-issuing-digital-certificates-to-students

4.3 STUDENT AND STAFF MOBILITY

The last decades study programmes have been relatively strict. Except for minors, there is little room for students to choose their own path within their study program. Student mobility is a development which aims to give the student more freedom over his own study program by enabling students to easily follow courses at multiple institutes in different countries. Currently institutes face many challenges when they want to enable student mobility. These challenges include student registration, and handing out grades and exchanging these between institutes. Students also face challenges regarding handing multiple accounts for the different institutes.

As described in the sections student registration and micro-credentialing there are possibilities to use the EU identity wallet to support student mobility. The student registration process can be eased by enabling the use of the EU identity wallet. For students, the handling of multiple accounts can be eased by allowing the use of the EU identity wallet within the existing identity federations. Although the use of the identity wallet should stay optional, here the NRENs can ease the process and experience of the students. There may also be possibilities to use the student registration process to register the home institute of students and so ease the exchange of grades.

Mobility issues also exist for staff and researchers working for several institutions at the same time, or taking up temporary (guest) roles at various institutions. Getting temporary access to institute accounts and resources typically involves complex identification and onboarding processes, which could benefit from being able to store and present all required IDs and related attributes with an eWallet.

Although eWallets may solve current mobility challenges, it should be kept in mind that these challenges are not all technical. For example, financial issues like how much visiting institutes should be paid also limit the development of student and staff mobility.

4.4 LIFELONG LEARNING

Lifelong learning is a development focussing on the support of individuals during their whole learning life. It assumes that people do not stop learning after receiving a diploma from an institute. Rather people keep developing after graduating. They gain new skills during work, and may also return to institutes to gain new knowledge and skills. When returning to an institute they face multiple challenges. First, they need to be (re)identified. Earlier institute accounts may have been deleted since the last time they were studying at an institute, or the person may have forgotten the password of the account he has not used for multiple years. These challenges might be solved by using an eduID. Here the issuing of an eduID to the EU wallet as described in section 4.1 can ease the challenges that user might face with remembering passwords and handling multiple accounts at different institutions. After finishing a course or when a new skill is acquired these can be recognised by handing out a verified credential, such as an EduBadge. This makes it both easy for the user to collect all his skill credentials and for the receiving party to verify the authenticity of achieved diplomas and skills.

4.5 RESEARCH COLLABORATIONS

Many international research initiatives are global by nature. For instance, CERN, the European Organization for Nuclear Research, consists of some 10.000 researchers from more than 170 institutes based in 53 countries. Researchers participating in such international research networks need global IDs. Such IDs are typically issued by member institutes in the form of person centric IDs signed with PKI certificates.

In the academic research domain, trust is already well organized. Many of these trust concepts are applied to the identity assurance framework. Hence there is no need for external audits and compliance declarations. However, a challenge is the fact that PKI is not very user friendly. Another challenge is the fact that in research networks, IDs are issued by the institutes but the research collaboration teams are responsible for correct IAM, traceability and control of resource usage by researchers. This poses liability issues for institutes.

Applying SSI based solutions, such as the eWallet, for international research collaborations brings many questions to the table that require further research and/or may be answered as the eWallet Toolbox is developed. For instance, how can eWallets be used outside of the EU? Even in countries that are not officially recognised by the EU? And how to use eWallets to grant access to research resources that typically have non-interactive interfaces and command line interfaces? How to deal with the lack of standardization in research resource user authentication mechanisms?

5 Conclusions

5.1 IMPACT OF EWALLETS ON NRENS AND PROVIDERS OF CREDENTIALS

In this section, we answer the research question:

How does the EU Digital Identity Wallet ecosystem impact the role of NRENs and providers of credentials?

The proposed eIDAS amendment requires educational institutes to accept eWallets for student registration processes with LoA High. This means institutes must take up the role of Relying Party in the eWallet ecosystem. They must be able to initiate the ‘’handover” of the applicant’s PID from his eWallet and to process the PID once transferred from the eWallet. Also, eIDAS requires all RPs to be registered as such by their Member States. This may involve a certain assessment of RPs to ensure they comply with the technical architecture, standards, references, guidelines and best practices as defined in the Toolbox.

Institutes may delegate the implementation and execution of eWallet Relying Party infrastructure and processes to their NRENs, much like they delegate trust and identity infrastructure and processes to NRENs today. As described, NRENs are well positioned to take up the role of RP, although certain NRENs may be challenged to provide the required resources to do so. Some concerns exist regarding institutes delegating the RP role to their NREN because this introduces a single point of failure in the eWallet processes and increases the risk of NRENs snooping on the information exchanged via eWallets. We expect NRENs to be able to leverage their strong capabilities and assets to manage these risks reliably and transparently and thus become highly trusted RPs.

Institutes can decide to take things a step further, and use eWallets to facilitate the use cases and initiatives as described in chapter 4. This requires they take up the role of Authentic Source and Attestation Provider in the eWallet ecosystem. These eWallet roles require institutes to implement more complex eWallet processes and infrastructures to issue and consume attributes, attestations and credentials. Again, NRENs are well positioned to take up these roles for their member institutes. However, international standards for eWallet research and education content are still lacking. NRENs can drive the development of such standards and, through GÉANT, act as a sectoral governance body for these standards.

If NRENs combine the roles of Relying Party and Authentic Source they can act as a so-called Wallet Proxy. In this role, the NREN handles eWallets for the educational and research institutes, at the same time allowing them to continue using their existing identity frameworks and eduIDs. Thus, the NREN acts as an intermediary between eWallets and the eduIDs. Over time, as service providers start supporting EU IDs themselves, the EU ID may replace the edu ID entirely. Also, as service providers over time choose to support eWallets themselves, both the Wallet Proxy and edu PID Issuer roles will no longer be required. It is not yet clear if the eWallet proxy concept will be included in the Toolbox, and if the concept will be allowed for bootstrapping research and education identity frameworks to the eWallet.

We conclude that NRENs are less likely to be able to take up a role as eWallet Trusted List Providers. It is expected that Member States will designate this role to other (public) entities. Also, NRENs are typically not set-up and accepted as a service provider to *all* research and educational organisations in a country, large and small.

Even if NRENs do not take up a role in the eWallet ecosystem, they may provide eIDAS infrastructure services to educational and research institutes, or possibly even other actors in the eWallet ecosystem. Infrastructure services are NREN core business, and NRENs have a strong track record for innovating identity infrastructures. Providing such services may allow NRENs to increase their economies-of-scale, effectively reducing costs for their members. However, leaving member institutes to implement wallet roles and processes themselves – or turn to third parties to do this for them – may be considered undesirable. Also, other wallet use cases may drive institutes to use other (new) trustworthy wallet service providers – with own infrastructures. This could over time erode the added value of the trust and identity services NRENs provide today.

For institutes, not assigning eWallet ecosystem roles to NRENs (i.e. to themselves or to (new) third parties instead) seem less viable, at least in the short to mid-term. This may change as the eWallet ecosystem develops and if eWallets become the primary means for all kinds of identity related use cases in the EU. As a result, the focus of institutions could shift from identity provisioning (IDP) to attribute and credential provisioning (f.i. micro-credentials such as EduBadges). NRENs are well positioned to contribute to the development of required international standards for educational attributes. Also, they may find there is a role to play as a broker or aggregator for service providers (relying parties) that do not (yet) support new standards for research and educational attributes.

The amendment of the eIDAS legislation creates a uniform European market of approximately 450 million users for eWallet providers. It is not inconceivable that tech giants such as Apple and Google will enter this market with certified eWallets. Aside from the tech giants, existing wallet providers are likely to develop into eWallet providers. But even if tech giants and wallet providers do not bring a single eWallet solution to the market, Member States must provide an eWallet for all inhabitants. Due to this expected availability of eWallets in the market, a scenario of NRENs developing and providing eWallets is not considered viable or relevant.

5.2 EWALLETS AND NREN INITIATIVES

In this section, we answer the research question:

How can existing NREN initiatives be leveraged to support the EU Digital Identity Wallets?

As mentioned in the previous section, eWallets must be supported as identification means during the registration of new students. In addition, the following use cases are expected to benefit from the application of eWallets:

- eWallets can carry verifiable credentials, such as diplomas, micro-credentials and other education and skills related documents (CVs, language passports, copies of degrees, work certificates, etc.). This allows education and training institutions as well as employers to easily authenticate, validate and recognise credentials of any size, shape or form. Promising candidates to issue to eWallets are diplomas and EduBadges. However, institutes and NRENS must deal with national differences in their legal responsibilities and options for issuing such credentials.

- eWallets provide opportunities to solve several issues and challenges related to (international) student and staff mobility. These challenges include student registration at foreign institutes, and handing out grades and exchanging these between institutes. Students also face challenges regarding handing multiple accounts for the different institutes. The student registration process can be eased by enabling the use of the EU identity wallet. For students, the handling of multiple accounts can be eased by allowing the use of the EU identity wallet within the existing identity federations. Although the use of eWallets is optional, NRENs can improve the processes and services for students.

- Mobility issues exist for staff and researchers working for several institutions at the same time, or taking up temporary (guest) roles at various institutions. Getting temporary access to institute accounts and resources typically involves complex identification and onboarding processes, which could benefit from being able to store and present all required IDs and related attributes with an eWallet.

- For lifelong learning, eWallets can be used to carry and present identification attributes and knowledge and skill credentials when returning to institutes for further education, simplifying onboarding and attestation processes.

- Finally, in the international research domain, the role and value of eWallets is still unclear. Here, eWallets bring many questions to the table that require further research and/or may be answered as the eWallet Toolbox is being developed. For instance, how can eWallets be used outside of the EU? Even in countries that are not officially recognised by the EU? And how to use eWallets to grant access to research resources that typically have non-interactive interfaces and command line interfaces? How to deal with the lack of standardization in research resource user authentication mechanisms?

5.3 ROLE OF GÉANT

In this section, we answer the research question:

Is there a coordinating or supporting role to be played by GÉANT in this development?

Depending on the ambitions of institutes and NRENs to apply eWallets for improving use cases around (international) student mobility and Lifelong Learning, GÉANT can support the development of the required eWallet research and educational content standards and act as a sectoral governance body for these standards.

Due to the possible significant changes eWallets may bring to the 'trust and identity' markets, we advise both institutes and NRENs to actively assess eWallet developments, not only in the research and education domain but in the market in general, and adapt the strategies for their trust and identity frameworks accordingly. GÉANT is well positioned to facilitate this through market research, eWallet technology assessments, market consultations for eWallet solutions and services, and providing a strong liaison with EC identity initiatives such as the Toolbox development.

5.4 FURTHER RECOMMENDATIONS

- NRENs are advised to closely monitor the Toolbox deliverables to understand the functional and organisational preparations required to work with the EU Digital Identity Wallets.

- NRENS are advised to collaborate with governments and private parties to assess how eWallets can be used to innovate identity related processes and develop new services in the realm of education, employability and skills. In this context, we suggest they monitor and possibly participate in initiatives around the development of the EU Skills Open Data Space, which may provide new eWallet use cases for research and education.

Appendix 1 – Research participants

The following persons participated in our research:

Participant	Organisation	Interview	Expert meeting
Christoph Graf	SWITCH	X	X
David Groep	NIKHEF	X	X
Frans Ward	SURF	X	X
Janina van Hees	Euroteq	X	X
Klaas Wierenga	GÉANT	X	X
Michael Linden	Elixir	X	X
Robert Ott	SWITCH	X	X
Bart Kerver	SURF/Innovantes	X	
Leif Johansson	Sunet	X	
Andrew Cormack	JISC		X
Arnout Terpstra	SURF		X
Esmeralda Pires	FCCN		X
Halil Adem	GRNET		X
Jon Shamah	EEMA		X
Jose Manuel Macias Luna	RedIRIS		X
Maarten Kremers	SURF		X
Michael Schmidt	GÉANT		X
Michiel Schok	SURF		X
Niels van Dijk	SURF		X
Peter Clijsters	SURF		X
Victoriano Giralt	GÉANT / University of Malaga		X
Zenon Mousmoulas	GRNET		X