



Nordic Council  
of Ministers

# IDENTITY MATCHING IN THE NORDIC BALTIC-REGION

# Contents

Cover letter	4
1. Introduction	6
2. AS-IS	10
2.1 Description of requirements	10
2.1.1 eIDAS – electronic IDentification, Authentication and trust Services	11
2.1.2 SDGR – Single Digital Gateway Regulation	13
2.1.3 OOP – Once Only Principle	15
2.2 Technological readiness	16
2.2.1 Data required for identity and record matching	16
2.2.2 An analysis and discussion of the availability and machine-readability	27
2.2.3 Description of identity matching in the Once only technical system	28
2.3 A state of play of processes and solutions for identity and record matching in the EU/EEA.	31
2.3.1 Processes and best practices for identity and record matching in EU/EEA countries	32
2.3.2 Summary of Issues and best practices	59
2.3.3 Identity and record matching processes and sub-processes	62
2.4 Common issues and difficulties	71
2.4.1 Description of the structural difficulties in Nordic-Baltic countries	71
2.4.2 Overview of data's quality and trustworthiness in the Nordic-Baltic region	90
2.4.3 Joint difficulties to tackle in collaboration	92

2.4.4 Summary of common issues and input to solutions	96
<b>3. TO-BE</b>	<b>100</b>
3.1 Overview of possible solutions	100
3.2 Description of highest potential solutions	107
3.2.1 eIDASNode+	107
3.2.2 Easy_EAA	114
3.2.3 QuickFix	120
3.2.4 Hard_EAA	126
3.3 Suggestions for Nordic-Baltic region	131
3.4 Suggestions for Member States	138
<b>Summary</b>	<b>142</b>
<b>4. Appendixes</b>	<b>146</b>
4.1 Terms and abbreviations	146
4.2 Methodological approach	151
METHODODOLOGICAL PRINCIPLES	153
4.3 Sources	154
4.4 Participants in workshops and interviews	161
4.5 Aspects analyzed per country	163
<b>About this publication</b>	<b>164</b>

This publication is also available online in a web-accessible version at:  
<https://pub.norden.org/temanord2024-511>

# Cover letter

The Nordic and Baltic region represents some of the most digitally advanced societies in the world. An enabling element for this is the availability and vast adoption of electronic identity (eID) means, both among citizens and service providers. This report is part of a mutual effort that was initiated by the Cross Border Digital Services (CBDS) Programme and the Nordic-Baltic eID Cooperation (NOBID) project with the aim to expand the Nordic-Baltic countries' national success in eID to also cover cross-border interoperability and digital mobility in the region.

The efforts in achieving cross-border digital mobility in the region are rooted to the shared visions and mutual interests of the Nordic and Baltic countries. These are constitutionalized under the umbrella of the Ministerial Council for Digitalization (MR-DIGITAL) at the Nordic Council of Ministers (NCM). The NOBID project operationalizes this by coupling the digital maturity of the region with the trust and willingness among the Nordic and Baltic countries to further integrate the region.

One key element in achieving this is solutions for cross-border identity matching of natural persons. This constitutes the process in which a service provider recognizes and serves a "returning user" from another country in the region. A returning user is a person who has previously been in the country where the service is provided but has since then moved back to his or her home country. This is a highly relevant situation for many service providers in our region, as there are many people moving between the Nordic and Baltic countries, for instance for working or studying.

The exact solution on this procedure is unique to every country and depends on the existing legal and technical national frameworks. However, the high-level challenges are the same on a regional perspective. To tackle this, we established a working group for identity matching, consisting of key experts from the Nordic and Baltic agencies and ministries responsible for digital identity in their countries. Together, we aim at sharing experiences, creating best practices, and casting a holistic view on the regional challenges.

This report presents an analysis of the as-is situation and provides perspectives on the possibilities for identity matching procedures in the future. It shall, however, be noted that further analysis and involvement of relevant key stakeholders, which was outside the scope of this report, is necessary. Furthermore, developments in the EU such as the revision of the eIDAS regulation that may impact the identity matching procedures in the region, was not finalized at the time of writing of this report.

It shall also be noted that the recommendations and opinions expressed in this report, directly or indirectly, represents the views of the authors, and doesn't constitute the official standing point of any of the countries, ministries, agencies, or experts involved in the work. The report serves as a knowledge foundation with insights and perspectives that might be inspiring and guiding us in our work going forward.

We would like to thank the consultants from Civitta and SK ID Solutions for their work and collaboration. We would also like to present our gratitude to the experts from the Nordic and Baltic countries, both within and outside the NOBID project, for their contribution to the insights that this report provides.

The Nordic-Baltic eID Cooperation Project – NOBID

# 1. Introduction

**The aim of this analysis** is to carry out region-wide recommendations that would help person to interact in a meaningful manner with all the Member States in the region, but also produce Member State (MS) specific policy suggestions to pave the way for that vision to be implemented in specific Member State.

## Background

The EU has prompted several initiatives to develop support services, both in public and private sector, to be available cross-border and, where that is preferred or necessary, in a personalized manner. However, as **eIDAS implementation report**<sup>[1]</sup> showed, the actual usage of cross-border services is low, and the availability is not reachable for most of the EU residents.

In the European Commission's report<sup>[2]</sup> on the evaluation of Regulation (EU) No 910/2014 on **electronic identification and trust services for electronic transactions in the internal market** (eIDAS) there are number of limitations imposed to secure, trustworthy, and easy-to-use electronic transactions that encompass electronic identification and authentication.

- Particularly relevant to the project's scope is the **availability of limited attributes** (elements of personal information) that can be reliably disclosed to third parties. In addition, the European electronic identity ecosystem is distributed across different national regulatory environments, levels of digital governance, and culture.
- Despite introducing references to eIDAS solutions in several sectors of EU legislation, the **eIDAS Regulation has not yet replied to the needs of specific sectors** (e.g., education, banking). One of the limitation factors of the current framework, with respect to these sectoral needs, is the lack of specific attributes by domains.<sup>[3]</sup>

The Commission staff working document,<sup>[4]</sup> accompanying the Commission's report, acknowledges that the Member States (MSs) have raised issues linked to the matching of eID identities with an existing national profile while providing cross-border services. **There are currently no cross-border processes at EU level to handle the situation where one person owns multiple eIDs issued or to assure that a person is successfully matched to correct eID under different notified eID schemes.**

---

1. <https://www.enisa.europa.eu/publications/eidas-overview-on-the-implementation-and-uptake-of-trust-services>  
2. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0290>  
3. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0290>  
4. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021SC0130>

This can lead to denial of access to services in cases where the receiving Member State cannot exclude duplication or match multiple legitimate eIDs from different eID schemes.

- In addition, non-harmonization of the minimum data set which is communicated in an authentication can also lead to denials of service.
- Some service providers require a national registry number to grant access to online public services, however not all Member states issue such a number. Consequently, cross-border users may be automatically denied access if the eIDAS authentication does not include such a number.
- Obtaining a national registry number often requires physical presence. This is an obstacle for users from abroad even in a case where they are eligible to obtain a national registry number and to access a service. The existence of the problem is well depicted by the fact that cross-border authentications provided by Member States show, factors wise, lower usage numbers compared to the usage of eID at domestic level.

**Single Digital Gateway** as a new obligation and **once only principle** (OOP) across EU has raised a need to solve the issue of the identity of a user. It is quite clear from public debates (incl. on draft eIDAS 2.0 regulation) that we are not going to see a common EU identifier assigned to EU residents, but rather we need to be able to match personal records from Member state to Member state and sometimes also within MS.

## Situation in Nordic-Baltic region

Nordic and Baltic countries differ heavily from most of the EU by having strong public sector data registries that are used to provide a rich selection of services for their residents. This region has so far had also a common approach in most countries that an individual is recognized in different datasets through commonly agreed unique identifiers or data sets. But even here we see some differences and deviations. For example,

- Identity code is available in Denmark, but that is missing from identity documents for Faroe Islands, and this means that any record made about them based on identity documents cannot reliably hold unique identifier.
- Within the eIDAS framework the minimal dataset for personal data includes family name but in Iceland the family names are (in most cases) not issued and thus needs to be faked in the records.<sup>[5]</sup>

---

5. Registers Iceland has created a database where names are split into two fields for almost all people registered, that is 1) Given Name/Names and 2) Surname. The Surname field can contain two surnames, example: Name (field 1): "Sigríður María", Surname (field 2): "Jónsdóttir Zoega".

Registration of Icelandic names in other countries is not always identical with the registry of Iceland, as until now other countries in most cases had to fake the Surname using the last part of the Given Name as Surname.

At the same time, the number of people that either live, work, study, or travel between Nordic and Baltic countries or who have done so in history, is one of the largest cross-border personal datasets.<sup>[6]</sup> These datasets carry actual meaning for persons' social benefits, health records, professional qualifications etc., and these are all kept with Member State records - with often no opportunity, or a very small one, to identify a person by means of electronic identification.

## Connections to other ongoing projects in Nordic-Baltic area

In August 2019 the Nordic Council of Ministers agreed on Vision 2030, with the goal of becoming the most sustainable and integrated region in the world by 2030. The work of MR-DIGITAL, on delivering cross-border digital services supporting the integration of the region, was set out in the ministerial declaration Digital North 2.0 and operationalised by the CBDS Programme.

**The CBDS Programme** is a strategic initiative from the **Nordic Council of Ministers (NCM)** that aims to accelerate the digital transformation of the Nordic-Baltic region. The programme will increase mobility and integration across the region through the development and deployment of cross-border digital services. This will benefit citizens, businesses, and public authorities in the region. The CBDS Programme was launched in 2020 by NCM. It supports the vision of making the Nordic-Baltic region the most integrated region in the world by 2030. The program facilitates close co-operation on selected digital services and data exchange between public authorities in the region.

Under the auspices of the Nordic Council of Ministers, **the CBDS Programme currently hosts two cross-border projects engaged with the implementation of the eIDAS and SDGR:**

- The Nordic Baltic eID project (NOBID)<sup>[7]</sup>
- The Single Digital Gateway - Once Only Proof of Concept Pilot project (SDG Project)<sup>[8]</sup>

A key component supporting cross-border digitalisation is the use of national electronic identities (e-IDs), both by citizens and businesses, to gain access to digital services in other countries. The framework for Nordic-Baltic e-ID cooperation is the **Nordic-Baltic eID Project (NOBID)**, which gathers e-ID experts from the whole region. The NOBID project is headed by the Norwegian Digitalization Agency (Digitaliseringsdirektoratet) and aims to deliver legal and technical e-ID

---

6. Holmberg, J., Lundquist, T., Hännikäinen, H., Liikkanen, S., Ulset, T., Helgadóttir, M., H., Neergaard, J., Jensen, H., Kousa, M. & Varis, A. (2019). Nordic Work Mobility and Labour Market. "More than 300,000 Nordic citizens live or work in another Nordic country and the number is on the rise. In recent years, about 50,000 people have moved to another Nordic country each year, for various reasons."  
7. <https://www.digdir.no/digdir/nordic-baltic-eid-project-nobid/1342>  
8. <https://www.norden.org/en/project/single-digital-gateway-once-only-proof-concept-pilot-project>



interoperability in the region. The project establishes service concepts for digital cross-border exchange of authoritative information for natural persons and legal entities, including semantics and Service Level Agreements (SLAs). NOBID has succeeded in establishing e-ID interoperability between Nordic and Baltic countries and continues the cooperation to ensure compliance with the eIDAS regulation.

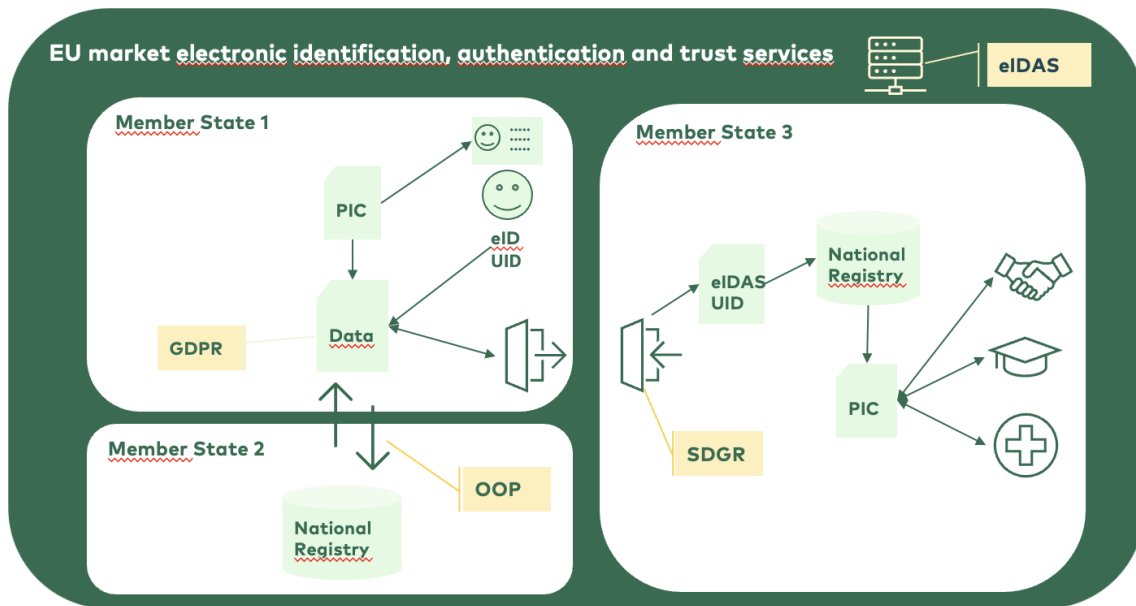
**The Once Only Proof of Concept Pilot project** addresses the Nordic and Baltic countries' shared concern about the functionality of the Once Only architecture in the European Commission's Single Digital Gateway Regulation. The project aims to identify common solutions that are simpler and more cost-effective for the Nordic and Baltic countries to implement. A general model for cross-border exchange of information can only be built if the Once Only architecture referred to in the Single Digital Gateway Regulation is considered. To ensure that no additional investments are needed, there is a need to launch the assessment and testing of the Once Only architecture and prepare recommendations and best practices for the exchange of information between the Nordic and Baltic countries. The project is led by the Finnish Development and Administrative Services Centre (KEHA Centre).

*//The project was finalised in June 2023, and it succeeded in developing opensource components for the key functions of OOTS: evidence request service and preview service.//*

# 2. AS-IS

## 2.1 Description of requirements

While setting out to create a predictable regulatory environment for trust services and ensuring that people can use their own national electronic schemes to access public services online in other EU countries, the state of play demonstrates shortcomings to the full implementation of the eIDAS regulation. As the implementation date for the SDGR and its 21 prescribed online procedures approached, national administrations faced a dual challenge of enforcing two complex and resource demanding regulations. However, as the eIDAS and SDGR are interrelated, the challenges prove similar for many countries. Resolving the central obstacles through cross-border cooperation is the key. One of these obstacles is identity matching.



**Figure 1** Identification matching areas affected by regulations (eIDAS, SDGR, OOP, GDPR).

Figure 1 illustrates what areas of identification and record matching are affected by regulations described below in this chapter. For the sake of the volume of this document and because of wide coverage of the topic elsewhere, the in-depth description of GDPR is not included. However, GDPR and identity matching are related because identity matching processes often involve the handling of personal data, and GDPR provides the legal framework for the protection of personal data within the European Union. Organisations conducting identity matching activities must comply with GDPR regulations to ensure the privacy and security of individuals' personal data.

## 2.1.1 eIDAS – electronic IDentification, Authentication and trust Services



eIDAS (electronic Identification, Authentication, and trust Services) is the regulation on e-identification and e-transactions effective in the European Union, which was adopted by the European Parliament and the Council on 23 July 2014. The purpose of the eIDAS regulation is to simplify the international use of digital services: it is possible to guarantee the comparability of trust services if the same requirements, codes of conduct and principles apply to all service providers and public institutions.<sup>[9]</sup>

The eIDAS Regulation:

- ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services available online in other EU countries.
- creates a European internal market for trust services by ensuring that they will work across borders and have the same legal status as their traditional paper-based equivalents.



Only by providing certainty on the legal validity of these services will businesses and citizens use digital interactions naturally.<sup>[10]</sup>

The first version of eIDAS was ready in 2014 and implemented in 2016. Now, the Commission is already working on an updated version. The Commission proposal amends and updates the existing eIDAS Regulation by responding to the challenges raised by its structural shortcomings and limited implementation and to technological developments since its adoption in 2014.<sup>[11]</sup>

---

9. <https://www.id.ee/en/article/eidas-i-e-regulation-on-e-identification-and-e-transactions/>  
10. <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>  
11. [https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_BRI\(2022\)699491](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)699491)

The reason for updating the regulation was that not all eID key interoperability components of the older version of eIDAS were obligatory for **EU Member States**. **As a result, only 14 of them completed their eID schemes which were all different.**

The new provisions will be mandatory for countries, which punishes those who have already achieved more and makes finding a common solution quite difficult. Madis Ehasu, Estonian Seconded National Expert at the European Commission who is actively developing the new eIDAS regulation, said that one of the key difficulties lies in finding common approaches considering substantial variations in legislations and cultures.<sup>[12]</sup>

Regarding identity matching, eIDAS requires that electronic identification means used for cross-border transactions must be reliable and secure, and the identification of the user must be verified using robust authentication mechanisms. This means that **the eID system must use methods that can confirm the identity of the user with a high degree of certainty and** establish rigid issuance process and lifecycle management of electronic identities.

Additionally, eIDAS requires that the identification process must be carried out in compliance with data protection laws, with due regard for the privacy and security of personal data. This includes ensuring that the user's **personal data is processed only for the purposes of identification and that it is not disclosed to unauthorized parties.** Furthermore, eIDAS also sets out specific requirements for the electronic identification means themselves, including technical specifications for the security features and mechanisms used for protection against unauthorized access and data breaches.

Identity matching is typically done by looking up and matching the identity received with the identities registered. For this purpose, the eIDAS Unique Identifier (eIDAS UID) can only be directly used if it is already known by the Evidence Provider. This may be true in cases where the Evidence Provider has already linked the eIDAS UID to a known identifier or has access to such a record. The eIDAS UID is a mandatory attribute in the minimum set of person identification data specified in the EC implementing regulation,<sup>[13]</sup> and its definition is detailed in the eIDAS SAML Attribute Profile.<sup>[14]</sup>

Notwithstanding the mandatory stipulation of the eIDAS UID, the persistency of eIDAS UID is not enforced and as consequence undermines its uniqueness characteristics. Some Member States issue an outbound identifier for each Member State, which is also usually derived. This means that the third part of the Unique Identifier, the combination of readable characters, may not have the same value for all requesting Member States. This means that in such cases, the eIDAS UID (PersonIdentifier) was issued for the specific context of the Online Procedure Portal, and it cannot be used by the relying party (Data Service).

---

12. <https://e-estonia.com/the-bumpy-road-to-european-digital-identity/>

13. Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) 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

14. <https://ec.europa.eu/digital-building-blocks/wikis/display/TDD/2.1+-+Identity+and+Record+Matching+-+Q3+2022>

How these outbound identifiers are generated is specific to each Member State and/or eID means. The derivation process could potentially prove challenging (or impossible even) for a matching function from the issuing Member State to identify the user based only on this identifier. Additional attributes may be needed. The information on the Unique Identifier, if it is derived and/or receiving Member State specific is communicated during the notification procedure and in the following resource. This information could be requested from the eIDAS Cooperation Network and configured accordingly.

## 2.1.2 SDGR – Single Digital Gateway Regulation



The Single Digital Gateway (SDG) project is created based on the Regulation (EU) 2018/1724 of the European Parliament and the Council dated on the 2 October 2018 on the creation of a single digital gateway to provide access to information, procedures and assistance and problem-solving services, amending the Regulation (EU) No. 1024/2012.<sup>[15]</sup>

The purpose of the Single Digital Gateway (SDG) is to

- **reduce any additional administrative burden** on citizens and businesses that exercise or want to exercise their internal market rights, including the free movement of citizens, in full compliance with national rules and procedures,
- to **eliminate discrimination** and
- to **ensure the functioning of the internal market** regarding the provision of information, of procedures, and of assistance and problem-solving services.

**The Regulation makes it mandatory for Member States and EEA countries to provide access to 21 digitalized administrative procedures in a safe and convenient way.** The procedures include (amongst others): requests for a birth certificate, vehicle registration, starting a business or submitting a corporate tax declaration.<sup>[16]</sup> These services must be established fully online, and deliver tangible results through a digitalized process, as well as implement the OOP. This means that users will be able to digitally interact with the public bodies during all stages of the process and be relieved of the administrative burden (submitting numerous documents and pieces of information). The online procedures will fetch the required evidence using the once-only infrastructure that the Regulation foresees. In this way, all the information already submitted to, or held by, the administrations in the country of origin, will not have to be re-submitted to the country of destination. This is how the OOP will work in practice.<sup>[17]</sup>

---

15. <https://www.gov.pl/web/finance/single-digital-gateway>

16. Full list of services is available in the Annex II of SDGR: <https://eur-lex.europa.eu/TodayOJ/>

17. <https://toop.eu/node/280>

The SDGR sets out several requirements related to Identity matching, which are detailed in the following paragraphs:

- **Secure and reliable electronic identification:** The SDGR requires that electronic identification means used for cross-border transactions must be reliable and secure, and the identification of the user must be verified using robust authentication mechanisms. This means that the eID system must use methods that can confirm the identity of the user with a high degree of certainty, such as biometric authentication or multi-factor authentication. The regulation requires that the eID means used must be certified under the eIDAS Regulation. This ensures that the eID system complies with strict security and privacy requirements.
- **Reuse of existing data:** The SDGR requires that public authorities must use existing data and information collected from other public authorities whenever possible. They must avoid collecting the same information from citizens and businesses more than once unless the information is necessary for a specific purpose.
- **Limited collection of personal data:** The SDGR requires that public authorities limit the collection of personal data to what is necessary for the provision of a specific public service or the fulfilment of a specific legal obligation. They must not collect more personal data than necessary or retain it for longer than necessary.
- **Protection of personal data:** The SDGR requires that public authorities protect personal data from unauthorized access, disclosure, or misuse. They must comply with the General Data Protection Regulation (GDPR) and other data protection regulations when collecting, processing, and sharing personal data.
- **User consent:** The SDGR requires that public authorities must obtain the explicit request of the user before collecting, processing, or sharing their personal data. Users must be informed about the purpose of the data collection, the legal basis for the processing, and their rights under data protection laws.<sup>[18]</sup>

Cross-border OOP will become a reality in the EU at the end of 2023, when the Member States are expected to finalize the integration of the 21 online procedures with the OOTS.<sup>[19]</sup> Establishing the Single Digital Gateway is an important milestone in enhancing the functioning of the EU Single Market. (see [Ch. 2.1.3](#))

---

18. Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide information, procedures, assistance and problem-solving services and amending Regulation (EU) No 1024/2012

19. The procedures in directives listed in SDGR article 14.1 also must be integrated with OOTS i.e., Service directive, Professional qualification directive and Procurement directives.

Access to the gateway will be available via the search function of the Your Europe portal, which has existed since 2006 to provide citizens and businesses information on EU and national rights. The establishment of a single-entry point will contribute to a more comprehensive and user-friendly package of information and assistance, which will help EU citizens and businesses navigate the internal market. Furthermore, the gateway will be conducive to more transparency in terms of rules and regulations relating to different business and life events.<sup>[20]</sup>

### 2.1.3 OOP – Once Only Principle



The Once Only Principle (OOP) System will allow both citizens and businesses to carry out all their administrative procedures across the EU in a faster, simpler, and smoother way. By December 2023, all Member States will have to comply with the Once Only Principle as referenced in the Single Digital Gateway Regulation (SDGR).<sup>[21]</sup>

The principle states that:

- citizens and businesses should only be required to provide information to public authorities once, regardless of how many times that information is needed by different public authorities.
- Under the OOP, public authorities must share information and collaborate with each other to ensure that data is collected only once and reused by other public authorities as needed. This means that citizens and businesses do not need to provide the same information repeatedly, which reduces the time and effort required to interact with public services.

The OOP applies to all EU member states and covers a range of public services, including social security, taxation, and starting a business. It is intended to promote the efficient use of public resources and reduce the administrative burden on citizens and businesses. **The implementation of the OOP requires the use of advanced digital technologies and interoperable systems to enable the sharing of information between different public authorities.** This includes the use of electronic identification and authentication systems, secure data exchange platforms, and data protection measures to ensure that personal data is processed securely and in compliance with data protection regulations.

The main objective of the OOP reducing the administrative burden of users and businesses by re-organizing public sector internal processes derives directly from the overall political objective of improving economic efficiency of the EU by facilitating cross-border trade through such initiatives as digital single market.<sup>[22]</sup> It

---

20. [https://single-market-economy.ec.europa.eu/single-market/single-digital-gateway\\_en](https://single-market-economy.ec.europa.eu/single-market/single-digital-gateway_en)

21. [https://commission.europa.eu/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-11-05\\_en](https://commission.europa.eu/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-11-05_en)

22. EU eGovernment Action Plan 2016-2020.

assumes that **collecting information is more expensive and burdensome than sharing already collected information**. Hence this principle proposes collecting information only once and then sharing this information, respecting other constraints, such as regulations. The political reality of the EU, however, is such, that precludes swift and direct application of the once-only principle, given that first, different EU Member States have:

- different understanding of the once-only principle,
- different approaches to public service provision,
- different IT systems that make such services possible,
- but also, different understanding of issues relevant to the once-only principle, such as protection of personal data, for example.<sup>[23]</sup>

While the OOP does not specifically regulate identity matching, it can impact the way in which identity matching is performed in cross-border transactions. In general, the OOP requires that public authorities should only request information from citizens and businesses once and should make efforts to reuse this information for subsequent transactions, provided that the information is still up-to-date and relevant. This can include personal information such as identity documents and tax identification numbers. When implementing the OOP, public authorities must ensure that they comply with relevant data protection laws, such as the General Data Protection Regulation (GDPR), and that they have appropriate measures in place to ensure the security and privacy of personal data.<sup>[24]</sup>

## 2.2 Technological readiness

### 2.2.1 Data required for identity and record matching

When people are moving, working, or studying abroad, it is usually only a matter of time when some services are needed while being in another country. **Even though people are moving across borders more and more,<sup>[25]</sup> their data rarely follows them.** The existing data in the country of origin is mostly never available, accessible, or usable abroad. In addition, some services can be increasingly obtained from other countries and long-term relations should be continued even though an individual moves between countries. Data sharing on "paper based" processes might still exist, and the data may not be comprehensive or up-to-date due to required manual work.

---

23. Krimmer, R., Kalvet, T., Toots, M., Cepilovs, A. and Tambouris, E., 2017. Exploring and Demonstrating the Once-Only Principle: A European Perspective. In Proceedings of the 18th Annual International Conference on Digital Government Research (pp. 546-551). ACM.

24. European Commission. (2020). European Interoperability Framework - Implementation Strategy. Brussels: European Commission.

25. The Nordic Statistics database. (2020, October 30). Who goes where in the Nordic region?



Three different scenarios of three different fields were studied and are described below:

- opening a bank account in another country
- identifying the person and accessing past medical history
- recognition of professional qualifications

These three scenarios are described from the two main aspects of technological readiness: data and actors.

### **Banking: opening a bank account in another country**

Opening a bank account is a process that involves identification of the person and collecting data related to the person's financial behaviour. Process must follow EU's anti-money laundering and countering the financing of terrorism (AML/CFT) rules.

Preconditions for opening a bank account vary depending on the chosen registration method. A physical presence in the bank office is suitable for all persons who qualify with banks' general terms. Usage of e-services with eID means for same purpose does impose significant limitation. Namely the eID mean issued within country of bank's residence is commonly required and must be complemented by person's physical ID-document. The latter can be either a person's national ID-document or the one issued by authorities of bank's country of residence.

Availability of personal identification number issued by the county where the bank is operating is crucial for identity verification. Imposed limitations for e-services channels are justified with strict requirements coming from AML/CTF rules, and risks coming from cross-border identity matching based on eID means can be seen as un-acceptable liability considering potential operational, financial, and reputational damages. Thereof person's eID mean originating from a country other than a bank's residence country cannot be used for onboarding through e-services.

### **Data**

Data collected during the opening of bank account through eID mean supported e-service must enable identity verification (1:1) of the person in the context of banks' country of residence.

Data collected from eID mean comprises of following attributes:

- family name(s)
- first name(s)
- date of birth
- personal identification number

Data available from person's physical ID-document:

- family name(s)
- first name(s)
- date of birth
- place of birth
- document number
- personal identification number in document issuing country.
- citizenship

In addition to personal identifiable information (PII) banks do request data that enable fulfilment of due diligence defined by AML/CFT rules.

Additional data presented by person:

- contact address (formal/informal)
- types of incomes
- tax payment countries
- expected monthly incomes and cash transaction amounts.
- accounts in other banks
- other country's regulation specific data

## Actors

**Table 1** Opening a bank account in another country actors and responsibilities

Actor	Action	Necessary preconditions, successful authorization of:	Successful identification/ authentication of:	Other directly involved' actors
Customer from country A	Identifies him/herself in bank of country B	eID mean issued in country B. Possession of physical ID-document	Authentication with eID mean issued in country B. Validity checks and verification of presented physical ID-document	eID provider in country B Database of stolen or lost documents (country of document's origin or Interpol SLTD (stolen or lost travel documents) database Identity proofing service provider of bank
Bank in country B	Validates PII retrieved from eID mean and physical ID-document. Validates additional data submitted following AML/CFT rules	All requested customer related data is made available to bank	PII and additional data are successfully validated against population registry and potential black/grey lists of banks. Additional data meets criteria established by AML/CFT rules	Population registry of country B
Customer from country A and bank in country B	Entering contractual relationship	PII is validated and AML/CFT rules fulfilled.	Acceptance of bank's terms and conditions by customer. Signing of contract by customer and bank.	

To conclude, cross-border usage of eID means is not supported for opening a bank account in another country. Limitations coming from AML/CFT rules force banks to restrict account opening e-services to accept only eID means issued within the residence country of the bank.

### Health: identifying the person and accessing past medical history

Treatment of patients without proper information on the patient's medical background and history poses a lot of risks. There are already ongoing collaboration and practices between the Nordic and Baltic countries. A good example of an already working operational solution is the ePrescription exchange between Finland and Estonia. There are also projects such as the health care and care through distance spanning solutions – project (VOPD) led by Sweden.<sup>[26]</sup> In addition to these, many of the Nordic and Baltic countries are already taking part in the European level eHealth Digital Services Infrastructure (eHDSI) initiative, whose main aim is in semantics and common standards and technologies.

### Data

Today, European **cross-border health data exchange** consists of two services:

- cross-border digital prescription and
- patient summary

These two services are a part of **eHealth Digital Service Infrastructure (eHDSI)**<sup>[27]</sup> or with a new name **MyHealth@EU**. This platform is administrated by the European Commission. The platform is not yet compulsory for the member states, therefore not all the countries are using it. However, the European Commission hopes/expects that by 2025 there will be 25 countries who have joined this platform. Since not all the countries have joined the platform, the exchange of data is not always possible. And when it is possible, it mainly works only one way.

The most important entities of eHealth DSI system are human beings (patients, HPs, administrators, etc.). However, there are many non-human entities in the eHealth DSI. The most important of them are documents in electronic form, which are of course always linked to a human entity.

Example (data related to human entity): Daniela Altenberg, born 29.12.1979 in Vienna, Austria, Father Gottfried Altenberg (\*6.6.1953), Mother Elisabeth Altenberg (\*6.3.1956, maiden name Eugenie) address of residence Vienna, Castle of Schönbrunn, No 1.).

---

26. Healthcare and care at distance. (n.d.). Healthcare and care through distance spanning solutions

27. The eHealth Digital Service Infrastructure (eHDSI or eHealth DSI) is the initial deployment and operation of services for cross-border health data exchange under the Connecting Europe Facility (CEF)

**Identity matching** is completely a responsibility of the health care provider. For example, in Estonia, HCP must make an enquiry to a patient's previous home country, previous home country checks from the population register whether a person has personal identification number, the person is alive and has allowed to share its medical records. Patients themselves don't have electronic access to their previous medical records with foreign country's ID.<sup>[28]</sup> However, it is possible to access one's data in case one still has the home country's ID and access to the home country's portals.

Within the eHealth DSI environment physical identity sources (passport, ID, diploma etc.) can be used within identification and authentication processes. **At least two-factor authentication**<sup>[29]</sup> is required for Health Professionals in the Country of Treatment: the authentication must be validated by the Country of Treatment.

It is the responsibility of each country to upload its own International Search Mask (ISM), to the configuration settings of the platform. And then this Search Mask clarifies what information about one's patient needs to be asked to uniquely identify a patient, which **varies a lot among countries**. Many countries have just one ID: it can be a personal identification number, or document number, social security number etc. However, some countries use multiple.

The eHealth DSI environment is a set of National Contact Points (NCP) communicating by means of public networks. NCPs are interfaces or proxies between national eHealth domains. These national eHealth domains are not under direct control of eHealth DSI. Patient data and identities of patients, HPs, HCPOs are placed in registries, repositories, or databases in national domains and most of the data processing takes place there. Therefore, it must be distinguished between processes running in the intrinsic eHealth DSI environment and the processes running partially or totally outside the intrinsic eHealth DSI environment within the national domains. eHealth DSI and authorities/participants from national domains will together provide identification and authentication services.

The **intrinsic eHealth DSI identity confirming and forwarding** covers the following points:

- Management of selected identity datasets and/or identifiers:
  1. of single persons (HP, patient).
  2. of a group of persons (legal entity of healthcare providers, e.g., HCPO).
  3. of single documents (patient consent).
- Management of outgoing requests for validation of provided identities within the "Circle of Trust."

---

28. However, patients still can request an extract from the medical records.

29. eID authentication: ID number + password or electronic ID card.

- Management of incoming requests and responses to such requests.
- A secure, trustworthy, and reliable acknowledgement and vouching for the correctness of information provided by the national infrastructure and the HPs.

**National authorities and institutions from national domains will provide:**

- the accurate management of identities lifecycle, from the creation of identifiers of entities until they terminate.
- the accurate management of identity assurance, authentication of the identity information, and the assessment of the required level of risk assurance for collecting and using identity information (named "trust level" in the following descriptions).
- the accurate management of identity information at the level of the relevant identity authorities and.
- the accurate management of local systems and/or services which support the "Circle of Trust" (NCP).

**The eHealth DSI services include the transfer of sets of agreed data**, particularly, a patient summary, that also includes a medication summary and data related to the ePrescription (prescription and dispensation). Most of the data included in those sets correspond to health data and therefore these documents are referred to as health data. Utilizing eHealth DSI services to access health data is contingent on successful identification and authentication of the health care professional, the identification of the patient, the fact that the eHealth DSI system "knows" the appropriate documents and the requestor is assigned to a role which is authorized to gain access to eHealth DSI.

**Currently, only patient summary is digitally accessible cross-border**, provision of other medical data is the responsibility of the patient (printing out the medical history, translation etc.). Currently, the patient summary dataset must include active health problems, diagnosis codes and history of previous diseases. Optional content includes blood pressure data, blood group and rhesus factor data, allergy data, facts about smoking and alcohol consumption, and surgeries and procedure data. The patient summary is more of a standardized dataset that can be provided in a coded form. And in many countries provision of even this data is not possible yet.

## Actors in MyHealth@EU

The following table summarizes the relevant activities of actors belonging to eHealth DSI roles (according to the basic scenario – HP from Country B needs patient's health documents from patient's home Country A). eHealth DSI is based on distributed systems and many functions will be executed by actors within national domains. The eHealth DSI role management depends strongly on cooperation with national authorities and operators of local systems. (See Table 2)

**HCPO:** In every country involved in eHealth DSI a national authority or a group of regional authorities must exist, able to define/manage HCPOs from its domain, participating in eHealth DSI. NCP will communicate with the respective national authority to keep the actual list of HCPO. eHealth DSI would define the minimal set of information necessary for unambiguous identification of HCPO.

**HP:** HPs identities will be managed in national domains. A national authority will maintain the list of all HPs in its domain and provide it to its national NCP. HCPO will provide NCP the roles assigned to its HP (if necessary). eHealth DSI would define the minimal set of information necessary for unambiguous identification of HP.

**Patient:** Each use case accessing the patient data, such as the Patient Summary and ePrescription/eDispensation use cases, requires the minimal set of necessary information for identification of a patient.

**Authorized Third Party (optional):** For member states allowing it, an authorized third party can perform any action the patient can perform.

**Health data administrator:** A health data administrator is primarily responsible for running systems which exchange health data on NCP. The second responsibility covers the support of patients whenever they want an extract of audit log data. Health data administrators are working for or on behalf of national authorities and from an eHealth DSI point of view the standard professional and security requirements fully suffice for this role.

**Table 2** MyHealth@EU actors and responsibilities

Actor	Action	Necessary preconditions, successful authorization of:	Successful identification/ authentication of:	Other directly involved actors
HP B	Requests services from Country A	HP in Country B	HP in country B the patient by Country A	National Infrastructure B, NCP B NCP A
Patient	Requests check and provision of audit log concerning the accesses to his health data	Successful authorization of HP	authentication of the patient at PoC	NCP A, Health data administrator
Authorized Third Party (optional)	For the member states allowing it, can perform any action the patient can perform	Successful authorization of HP and authentication of the patient at PoC NCP-B and NCP-A must both authorize a third party to act on behalf of the patient	patient at PoC	Patient, NCP A, Health data administrator
NCP B	Requests services from Country A	Successful identification and authorization of NCP A Authentication of the patient	NCP in county B The patient by country A	NCP A
NCP A	Responds to service requests of NCP B	Successful identification and authentication of NCP B Authentication of the patient Authorization of HP/HCPO	The patient by country B NCP A	NCP B Identity authority managing the databases of patients, HPs, HCPOs
HCPO or other external service provider	Provides required information to NCP	Mutual successful authentication of both parties	Both parties	NCP B HCPO or other external service provider
Health data administrators	Administrates systems processing data and provide some services (e.g., excerption of audit logs)	Successful identification of health data administrators Authentication of health data administrators Assigning the role of health data administrators	Health data administrator	NCP or HCPO



In many countries, **not all the health care providers have joined with the services**, so for example in Netherlands, there is currently just one Hospital that uses eHDSI. Main concerns for many countries are data security, trust issues and encryption used. Standards, privacy issues, technologies and translations are decided and included in eHealth Digital Services Infrastructure and the decisions made already in eHDSI are preferences for many countries.

It is planned that in 2025–2026, the technical prerequisites for the **European Commission's central solution** will be created, so it will be possible to share laboratory analysis data, hospital treatment summary data, medical records, and test response data.

### Academia: recognition of professional qualifications

Professional recognition is the appreciation of a foreign qualification for the purpose of employment in a certain profession. The recognition of qualifications for professional (employment) purposes depends largely on whether the profession in question is regulated or is not regulated in the host country.<sup>[30]</sup>

### Data

IMI allows competent authorities to check data within the EU by making inquiries to other countries' competent authorities and verify the data. ENIC/NARIC Network allows to make an analysis on a diploma and gives assurance about the higher education institution and confirms that the diploma was issued to a particular person.

However, there are no general rules for identification of persons. Competent authority generates a deed of identification that is not shared amongst other competent authorities and is not updated in case of personal data changes. So, if a person has different qualifications in different fields, one must go through two separate processes for identification and recognition of foreign qualifications.

### Actors

Depending on the field of study, different **competent authorities** (usually ministries, professional associations, etc.) **must evaluate a person's qualification** according to the Directive 2005/36/EC.<sup>[31]</sup> For example, if one's medicine studies diploma acquired abroad needs to get recognized, then one must turn to the Health Board or if one has acquired a teacher's diploma, then one must turn to the Ministry of Education and Research etc. What makes integrating this field to Single Digital Gateway (SDG) difficult is the fact that in most countries, every competent authority has its own system of recognition of foreign qualifications. Since the way in which people are identified is not regulated, some systems are quite primitive and still use e-mails, some systems use ID-card based authentication.

---

30. <https://www.enic-naric.net/page-professional-recognition#:~:text=Professional%20recognition%20is%20the%20recognition,regulated%20in%20the%20host%20country.>

31. Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications

**Table 3** Recognition of foreign qualification, actors and responsibilities

Actor	Action	Necessary preconditions, successful authorization of:	Successful identification/ authentication of:	Other directly involved actors
Person (from country) A	Requests diploma recognition from country B	Person identification following Competent Authorities requirements Presenting diploma	Person A in Country B	
Competent Authority of country B	Verifies diploma data and qualification	Data exchange system (IMI, ENIC/NARIC)		Competent Authority of country A
Competent Authority of country A	Confirms diploma data and qualification	Data of diploma		National data sources for educational and qualification records in country A
Competent Authority of country B	Issues deed of recognition	Diploma data and qualification confirmed by Competent Authority of country A		

Currently, competent authorities are mainly using **ENIC/NARIC<sup>[32]</sup> Networks** and **IMI (internal market information system)<sup>[33]</sup>** to make decisions regarding evaluation of qualification. The Internal Market Information System (IMI) is a secure, multilingual online tool that facilitates the Exchange of information between public authorities involved in the practical implementation of EU law. IMI helps authorities to fulfil their cross-border administrative cooperation obligations in multiple Single Market policy areas. In other words, IMI mediates queries from competent authorities in different countries. The ENIC-NARIC Networks are the result of an ongoing collaboration between the national information centres on academic recognition of qualifications of in total 55 countries. The national information centres operate under the principles of the Lisbon Recognition Convention (1997).<sup>[34]</sup>

### 2.2.2 An analysis and discussion of the availability and machine-readability

Based on three different scenarios of three different domains studied and are described in chapter 2.2.1, one can see remarkable challenges to be tackled if cross-sectoral data availability and data machine-readability would be targeted. Main aspects that must be confronted would be following:

- Implemented systems do vary from country-to-country dependent on availability of resources and/or volumes of cases. In addition, within the country implementations in sub-domains of specific domain may have significant discrepancies.
- Identity management processes are defined following requirements and risks-imposed domain. Requirements for identifying persons can be missing although the domain is regulated on EU-level, and matching identity with record is crucial.
- Domain specific data is not deployable for cross-sectorial usage, as it is commonly prohibited due to data protection constraints, data can be non-disclosable for reason of being a business/bank secret.
- Data is handled by numerous competent authorities, who have their own registries. Data is not often shared to allow automated processes for further use based on the received (digitized) data.
- Personal identifiable information at rest in most domains' registries is not updated if any change in attributes occurs.
- There are EU level systems for domain specific communication and data exchange, but their interfaces are designed differently. Besides human-to-machine interaction human-to-human interfaces are still deployed.

---

32. <https://www.enic-naric.net/page-homepage>

33. [https://ec.europa.eu/internal\\_market/imi-net/index\\_en.htm](https://ec.europa.eu/internal_market/imi-net/index_en.htm)

34. <https://www.coe.int/en/web/higher-education-and-research/lisbon-recognition-convention>

Human-to-machine interface does provide better options for data machine-readability, whereas human-to-human interfaces exploit free text data fields, and no format harmonization has been achieved either for evidence exchanged as digital files. A lot of cross-border identity and record matching is based on paper documents and manual work.

- Implementations are made to solve single domain specific use cases at the time and do not scale nor provide reusability of data.

To sum up the aspects provided above, it can be stated that availability and machine-readability of data is constrained by existing implementations and legislation. Thus, deploying them as-is for a large-scale identity and record matching is not feasible.

From identity and record matching perspective it should be targeted, that personal identifiable information is handled in cross-domain use cases in a manner that enables deployment of harmonized principles facilitating the matching necessities. Providing solution, which centrally deals with identity management (creating identities accompanied by adequate attributes, mechanisms for updating the attributes (while keeping initial values) and enriching identities with attributes originating from other countries (e.g., personal identification numbers) and is available for cross-domain usage should be focused on.

### **2.2.3 Description of identity matching in the Once only technical system**

To date all countries have opted to consider unique user only within a member state. Linking data between member states based on user attributes (see Table 4) is almost non-existent.

The technical and operational specifications of the Once-Only Technical System (OOTS) is laid down in the European Commission's Implementing Regulation (EU) 2022/1463. Regulation (EU) 2022/1463 foresees usage of eIDAS nodes for cross-border authentication of a user by electronic identification means issued under electronic identification schemes notified in accordance with Regulation (EU) No 910/2014.<sup>[35]</sup> Authentication performed through eIDAS node should enable evidence providers to identify users by matching the user identification data to evidence providers' existing records.

Identity matching is the role and responsibility of evidence providers following Regulation (EU) 2022/1463. Evidence providers' application services shall be capable of identifying the user through eIDAS node, perform matching of PII with identities known to evidence providers and retrieving correct identity evidence from their records. Evidence providers may require users to provide additional attributes

---

35. eID schemes from the Member State of the Evidence Provider, which are deemed adequate for the access to the Evidence Providers' services may also be relied upon. This includes both notified and non-notified eID schemes.

beyond the mandatory attributes of the minimum data set listed in the Annex to Implementing Regulation (EU) 2015/1501 for the purpose of identity and evidence matching. Referenced additional attributes can be either optional attributes of the eIDAS minimum data set and/or sector specific attributes that may be made available via the eID scheme used, if it is allowed by the national law and if the user gives their consent for this purpose. However, the use of eIDAS node does not preclude the use of other mechanisms to provide complementary or additional security measures.

It is mandated that evidence can be processed only in case identity matching generates single result.

Neither Regulation (EU) 2022/1463 nor OOTS Technical Design Documents do specify methods for identity matching. OOTS Technical Design Documents do acknowledge the variety of combinations of how personal identification numbers may be presented through eIDAS node (personal identification number being derived or not, derivation receiving Member State specific or not), but logic design for handling various combinations is left up to national implementations.

Hereby table of Identity attributes will be compiled to illustrate possibility of finding common solution for Nordic-Baltic countries (Table 4).

Exceptional in this regard is cross-border data transfer between Nordic countries based on population registry and connected to migration data. There are procedures where a new address in a new member state of the person moving out from a country is listed automatically to the population registry of the country person migrated from.

**Table 4** Identity attributes of European countries

COUNTRY	EIDAS BASIC DATASET				ADDITIONAL ATTRIBUTES									
	EUID	FIRST NAME	FAMILY NAME	DATE OF BIRTH	GENDER	OTHER NAMES	NATIONALITY/CITIZENSHIP	COUNTRY	PLACE OF BIRTH	CENTURY OF BIRTH	CURRENT ADDRESS	BIOMETRY	FIRST NAME AT BIRTH	LAST NAME AT BIRTH
Estonia	x	x	x	x	x		x		x					
Spain	x	x	x	x	x	x								
Luxembourg	x	x	x	x	x	x	x	x	x		x			
Netherlands	x	x	x	x	x		x				x			
Norway	x	x	x	x	x		x	x	x					
Lithuania	x	x	x	x			x							

## 2.3 A state of play of processes and solutions for identity and record matching in the EU/EEA.

The development of a European digital identity is not new. The 2014 eIDAS regulation has set standards for digital identification methods across the European Union (EU) for citizens and legal persons. The goal of this regulation is to **strengthen the European Single Market by promoting confidence and convenience in cross-border electronic transactions**. These benefits have not come to fruition as initially planned: since the regulation came into effect in September 2018, only 59% of the EU population (living in 14 Member States) can use an electronic national identity document cross border. To achieve the eIDAS' goals, the Commission has proposed an amendment of the regulation (eIDAS 2.0) which mandates a European Digital Identity Wallet (EUDI-Wallet). This is a nationally provided mobile application with which each EU citizen can identify themselves at every public institution in the EU, as well as at private parties which rely on unique identification for the provision of their services.<sup>[36]</sup>



A limited number of Member States have provided the number of relying parties connected to their eIDAS node and the **situation can vary considerably between Member States depending on size and organization of their public services**: in some countries, each municipality provides some specific services and would therefore need to connect to the national node while in other countries, key public services are provided centrally.

To assess the potential cross-border usage for public services, different proxies can be used. According to Eurostat, in 2019, less than 4% of EU citizens of working age were residents of another EU Member State than where they hold their citizenship. In principle, they should be able to use one eID to access public services in both Member States. In addition, there are online public services where user authentication is needed and that can be used by e.g., tourists (about 30% of EU population travel yearly to another Member State) such as buying tickets for public transport, museums or subscribing to bike rentals.



It is likely that the number of public services connected to the eIDAS network remains very low, since citizens **access to services will continue to depend on technical and architectural choices made by Member States on their national identity systems**. For instance, it is expected that some Member States will not

---

36. European Commission art. 12b, 2021

change their approach not to centralize their eGovernment services on central platforms or gateways, thus not offering their citizens a convenient access to the eIDAS network and an effective usage of notified eID schemes. Similarly, it is expected that the number of cross-border authentications to remain very low, particularly when compared to the usage of the eIDs at national level.

To assess the overall potential of eID use, we can rely on existing use as proxies. Available data from some Member States (e.g., NO, SE, EE, LV, LT), where user authentication solutions are widely re-used by different service providers, authenticating oneself with a legal identity is done roughly around 20 times per month, of which 1 occurs in the public sector. If that relationship is extrapolated to the EU level, we can assume the potential for EU to be roughly 100 billion user authentications per year of which 5 billion in the public sector. Based on these assumptions, for example, if we expect 3% of people living in another Member State to only use eIDAS in the current scope, **the potential of eIDAS authentications in this case would be 150 million per year.**

Regarding the articulation of relationships between eIDAS and private sector service providers, these are expected to remain suboptimal. Even if all notifying Member States potentially open their eIDAS nodes to the private sector services providers across the Union, the diversity of national conditions for the use of the national eID infrastructures will still make it very difficult for the service providers to build a sustainable business plan or to accurately estimate the potential of this openness to expand their business cross-border. Besides, private sector service providers have made available cross-border usage of eIDs and digital signatures through gateways like Signicat, Dokobit, TrustLynx amongst many other companies. Moreover, given the difficulty raised by the constraint to harmonize the various approaches followed at national level, a revenues model and establishing clear liability rules would be difficult to construct.<sup>[37]</sup>

### 2.3.1 Processes and best practices for identity and record matching in EU/EEA countries

After the desk research of identity matching best practices in EEA countries,<sup>[38]</sup> representatives of following eight countries were available for closer look of their practices and from those representatives of four countries agreed to participate on deeper analysis and process related interviews. The overview of the results is presented here in the same order (3 countries short overview and 5 countries best practices plus processes, see analysed aspects per country at Ch. 4.5). As a conclusion of analysis, a merged process of identity and record matching based on five countries (ES; LU; NL; NO; EE) was drawn (see Ch.2.3.3).

---

37. [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en)

38. [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:European Economic Area \(EEA\)](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:European Economic Area (EEA))



Interviews revealed three main phases of the identity and record matching process which are used to structure the interview summaries (below) of the referred five countries. Those three phases are: providing identity; identity matching; and data sharing and record matching.

Those phases were refined during further analysis and merged process (see Ch.2.3.3) is described also by three-part, but somewhat different division (identity matching; e-service usage; and record matching). However, high level process descriptions of interviewed countries consist of five steps for providing more details.

### Germany (DE, not interviewed)

The German eID is based on government-issued chip cards (eID cards) using certified chips and strong cryptographic protocols. The following types of eID cards are currently part of the scheme:

- German identity cards (Personalausweis) issued to German nationals living in Germany or abroad,
- German resident permits (Aufenthaltstitel) issued to non-EU nationals living in Germany, and
- German eID card for Union citizens (Unionsbürgerkarte) issued to citizens of the European Union and nationals of the European Economic Area.<sup>[39]</sup>

Due to the nature of the German eID system that operates without a central component, the German eID scheme is integrated into the eIDAS Interoperability Framework via the middleware integration model in accordance with the eIDAS technical specifications.<sup>[40]</sup> In Germany, the use of a general unique identification number is considered as prohibited, based on judgements of the German Federal Constitutional Court; in particular, the population census decision of 15 December 1983.<sup>[41]</sup>

Public-sector bodies of other Member States of the European Union are authorized to request person identification data from the German eID of a user. For this purpose, Germany will provide an authorization certificate to each Member State free of charge. Identification and the initial registration at a commissioned authorization CA will be performed via the Point of Single Contact according to a dedicated procedure. After initial registration, the German eIDAS middleware automatically updates the authorization certificates. Provisioning of authorization certificates also includes the necessary eID revocation lists.<sup>[42]</sup>

---

39. German\_eID\_Whitepaper

40. German\_eID\_Whitepaper

41. <https://verfassungsblog.de/digital-id-eu/>

42. German\_eID\_Whitepaper

## Poland (PL, not interviewed)

Currently there is no specific solution in place in Poland to enable universal cross-border identity matching.

For foreigners who live in the Poland there is a possibility to apply for a Polish identifier (a PESEL number regulated by the Act of 24 September 2010 on the Population Register) and one of the national notified eID means – trusted profile (pl. *profil zaufany*). Having a PESEL number and a trusted profile opens access to all Polish public digital services. Moreover, Poland allows access to certain public digital services for holders of notified eID means from other Member States through the [biznes.gov.pl](https://biznes.gov.pl) domain.

## Malta (MT, not interviewed)

Identity Malta Agency, being Malta's identity management national authority has successfully pre-notified the Maltese scheme of the Maltese eID card and e-Residence documents and has been confirmed as achieving level of assurance "high" in line with the e-IDAS Regulation. In Malta the e-IDAS Node permits Maltese citizens to use digital public services of other EU MS and gives European citizens access to the digital services of the Maltese government. It provides for a reliable authentication mechanism and allows for the mutual recognition of national electronic identification schemes. The technical infrastructure is operated by MITA, being the public entity vested with the responsibility to provide ICT infrastructures, systems, and services to the Government of Malta.

## Spain (ES, interviewed)

The Spanish national identity card, known as the *Documento Nacional de Identidad* (DNI) or *carnet de identidad*, contains the following information:

- Last names (all Spanish citizens are required to have two last names)
- First name
- Gender
- Nationality
- Date of birth
- Serial number, which includes a security feature, expiry date, and signature of the cardholder
- Photo of the cardholder, in black and white and a bigger size than all the previous cards
- DNI number and security letter under the photograph

The Spanish ID card has evolved over time, and the current version is an electronic identity card with unique features.<sup>[43]</sup>

### Providing identifier

The DNI is issued by the National Police and is mandatory for Spanish citizens (fourteen years or older). The same identity number (identifier) is also used for tax purposes, receiving the name of *Número de identificación fiscal* (NIF)<sup>[44]</sup>. The NIF has 9 digits, with the first digit being a letter that denotes the type of entity, and the last digit being a check digit that can also be a letter.<sup>[45]</sup> The format of the NIF depends on the type of entity it represents:

- For individuals: The NIF for individuals is the same code as their identity document. For Spanish citizens, it will be the DNI (Documento Nacional de Identidad), which consists of 8 digits and one letter for security. The letter is found by taking all 8 digits as a number and dividing it by 23. The remainder of this digit, which is between 0 and 22, gives the letter used for security. The letters I, Ñ, O, U are not used. The letters I and O are omitted to avoid confusion with the numbers 0 and 1, while the Ñ is absent to avoid confusion with the letter N.
- For foreigners residing in Spain, the NIF will be the NIE (Número de Identificación de Extranjero), which is 9 characters in the format A-NNNNNNNA, where the first character is either X, Y or Z and the last character is a checksum letter.<sup>[46]</sup>
- For legal entities: The NIF format for legal entities consists of a letter that will depend on the legal form it has, 7 digits, and the control code that can be a letter or a number.

Foreigners legally residing in Spain or who intend to purchase property are issued with a *Número de Identificación de extranjero* (NIE) or Foreign Identification Number<sup>[47]</sup>:

- If they are nationals of other Member States, they use their own national identity card to prove their personal identity (e.g., a French CIE) but they use their NIE as identifier for any relationship in Spain.
- If they are nationals of third countries, they get issued a *Tarjeta de Identidad de Extranjero* (TIE) or Foreigner Identity Card,<sup>[48]</sup> containing the NIE identifier, which they use to prove their personal identity. The NIE is also used for tax purposes.

---

43. <https://www.mobbeel.com/en/blog/spanish-id-cards-evolution-and-meaning-of-dni-3-0-fields/>

44. <https://www.norden.org/en/project/single-digital-gateway-once-only-proof-concept-pilot-project>

45. <https://taxid.pro/docs/countries/spain>

46. <https://www.tas-consultoria.com/blog-en/nif-spain-obtain/>

47. <https://www.norden.org/en/project/single-digital-gateway-once-only-proof-concept-pilot-project>

48. <https://visaguide.world/europe/spain-visa/foreigner-identity-card/>

The Foreigner Identity Card (TIE) which is issued to foreigners authorized to stay in Spain for more than six months<sup>[49]</sup>:

- The card contains the individual's information, name, surname, period of validity, and a unique number known as the Foreigner Identity Number (NIE)
- The NIE is a personal unique number given to every foreigner who intends to stay in Spain longer than six months and appears on all documents of the foreigner processed and issued in Spain, including the Foreigner Identity Card
- The identity and record matching system in Spain is done to increase the success rate of identity and record matching done on the side of the Online Procedure Portal<sup>[50]</sup>

There are several digital options available in Spain for applying for a personal ID or using public services:

- **Spanish Digital ID:** Spanish citizens and non-Spanish legal residents can apply for a digital ID online, register with the system using a DNIe or previously installed FNMT (*Fábrica Nacional de Moneda y Timbre*) digital certificate, or apply for a digital certificate from the National Currency and Stamp Manufacturer (*Fábrica Nacional de Moneda y Timbre*)<sup>[51]</sup>
- **Digital Certificate:** A digital certificate is needed to verify a person's identity online and formalize any legal process effectively. It can be obtained by any Spanish or foreign citizen over 18 years old who holds a DNI, NIE, or NIF, from the Sede Electrónica website. The certificate can be used to sign and prove identity safely online and allows the holder to do online procedures with the Spanish Public Administration, such as paying taxes, applying for certificates from the Civil Registry, or applying for the Spanish Criminal Record Certificate.<sup>[52]</sup> It is also needed not only to register as self-employed (*Autónomo*), but also to register documents when person is applying for TIE, making tax declarations, and joining the Social Security system, among other things<sup>[53]</sup>

## Identity matching

To obtain a digital certificate, an applicant needs to fill in personal information such as NIE, first surname, and email address. The process may require video identification and may cost a fee.

Not all municipalities are digitally approachable for using services. That depends on the size of municipality and the regional governments support to the digital services.

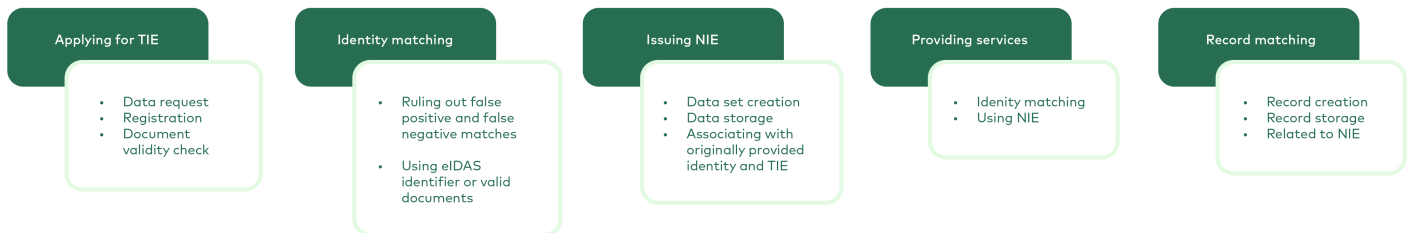
---

49. Full list of services is available in the Annex II of SDGR: <https://eur-lex.europa.eu/TodayOJ/>  
50. <https://ec.europa.eu/digital-building-blocks/wikis/display/TDD/2.1+-+Identity+and+Record+Matching+-+Q1+2023>  
51. <https://www.barcelona-metropolitan.com/living/settling-in/how-to-get-your-spanish-digital-id/>  
52. <https://www.exteriores.gob.es/Consulados/toronto/en/ServiciosConsulares/Paginas/Consular/digital-certificate.aspx>  
53. <https://www.ageinspain.org/post/digital-certificate-guide>

- In smaller municipalities (up to approximately 50 000 inhabitants) mostly or only data sharing "on paper" is in use.
- Larger municipalities (starting from approximately 50 000 inhabitants) also provide digital services for persons who have national identity (personal code and digital certificates).

For several years there has been an active push from the government to use electronic id. E.g., regarding taxes and any introduction to public services eID is a main key in terms of public services (see Figure 2).

- The TIE application process requires the submission of various documents, including proof of identity and capacity, and foreign documents must be legalized or apostilled and, where applicable, must be submitted together with an official translation into Spanish<sup>[54][55]</sup>
  1. The student must apply for a Foreigner Identity Card within a period of one month from their entry into Spain, at the Foreign Nationals' Office or the Police.



**Figure 2** High level process of Identity and record matching in Spain

### Data sharing and record matching

Already identified users (with valid TIE) can connect either by national or eIDAS identifier. When connecting digitally, a respective choice will be presented to the person to use national or eIDAS identifier.

54. <https://www.exteriores.gob.es/Consulados/londres/en/ServiciosConsulares/Paginas/Consular/Visado-de-trabajo-por-cuenta-ajena.aspx>  
 55. <https://www.exteriores.gob.es/Consulados/londres/en/ServiciosConsulares/Paginas/Consular/Visado-de-trabajo-por-cuenta-ajena.aspx>

- Today it is possible to recognize EU Member States identifier as well as save it and use it for identity.
  1. Earlier data about the past of a foreigner cannot be matched.
  2. If a person is from the EU, then eIDAS identifier can be used for identity matching.
  3. France and Portugal create the most of identity matching cases. Both citizens can use their national electronic ID
  4. If a person is not from the EU, then a PIN based account can be made.

National ID has to be the Spanish identifier for most local services, but there are some sectoral exceptions and issues regarding (see Table 5):

- **services meant only for residents:** to use those one must have Spanish national ID. For the rest of the services also other countries national ID can be presented.
- **banking:** privacy focused now, so when person is asking credit from bank in Spain, then only identity is not enough, but person can decide, what data to present. Still the bank can refuse to serve if the data are not enough.
- **education:** When person needs to get in contract with university the problem raises when there is need to provide current degree from abroad – the documentation must be translated to Spanish and proofed by certified authority. Older diplomas from years ago are not digitized. In EU degrees from recent years are in digital database and most EU universities can share their records (degrees). (see Ch 2.2.1).
  1. Matching issues remain in regards of name changes or with people from third countries. For those people a new sectoral identity must be created, and data connection made to an earlier degree.
  2. No automatic connection between a person' s new and former sectoral ID-s are made.

**Table 5** Spain – identity and record matching related issues

Regarding	Description of the issue	Solved how?	IF not 100% solved, then why?
Process	Smaller municipalities are not providing digital services	Government policy and nudging towards digital services	Depends on decision and available funds of every municipality
Subject	Sectoral ID-s are causing multiple identities	Manual connections are made between data and identities	-
Object	eIDAS – number of credentials is too limited for the Spanish national ID	Creating national Identifier for the person (duplicated identity)	-
Regulation	eIDAS data set limits set by regulation	-	Not under control of single Member State
Relying Parties	-	-	-
Technology	-	-	-
Infrastructure	-	-	-
EU	-	-	-

Compiled according to the interview with the representative of University of Murcia (expert of security and identity related topics)

Summary of differences in the process of obtaining a digital certificate for foreigners (for use in Spain):

- Foreigners need to obtain a Foreigner's Identity Number (NIE) before applying for a digital certificate. The NIE is a unique identification number assigned to foreigners in Spain, and it is required for all financial and administrative matters.<sup>[56]</sup>
- Foreigners can apply for a digital certificate online through the Sede Electrónica website, just like Spanish citizens. However, the application process may require additional documentation, such as a copy of the applicant's passport and a copy of their NIE.<sup>[57]</sup>
- Foreigners may need to provide proof of their legal status in Spain, such as a residency certificate or a work permit, to obtain a digital certificate.
- The process of video identification may be different for foreigners, depending on their legal status in Spain. For example, non-residents may need to provide additional documentation to complete the video identification process.
- To summarise, while the process of obtaining a digital certificate is similar for Spanish citizens and foreigners, foreigners may need to provide additional documentation and proof of their legal status in Spain.

### Luxembourg (LU, interviewed)

In Luxembourg, identity matching of citizens relies on a persistent national identification number, as foreseen by the law of 19th June 2013 on identification of natural persons.<sup>[58]</sup> An identification number is assigned to every natural person registered in Luxembourg's national register of natural persons, which includes nationals, residents, and any person interacting with a national public administration using this number.

### Providing identifier

Foreign citizens can obtain a LU national identification number via various registration processes, including fully online if they own an eID means notified under eIDAS. When a person from abroad requests for LU national ID, an eIDAS identification is used today. To support the process, the original minimum dataset required for LU national ID was changed, as previously gender was asked, but e.g., Germany doesn't provide this attribute. That means using only eIDAS minimum dataset today (see Table 6).

---

56. <https://costaluzlawyers.es/for-you/a-full-guide-on-residency-and-nationality-options-in-spain/>

57. <https://costaluzlawyers.es/blog/fag-guide-to-the-new-digital-nomad-visa-in-spain/>

58. <https://legilux.public.lu/eli/etat/leg/loi/2013/06/19/n3/jo>



The Luxembourg national identification number has a different format for natural and non-natural persons.

- For non-natural persons, the identifier has 11 digits, and the last digit is a check digit.<sup>[59]</sup>
- For natural persons the national identification number for natural persons has 13 digits<sup>[60]</sup>. The digits in the national identification number represent the following data:
  1. RRRRRR: Birth date of the person in the format YYMMDD
  2. SSS: Serial number assigned by the National Registry of Natural Persons
  3. C: Check digit

To evidence the information required for the creation of the national identification number, the natural person should provide the following information: names, surname, date, place, and country of birth, gender, nationality, and private address.<sup>[61]</sup>

---

59. <https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/tax-identification-numbers/Luxembourg-TIN.pdf>

60. <https://guichet.public.lu/en/support/glossaire/rnpp.html>

61. <https://www.mondaq.com/shareholders/1190004/registration-of-luxembourg-national-identification-numbers-numro-de-matricule-with-the-luxembourg-register-of-commerce-and-companies>

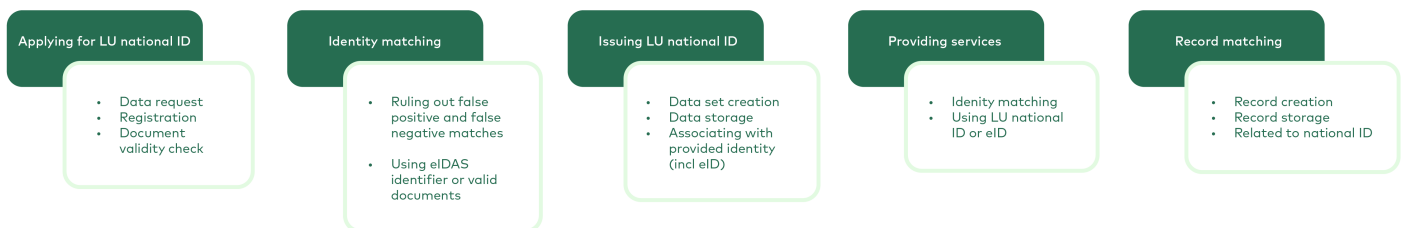
**Table 6** Luxembourg – identity and record matching related issues

Regarding	Description of the issue	Solved how?	not solved why?
Process	Sector specific approach to datasets and sharing principals	Some data are shared "on paper", which means not shared digitally.	No standardized approach agreed in state, sector specific processes
Subject	Citizen from abroad can have multiple eID's from same country or different country.	Manually associating the various eIDs with a single LU identity (i.e., the one in LU national population register). National population register calling the person, requesting documents, checking, and then merging data.	-
Object	Legislation prohibits to share national ID number with parties abroad	Derived unique identifier based on LU national ID number, created by algorithm, by country and by relying party. The same code is used also in the future and tied: unique person eID = requesting country + requesting organization	National regulations
Regulation	ID number cannot be saved by private sector (with some exception, e.g., healthcare)	Person can choose what to share by giving an official consent	National regulations
Relying Parties	Largely sector specific processes	-	Every sector and organization are deciding their solution. Private sector cannot store national ID number, with a few exceptions which are all enumerated in a national law
Technology	-	-	-
Infrastructure	-	-	-
EU	Pinpointing false positive or negative matching cases	-	eIDAS minimum dataset

## Identity matching

Matching and providing of services is based on national identifier – 1 identifier per natural person. When asking for service, one must provide the national ID, which is a primary key to access all the information in various databases.

- Person can apply for national ID via web page<sup>[62]</sup> by providing minimal set of data. If additional data is required, the consent will be asked, and applicant can decide whether to share more data or not. All additional checks (points 1,2,3 below) are done separately and manually by agents of the National Population Register service, outside of the online eIDAS-based registration.
  1. Identity document and facial biometry matching,<sup>[63]</sup> number of checks done on the document (is it genuine) according to procedures. Physical set (EU ID documents database PRADO,<sup>[64]</sup> describes how the document should look like), the same information about ID documents from outside EU is also available.
  2. Electronic security – chip with signed data from member state, mobile app is used for that.
  3. Question of document validity – many public sector institutions have no access to the SLTD database to check is this document stolen for example? In case of doubt the authorities of issuing MS will be contacted.
- Business owner is connected to the company, that must be registered in Luxembourg. EU network business register BRIS<sup>[65]</sup> links all the business registers data from all MS's.



**Figure 3** High level process of Identity and record matching in Luxembourg

62. [https://eidas.services-publics.lu/cisie-sp/initRegistration?reg\\_lang=en](https://eidas.services-publics.lu/cisie-sp/initRegistration?reg_lang=en)

63. A civil servant will visually compare a person's face with the photo on a presented ID document. There is no kind of automated or computer-based face recognition/matching system in use.

64. <https://www.consilium.europa.eu/prado/en/prado-start-page.html>

65. [https://e-justice.europa.eu/content\\_business\\_registers\\_at\\_european\\_level-105-en.do](https://e-justice.europa.eu/content_business_registers_at_european_level-105-en.do)

## Data sharing and record matching

Every person with LU national ID can have a personal digital space provided by LU on the national citizen portal (MyGuichet.lu)– where the person can use different services. This service is available to everyone with a national identifier, but a person must request its creation. There are some issues (Table 6):

- Citizens can have multiple eID from the same country or different countries, as well as different names for some cases. Unique identifiers provided by various eID means of single person are not matching, so different identities must be manually associated. For this association the National Population Register will call the person, requesting documents, checking, and then merging data.
- Private and public sector service providers options are quite different.
  1. In the public sector all sector-specific processes rely on the national identification number. And public administrations supporting these processes have access to the central national population register.
  2. But national ID numbers cannot be stored by the private sector, therefore they must use another way to identify the person.
  3. On education field depends on University, but mainly the data should be provided "on paper". Some Universities in certain networks can exchange data directly.
  4. Medical sector – patient history from abroad is shared mainly "on paper."
  5. Financial sector - some banks are online, some have digitalized part of their bank account opening process, some are still operating with data sharing "on paper".

When interacting with LU public entities, citizens provide their identification number for identity matching. Alternatively, they may use their notified eID means and authenticate via eIDAS, since their eID means has been associated with their national identification number during registration.<sup>[66]</sup>

## Netherlands (NL, interviewed)

In the Netherlands, online unique identification in the public sector is often established by comparing a citizen's Citizen Service Number (CSN) to a record of that citizen at a public RP<sup>[67]</sup> (Moniava et al., 2008). The possession of a CSN is for instance required for accessing tax records. There are however public services which do not require unique identification with an CSN: for example, when requesting the photo taken of the car responsible for a speeding ticket at the CJIB (the Dutch Central Judicial Collection Agency).

---

66. <https://legilux.public.lu/eli/etat/leg/loi/2013/06/19/n3/jq>

67. Relying Parties

## Providing identifier

Dutch CSN is a unique number of 9 digits, including check digit; that contains no personal data.

Besides the CSN, the following four unique and persistent identifiers are used in the Dutch eIDAS identity matching process of foreign eID means (Nora, 2017; Verheul, 2019).

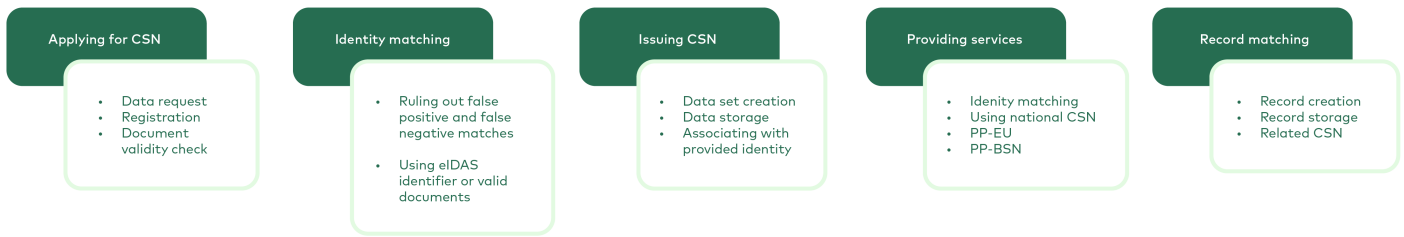
- **eIDAS identifier:** the identifier which is used in the eIDAS minimum data set (PID). For each MS, the identifier is formatted as:  
[home\_MS/destination\_MS/ID (e.g., GE/NL/1234AB)]
- **PP-EU:** a polymorphic pseudonym which is derived from the eIDAS identifier. This identifier is used for Dutch RPs in the private sector.
- **PP-BSN:** a polymorphic pseudonym which is derived from the BSN. Every eID mean a citizen uses receives a different PP-BSN. The BSN is only derivable from the PPBSN by Dutch RPs which have a decryption key. This key is only given to authorized RPs.
- **PP-RP:** a pseudonym specifically for each Dutch RPs. It is a pseudonym of the former two identifiers (the PP-EU, PP-BSN), constructed by encrypting this identifier with the public key of the RP. Therefore, only the authorized Dutch RP can derive the decrypted identifier. A RP does not have access to the PP-EU, PP-BSN, and PP-PS: they are only for internal communication between the Dutch eIDAS Connector and the BSN Connector.<sup>[68]</sup>

## Identity matching

Focus on identity matching is to avoid false positive matches first and only after those false negative ones. Matching is done starting with surname and date of birth (age). In case of one positive match, additional ID document data are asked, if these are not shared then last 3 digits of CSN is provided and confirmation is asked from the person. If more than one match is found in the database, then the matching is forwarded immediately to the manual process (back office). More attributes will be asked from the country of origin and the person must give consent for that. If still in doubt, then identity match won't be done to avoid false positive and possible frauds caused by it. (see Figure 4)

---

68. <https://repository.tudelft.nl/islandora/object/uuid%3A5d52babb-c6b0-4c96-8f93-8f3129ba448d>



**Figure 4** High level process of Identity and record matching in Netherlands

Matching itself is not a problem, the data are – e.g., people already with multiple identities in other countries and in addition there are problems with old identity documents. The more identity related data is gathered through time, the better the matching will be.

A person with no eID code must come to the physical location and present ID (paper documents, ID card) Local ID document is linked to the name, date of birth, gender, nationality, and home address. For people from abroad the main identity matching attributes are birth date and family name. In case of doubt the data of parents are requested, but sharing these is not obligatory. Still, when refused to share this information, and if it leaves doubt of person's original identity (from abroad), this can end up with refusal to provide CSN. (see the list of issues at Table 7)

It is possible to connect identities manually. This option was created because of 2 main reasons:

- Differences in spelling of names in different languages (e.g., prefix De': In Netherland it is separated, in Belgium it is concatenated into one name)
- Very common names with even together with birth date can give more than 1 positive hits from database. (e.g., German surname with a very common name in Netherlands can give up to 10 hits with the same birth date).

On the other hand, it creates another problem, where connections could be made recklessly. To prevent that from happening the procedure allows only 2 people to connect identities, and related logs are stored.

### Data sharing and record matching

In the Netherlands, all public organizations working with personal data use the Citizen's Service Number to identify people and to communicate between public organizations. Without this CSN it is not possible to access most of the public services of more than 1000 government institutions.

**Table 7** Netherlands – identity and record matching related issues

Regarding	Description of the issue	Solved how?	If not 100% solved, then why?
Process	Person who doesn't have CSN code, must come to the office and present data	From abroad people can connect via eIDAS and can use eIDAS identifier.	Still physical presence is required for identity matching
Subject	False negative matches can happen because of the spelling differences between languages	The name details (letter combinations like name prefixes etc.) are coded to match language specific changes in the surname	Focus is on avoiding false positive matches.
Object	More than one positive hits from database	In case of 2 positive hits person is asked to confirm last 3 digits of CSN (yes/no) Manual connection of identities is possible	If still in doubt, then the connection of identities will not be done (to avoid false positive and possible frauds)
Regulation	In case of doubt in >1 positive hits legislation prevents from demanding additional data. Either new identity should be provided, or identity connection made.	Person is asked to share data voluntarily	Person can refuse sharing additional data and public services must be provided still but under new identity
Relying Parties	Most public service providers have their own systems established	One central database with all the persons, accessible to all service providers	-
Technology	-	-	-
Infrastructure	-	-	-
EU	-	-	-

Compiled according to the interview with the representative of the National Office for Identity Data (Ministry of the Interior and Kingdom Relations)

Incoming eIDAS-traffic comes with a Unique ID and attributes (name, surname, date of birth). Service will be provided if the attributes can be matched to a registered identity.

## Norway (NO, interviewed)

### Providing identifier

The identification process requirements when applying for identification documents depends on an individual's citizenship and the basis for their residence permit in Norway<sup>[69]</sup> and it includes data sharing "on paper".

- Nordic citizen: Norway, Sweden, Iceland, Finland, Denmark, the Faroe Islands or Greenland
  1. Passport or national ID card with a photograph of the person and information about the person's citizenship and gender is required. When moving to Norway from another Nordic country, a valid driving license will also be accepted, together with a printout from the national population register of the country one is moving from, with information about citizenship and gender. The printout must be dated and no older than three months. It must also be signed and stamped.
  2. Children under the age of 18 may use their birth certificate/printed confirmation of their birth registration from the National Population Register in a Nordic country together with a passport photo and a printout from their home country's national population register that shows their citizenship and gender. The printout must be no older than three months. It must also be signed and stamped.
- EU/EEA/EFTA citizens: Passport or national ID card with a photograph and information about citizenship and gender.
- There are some exemptions for some groups, like asylum seekers, refugees, persons who are unable to get a passport from their home country, and others.

The Anti-Money Laundering (AML) legislation requires that customers provide valid proof of identity when entering a customer relationship. Valid proof of identity includes Norwegian and foreign passports, Norwegian national ID cards, Norwegian driving licenses, Norwegian bank cards with photographs, national ID cards issued by an EEA country, Norwegian immigrant's passport, Norwegian refugee travel document, and electronic proof of identity in accordance with the AML Regulations.<sup>[70]</sup>

---

69. <https://www.skatteetaten.no/en/person/national-registry/identitetsnummer/id-kontroll/>

70. <https://www.finanstilsynet.no/en/topics/money-laundering-and-financing-of-terrorism/the-aml-legislation-and-requirements-for-valid-proof-of-identity/>



For permanent ID any person should have a permit for residency – this can be acquired by presenting a passport (ID document).

- To apply for work, permit also sending documents is accepted today, but the quality of this method is questionable and will most probably be discontinued. Physically appearing to receive the work permit the office.
- Enrolment for ID cannot be done digitally today. It is under decision whether to issue national identity card for foreigners, but still, physical appearance is required to receive the ID document.

All together **three kinds of identifiers** can be defined regarding Norway:

- Personal unique identifier, restricted by population register legislation, prevents changes of attributes, as every change requires change in the legislation.
- Internal identifier – sectoral numbers (like in taxation or health care)
- Third identifier is under consideration – which would be more flexible in regards of Norway legislation and would allow additional attributes and change of some data (like address and similar).

**A national identity number consists of eleven digits**<sup>[71]</sup>:

- Date of birth: In most cases, the date of birth is the first six digits. For example, if person is born on 22 June 1976, the first six digits in your national identity number are 220676.
- Individual number: The next three digits are individual numbers, where the third digit refers to the holder's gender: even numbers for women and odd numbers for men.
- Verification number: The two last digits are for verification.
- The last five digits in the national identity number can be referred to as a "personal number".
- In some cases, the first six digits are not the date of birth – in case there are no available national identity numbers for some dates. Then, the first six digits will show the day and month on which person received your national identity number instead. The correct date of birth will still be recorded in the National Population Register in the field for date of birth.

Changing information regarding one's identity is possible: person can apply to change their registered information regarding place of birth, country of birth, citizenship, and date of birth through the Norwegian Tax Administration.<sup>[72]</sup>

---

71. <https://www.skatteetaten.no/en/person/national-registry/identitetsnummer/fodselsnummer/>

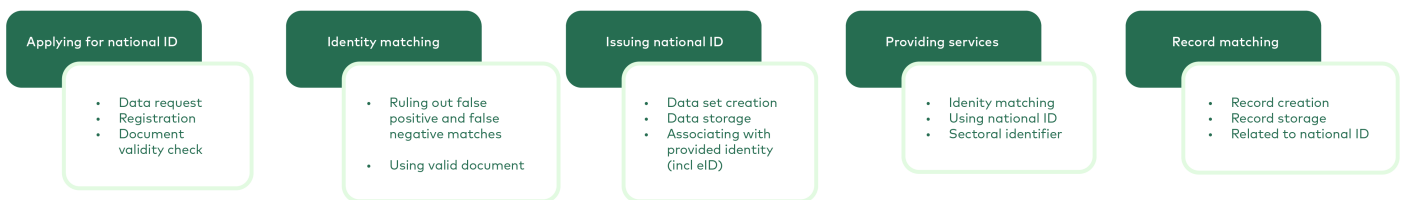
72. <https://www.skatteetaten.no/en/person/national-registry/change/information-regarding-your-identity/>

## Identity matching

All foreigners working onshore in Norway are required to meet at a tax office for an ID control to verify their identity.<sup>[73]</sup> Tax Administration offers ID checks in 42 selected tax offices.

Data sharing "on paper" is only under discussion if a person cannot be identified with regular processes. Norway focuses first on avoiding frauds with multiple identities – so priority is to avoid false negative matches and right after those false positives. (see also Figure 5)

The **status of person's identity basis** can be either checked or not checked<sup>[74]</sup> in the National Population Register. An ID check is an identity and identification check. To undergo an ID check, one must attend in person and show an identification document. Information of one's "ID check" status will be registered in the National Population Register, and it is available to public and private enterprises that use the National Population Register. It can be decisive for access to several rights whether a person's identity has been registered as checked in the National Population Register. It is the relevant public or private enterprise offering a service that determines whether identity needs to be checked to use their services.



**Figure 5** High level process of Identity and record matching in Norway

Biometric data are considered sensitive and not used for eID. It is considered using web apps for digital biometric enrolment, but not explored much so far. Central passports register stores photos and fingerprints, and these data can be checked, to make sure that no duplicate identities are created. However, double identities cannot be completely ruled out since one-to-many queries are not allowed with biometrics. Biometrics can only be used for a 1:1 comparison, to make sure that the person is who he/she claims to be. This process is under the control of the police. Current legislation does not comply with the identity matching solutions connected to biometric data. Uniqueness and quality of personal identity decreases, therefore. (see the list of issues at Table 8)

73. <https://blogg.magnuslegal.no/en/id-control-for-foreign-employees-in-norway>

74. <https://www.skatteetaten.no/en/person/national-registry/identitetsnummer/id-kontroll/>

## Data sharing and record matching

The population register is very high quality, and it is very often used as a comparison for other systems, which means that national identity number is used very widely. If people from abroad cannot be connected to the registered ID number, it is not possible to use public services. There are some exceptions – e.g., applying to university or paying taxes, for that internal identifiers are used. Health care also handles foreign patients – who don't get Norwegian identifiers, and very limited range of digital services are accessible for them. In corona pandemic situation those internal identifiers were temporarily used as a person's identifier in Norway, but this system was not extended.



According to the interview: to improve identity matching for Norway, sharing internationally the unique national identifier of person, from his/her country of origin would be very helpful. Regarding Nordic countries at least as well as countries that Norway have relations. This can be considered because of some bilateral agreements and several large service providers, who already have this information. In many cases today the national identifier of other countries is stored in the population register, which increases the hit rate significantly.

**Table 8** Norway – identity and record matching related issues

Regarding	Description of the issue	Solved how?	If not 100% solved, then why?
Subject	If persons from abroad cannot be connected to the registered ID number, it is not possible to use public services.	Sectoral internal identifiers are used. In corona pandemic situation those internal identifiers were temporarily used as a person's identifier in Norway, but this system was not extended.	There are some exceptions – e.g., applying to university, paying taxes or receiving critical health care.
Object	People have a long history and rights for services (like pensions). They come with a minimum data set from abroad or with a passport. And data quality differs a lot therefore.	A person is asked to share additional data and documents to find a match. Status of identity check is available to public and private enterprises that use the National Population Register.	Inflexibility in population register and rigorous government systems connected to that register.
Regulation	Personal unique identifier related regulation prevents changes of attributes	Third identifier is under consideration – which would be more flexible in regards of Norway legislation and would allow additional attributes and change of some data.	Restricted by Population Register legislation and therefore every change requires change in the legislation.
Relying Parties	Data is not shared between countries flexibly.	Physically appearing to present data and or receive work permit or ID document.	Variations of legislation of population registers in different countries.
Technology	-	-	-
Infrastructure	-	-	-
Cultural	People are not ready to consider possibility to use EU unified identifiers.	-	-
EU	In some cases, it is not possible to find a user in the eIDAS register, even if the person is registered.	-	eIDAS mandates sharing information but does not mandate access to services.

Compiled according to the interview with the representative of The Directorate of Digitalisation

## Estonia (EE, interviewed)

Estonia has personal identification code and ID documents as many other countries, that allow foreigners to deal with their personal or business matters.

### Providing identifier

All Estonians, no matter where they happen to reside, have a state-issued digital identity. This electronic identity system, called eID, has existed since year 2002 and is the cornerstone of the country's e-state. e-ID and the ecosystem around it is part of any citizen's daily transactions in the public and private sectors. All Estonian eID tools operate primarily on the Estonian personal identification code for identification. People use their e-IDs to pay bills, vote online, sign contracts, shop, access their health information, and much more.<sup>[75]</sup>

ID-card is mandatory for every Estonian citizen and residence card is mandatory for all residents living in Estonia. Estonians can use their e-ID via state-issued ID-card, using Mobile-ID, which can be used on any mobile device with SMS functionality, or Smart ID app on their smartphones. Holders of a digital identity need not be Estonian residents anymore, however.

Since 2014, an **e-residency of Estonia** (also called virtual residency or E-residency) concept was implemented for anyone who wishes to become an e-resident of Estonia and access its diverse digital services, regardless of citizenship or location. Behind that is an aim to make it easier for foreigners to access Estonian business environment remotely and thereby attract location-independent entrepreneurs such as software developers.

E-Residency of Estonia is a program that enables creating a borderless digital society for global citizens. The program provides holders of e-Residency with a transnational digital identity (e-Resident's digital ID) that allows to securely authenticate non-Estonians in Estonian online services, such as company formation, banking, payment processing, and taxation and sign documents.

**A personal identification code** is a number formed based on the gender and date of birth of a person which allows the specific identification of the person.<sup>[76]</sup> The basis for the formation of personal identification codes is:

- the EVS 585:2007 standard "Personal identification code. Structure"
- the Population Register Act
- and the regulation by the Minister of the Interior which regulates the formation, distribution and granting of personal identification codes.

---

75. <https://e-estonia.com/solutions/e-identity/e-residency/>

76. <https://www.siseministeerium.ee/en/activities/population-procedures/population-register#personal-identificat>

Personal identification code consists of 11 digits, the first of which shows the gender of a person as well as the century of birth, and the next six show his or her date of birth. The following three digits are sequential numbers for children born on the same day and the last is a control number which is calculated according to a special formula.



A person of the third gender must choose a gender on a dual scale, either "female" or "male". The structure of the Estonian personal identification code does not support the third gender and the code cannot be changed very easily; the change would be very costly for the state. (see the list of issues at Table 9)

The personal identification code is provided during the registration of family events, but it is not provided based on family relationships (for example, a personal identification code is given to a child born abroad to an Estonian citizen, but not to their foreign parent who has no other connection to Estonia).

In the case of residing in Estonia, it doesn't matter whether it is temporary or permanent residency. If a person obtains the right of residence or a residence permit for living in Estonia, they will also receive a personal identification code. However, a personal identification code is not provided to foreign nationals staying in Estonia based on a long-term (e.g., one-year) visa.

- If an individual stays in Estonia temporarily; for example, lives in Latvia but works in Estonia, he or she may **apply for a personal identification code** in the nearest local government of the county centre in person. If an individual cannot apply in Estonia, he or she can do so in an Estonian foreign mission in a foreign state.
- Citizens of the European Union can submit their application for a personal identification code to the local government agency together with their notice of residence.

**Foreigners can** apply for e-Residency in Estonia, according to these steps (During this process, the person will be assigned an Estonian personal identification code):

- Check eligibility: Foreigners who want to apply for e-Residency in Estonia must ensure that they have a clear understanding of the reason they are applying for e-Residency<sup>[77]</sup>
- Apply for an e-Residency digital ID: Foreigners can apply for an e-Residency digital ID, which provides access to Estonia's business environment, by applying to the Estonian Police and Border Guard Board (PBGB).<sup>[78][79][80]</sup>

---

77. <https://learn.e-resident.gov.ee/hc/en-us/articles/360000625078-Who-is-eligible>

78. <https://www.politsei.ee/en/instructions/e-resident-s-digital-id/frequently-asked-questions>

79. <https://e-estonia.com/solutions/e-identity/e-residency/>

80. <https://www.theguardian.com/world/2014/dec/26/estonia-offers-e-residency-to-world-what-does-it-mean>

1. Submit identification documents: The identification documents accepted by the PBGB are passports or European Union identity cards<sup>[81]</sup>
  2. During the application process, applicants will need to provide their CV, motivation statement, copy of their travel document/ID, and passport-style digital photo<sup>[82]</sup>
- Pay the application fee: Applicants need to pay the application fee using VISA or Mastercard
  - Wait for approval and card delivery: The Estonian Police and Border Guard Board will review the application and conduct a background check. Applicants may be asked additional questions for clarification purposes. Once the processing of the application is complete, the applicant will be notified by email. After the application is approved, the unique card is printed and delivered to the chosen pickup location.
  - Collect the e-Residency digital ID: Applicants can collect their e-Residency digital IDs at the PBGB service office indicated in the application or at an Estonian embassy. That means applicants need to cover also travel costs to get to the pickup location.

Granting a personal identification code does not grant the right to stay, live or work in Estonia – these rights must proceed from other bases prescribed by law. A personal identification code shall be granted to a person after they are entered in the Population Register.

In any case, once the personal identity code (identity) is created in the Population Register, it will be stored there forever and never will be archived. Therefore, in time, different status is added to the identity, depending on the status of the person (e.g., "living" or "deceased"). Every service provider can decide themselves which identity statuses are acceptable for providing their services.

## Identity matching

**Foreigners who apply for a personal ID number** in Estonia, which is different from e-residency, go through an identity matching process (see Figure 6):

- Application: The applicant must apply for a personal ID number to the Estonian government
- Verification of identity: The applicant must provide proof of identity, such as a passport or national ID card, to verify their identity.
  1. False positives are prevented, as possibly duplicated identities are not automatically merged, but will be manually validated<sup>[83]</sup>

---

81. <https://learn.e-resident.gov.ee/hc/en-us/articles/360000633237-How-to-apply-FAQ>

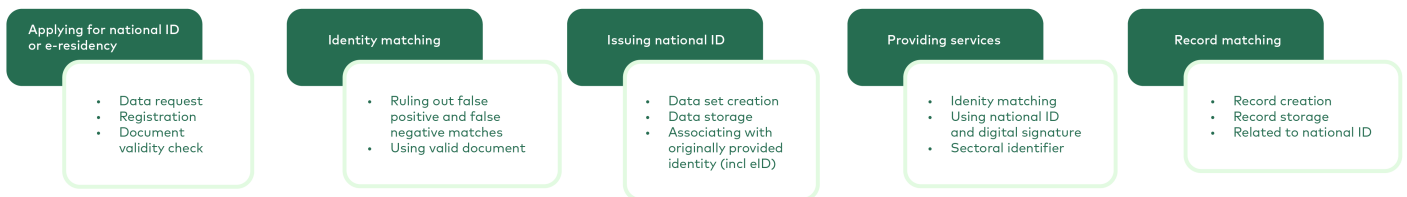
82. <https://www.e-resident.gov.ee/become-an-e-resident/>

83. This is done by officials who, based on experience, send queries with different datasets to various databases, to find possible previous EE identities.

- Issuance of personal ID number: If the applicant passes the verification (population register) the Estonian government issues them a personal ID number.

**Foreigners who wish to obtain an Estonian identity document** and/or e-residency must also go through identity matching process (Refer to Step 2 in previous list and Figure 6).

- Once the identity matching process is complete, foreigners can use their e-Residency digital ID to access Estonian public e-services, declare Estonian taxes online, and more.



**Figure 6** High level process of Identity and record matching in Estonia

With an Estonian citizen who has a valid ID document, everything is simple and clear. If a foreigner applies to a municipality for example in connection with the registration of a place of residence, a simple search will be carried out on applicant in the Population Register in different combinations (if necessary, the surname will also be excluded from the search if it has been changed). The problem may arise **if the search is not carried out with sufficient thoroughness, because if a match is not found, then the local government will create a new identity.** Later, when duplications are detected, the Population Register connects the identities manually.



When applying for an identity document, for example, the Police and Border Guard Board (PBGB) accepts the application and tries to identify the person based on the data of the Population Register. If no match is found, PBGB will order the creation of personal code from the Information Technology and Development Centre (SMIT) of the Ministry of the Interior, while SMIT will not initiate the creation of a personal identification code without prior search in the Population Register. SMIT's extensive experience in performing searches helps prevent the creation of duplicate identities.



Digitally, identity cannot be matched with eIDAS now. Estonian e-services operate mainly based on an Estonian personal identification code, and today there is no e-service solution that could issue an Estonian personal identification code to the user of the eIDAS eID tool (incl. the identifier provided therein).

Population Register can also add the foreign personal identification code to the identity data and these data are collected whenever possible. It is still entered in the free text field since the **actual quality of the foreign personal identification code obtained is not known**. However, this information has legal significance, as does any other information entered.

### Data sharing and record matching

Once the e-Residency digital ID is collected, foreigners can use it to access Estonian public e-services, declare Estonian taxes online, and more as described earlier.

In this regard, a distinction must be made between two types of IDs. Personal identification code, which is used for entry into the state's data system, and database-based unique identifier (UID), used to identify and link a person's data solely within a specific database. In the latter case, the document will not be issued, only the code. This code is used for example when the employer needs to formalize the person's employment in the Workers' Register. As this employee will never come to Estonia, he/she does not need an Estonian identity document.

There are extremely few people who do not have a personal identification code in Estonia and who at the same time receive any service.

**Table 9** Estonia – identity and record matching related issues

Regarding	Description of the issue	Solved how?	If not 100% solved, then why?
Subject	-	-	-
Object	Digital association with eIDAS is not possible yet	-	-
Regulation	For personal ID an applicant must choose gender on a dual scale (female/male)	There are ongoing discussions how to build multiple scale for describing gender	The gender is built in the personal ID code and cannot be excluded.
Relying Parties	Quality of background check depends quite often on the experience of the person conducting search	In most cases the process brings the identity matching to the most experienced party (SMIT) and the duplication will be discovered	-
Technology	-	-	-
Infrastructure	-	-	-
Cultural	-	-	-
EU	-	-	-

Compiled according to the interview with the representative of The Estonian population register.

Data exchange works in Estonia with Finland, Latvia, and Lithuania, whereas Finland does not share personal identification code, which means manual work for the Estonian side. The information exchange takes place regarding Estonian citizens, in connection with the registration of residence and (in the Baltics) also regarding family events (birth, death, marriage, divorce, etc.). In the case of other persons, there will be a one-time flow of data in the future, where, for example, if a Russian citizen with an Estonian residence permit moves from Estonia to Finland, a one-time set of data will come to Estonia about the fact that the person arrived in Finland.

### 2.3.2 Summary of Issues and best practices

Interviews of representatives of five countries (Spain ES, Luxembourg LU, Netherlands NE, Norway NO, Estonia EE – see [Ch. 2.3.1](#)) revealed some issues which have an influence on the process and its information exchange. During the analysis different countries were analysed from different aspects (see Table 18 in [Ch. 4.5](#)) and therefore issues and difficulties are described from two different angles: related to processes (here in [Ch. 2.3](#)) and related to structural challenges (see [Ch. 2.4](#)).

All those countries share a common **issue**, that at least one physical contact is required at some point in the process of enrolment for local ID, which means that at least once a person must come to the issuing authority for the identity matching.

Quite common is also **treating the personal ID number as sensitive personal data**, which cannot be easily stored or shared by service providers, therefore. That is an issue as historic secrecy has led to processes when knowledge of this code is considered proof of identity and most of the personal ID numbers viewed include semantic information that for privacy reasons persons may choose to rather not share. Also, it can be an issue in the countries where ID number can be easily used to make financial commitments, leading to frauds.

When it comes to using public services with acquired local ID, it can happen that **not all municipalities offer digital services and there are lots of private sector specific processes**, that are not connected to national ID and are often not digitalized.

These are all important obstacles to overcome when planning flexible and comprehensive cross border identity and record matching solution. To sum up issues, all the countries face the possibilities of both positive false matches (accidentally connecting different people's identities) and negative false matches (not connecting the same person's different identities).

To overcome those issues, different strategies as **best practices** are used by countries, like:

- one central database of all identities (including small amount of available information of foreign identities connected to the local ones),
- video identification,
- central passports register stores photo and fingerprints, which can be checked, to make sure that no duplicate identities are created,
- manual supervision over connecting duplicated identities (same person with more than one matches from the database),
- name details are coded to match language specific changes in the surname,
- infinite shelf life of ID number (= identity) with added status (like "living" or "deceased"),
- and using digital signature together with ID number for making any commitments.

Following Table 10 covers common and country related issues and best practices.

**Table 10** Identity and record matching best practices and issues across EU/EEA countries.

Icons in table: "+" best practice solution for process related issue; "-" reason behind unsolved process related issue.

Member state (interviewed)	Providing identifier	Identity matching	Sharing data to service providers	Record matching
Common issues for many countries	- Physical contact required at some point in the process of digital enrolment for local ID.	- Citizen can have multiple eID from same country or different countries, as well as different names for some cases.	- Personal identifier considered as sensitive personal data.	- Private sector specific processes, not connected to national ID and often not digitalised.
Spain	+ There are several digital options available in Spain for applying for a personal ID or using public services. - Depending on its size, not all municipalities are digitally approachable for services.	+ Video identification is possible.	- In some sectors (like degree documentation in education sector) the documentation must be translated to Spanish and proofed by certified authority.	- Sector specific processes, not connected to national ID and mostly not digitalised.
Luxembourg	+ Fully online application process available for persons owning an eID means notified under eIDAS.	+ Possibility to manually connect identities.	- Private sector service providers cannot store national ID.	- Private sector specific processes, not connected to national ID and mostly not digitalised. + Education sector EU wide networks allow digital data sharing.
Netherlands	- One central database with all identities.	+ The name details (letter combinations like name prefixes etc.) are coded to match language specific changes in the surname. + Possibility to manually connect identities.	+ Presenting a polymorphic pseudo-ID to abroad.	- Every service provider has access only to its own records.
Norway	+ Unique national identifier from other MS (if received) is stored in the population register. - Enrolment for ID cannot be done digitally today.	+ Central passports register stores photo and fingerprints, and these data can be checked, to make sure that no duplicate identities are created.	+ Status of identity check is available to public and private entities that use the National Population Register.	+ In many cases today the national identifier of other countries is stored in population register, which increases hit rate significantly.

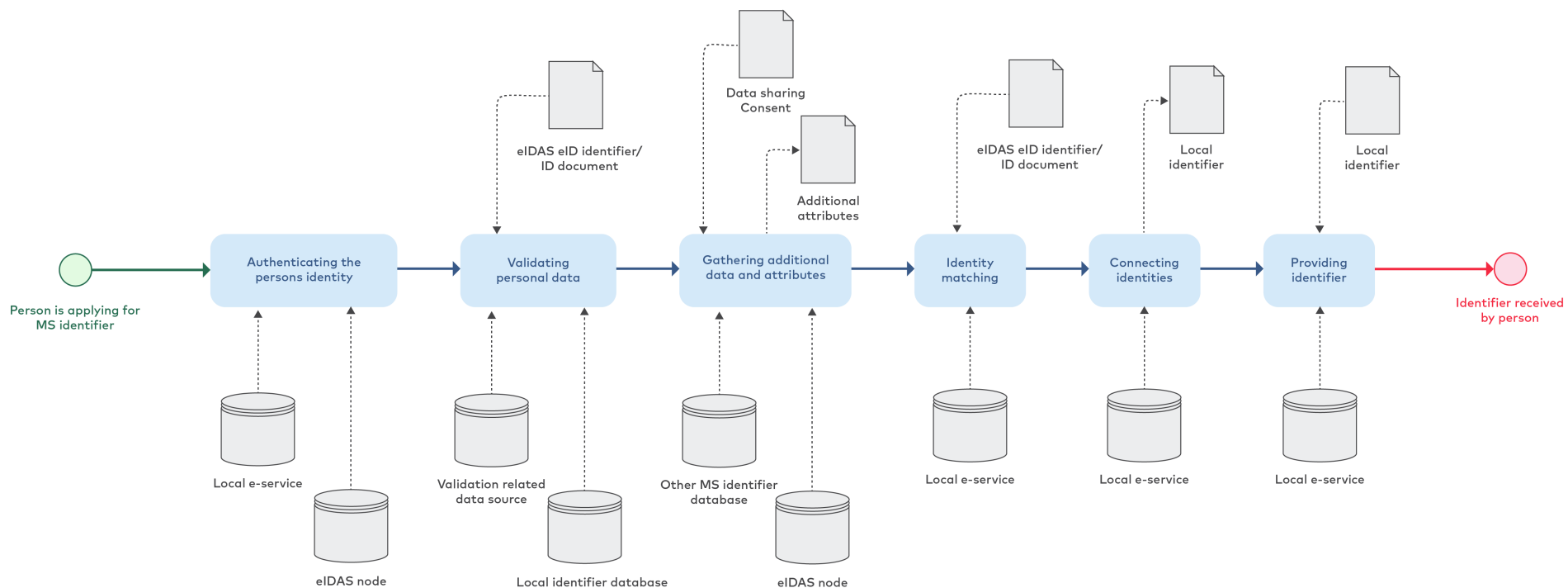
Estonia	<ul style="list-style-type: none"> <li>+ Unique national identifier from other MS (if received) is stored in the population register.</li> <li>+ Online application process is available (e-residency), still requiring one physical contact to receive the personal ID.</li> <li>- Digital association with eIDAS is not possible yet.</li> </ul>	<ul style="list-style-type: none"> <li>+ The identity of the person, once created in database, is forever. Only its status will change in time (e.g., "deceased").</li> <li>- Quality of background check depends quite often on the experience of the person conducting search.</li> </ul>	<ul style="list-style-type: none"> <li>+ Personal ID code is not considered as sensitive data, as the code alone cannot be used for any services or transactions (e.g., frauds).</li> </ul>	<ul style="list-style-type: none"> <li>+ Digital certificates (as signature) are used together with personal ID code (both included in e-ID) for approaching to services.</li> </ul>
---------	--	---	---	--

---

### 2.3.3 Identity and record matching processes and sub-processes

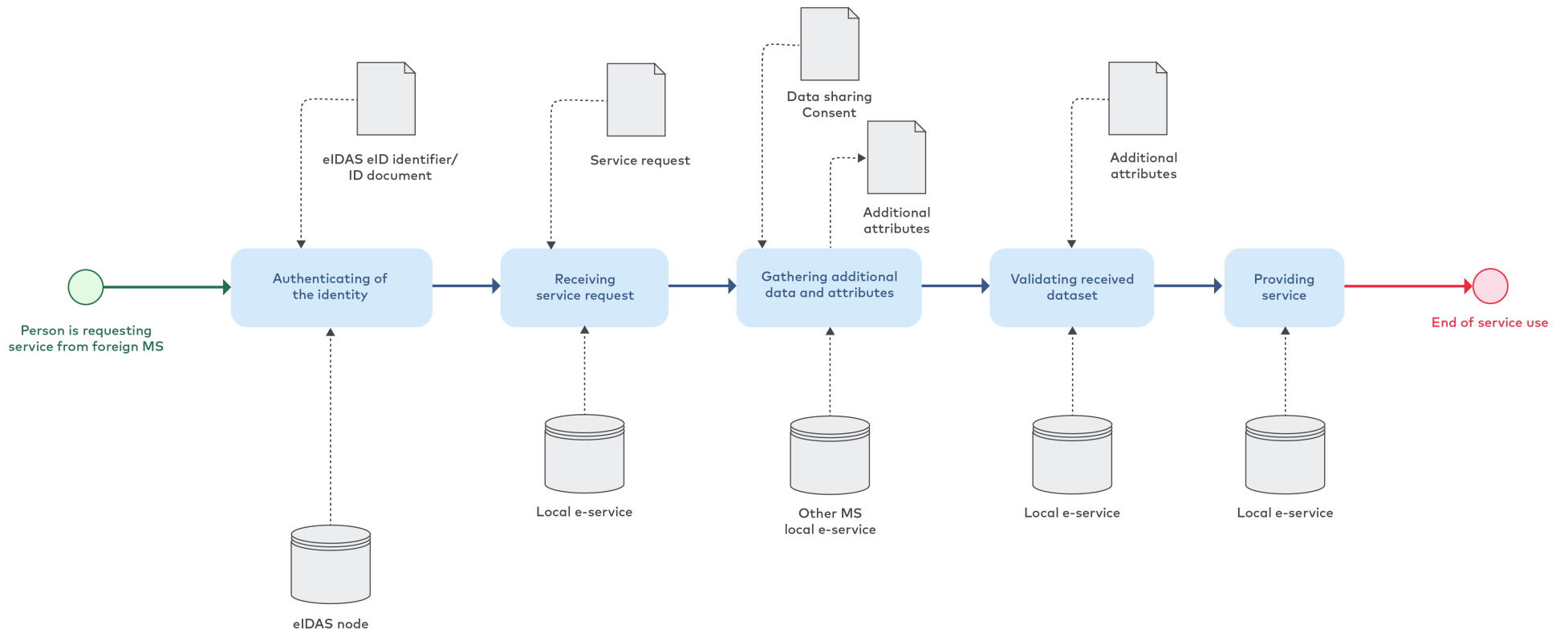
As mentioned earlier, the interviews revealed three main steps in identity and record matching process: providing identifier; identity matching; and data sharing and record matching. Those phases were refined during further analysis and a new three-part division was derived, as well as following sub-processes were drawn accordingly:

1. **Identity matching** – which includes all steps of acquiring an ID of Member State (MS).



**Figure 7** Identity matching sub-process happy path

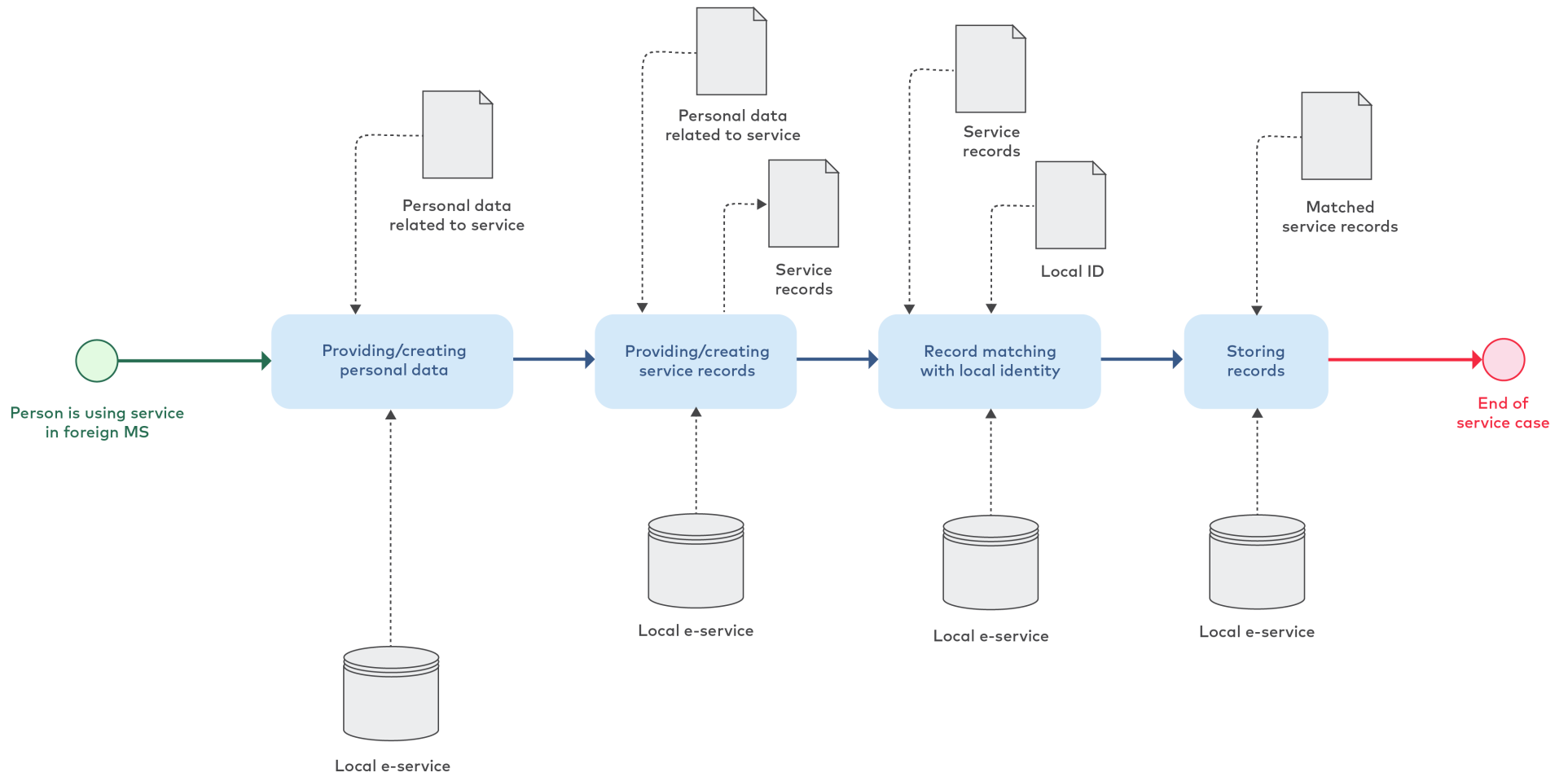
2. **E-service usage** – that describes steps from applying for MS service by using the identity of foreign MS up to providing service.



**Figure 8** E-service use sub-process happy path

3. **Record matching** – involves steps after service providing, when service-related data are stored and matched with the identity.





**Figure 9** Record matching sub-process happy path

Processes are drawn in Bizagi modeler, and BPMN notation is used. The description includes starting, intermediate and ending events, as well as tasks, related systems, and data. All processes are described as a **"Process Happy Path", which is an ideal and less complicated version of the process, where no interruptions or terminations occur.**

According to interviews conducted during analysis, a **merged process of identity and record matching** was drawn (see Figure 10). This generalized approach was initiated by the fact that the process itself in different countries was basically the same. Only the method of some steps varied from manual to digital and the names of systems used were different. So, all the gathered knowledge of the processes in different countries are merged into one view and the steps that varied from manual to digital are highlighted in ***bold italic*** font on the process graphical notation at Figure 10. The latter is accompanied by process sequence table that describes details of every step (see Table 11). While graphical notation gives broader overview of the process, the sequence table allows to analyse steps and their relations more closely.

Sub-processes (see Figure 7, Figure 8 and Figure 9) are described without distinguishing Relying Parties, intermediate events and gateways (referred as Event and Gate at Table 11). Due to their sequence, the sub-processes are joint into one merged process (see Figure 10) by using vertical distributor for their distinguishing. Separate horizontal lanes are used for appointing main Relying Parties and service users.

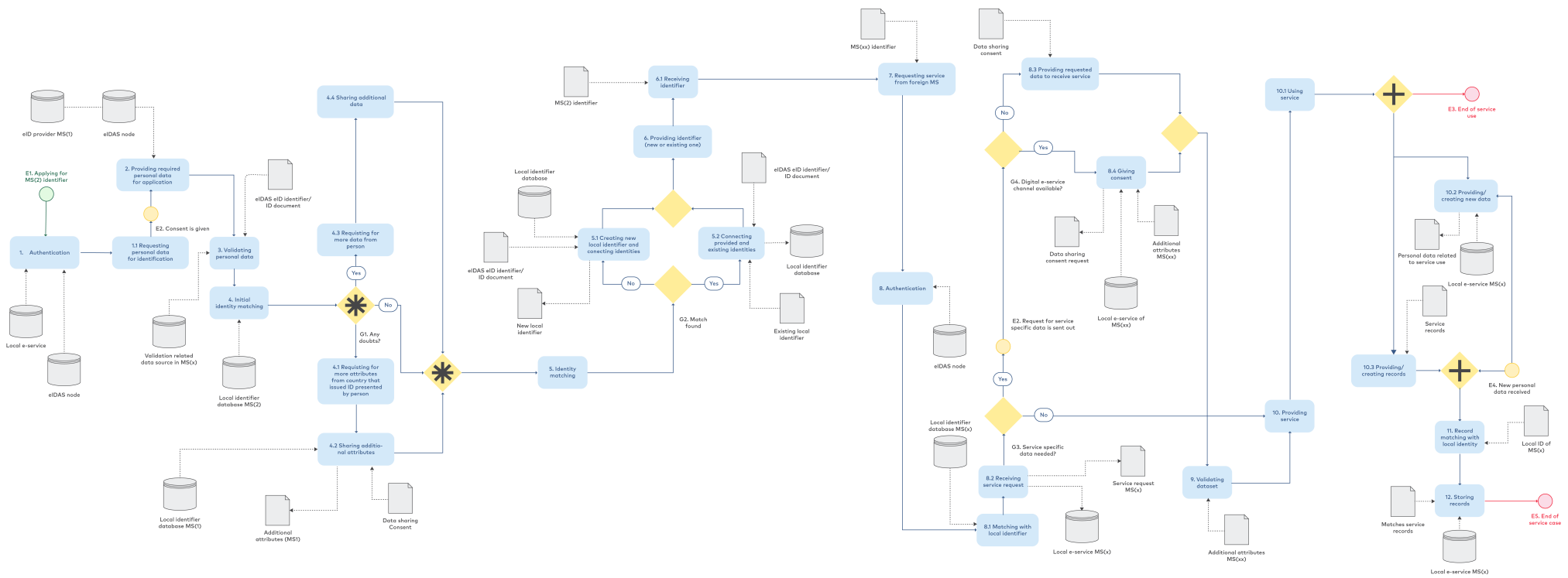
**Table 11** Sequence tabel of identity and record matching process.

Step	Description	Type	Belongs to sub-process of	Related system involved (first acquaintance)	Relations	Relying party* or service user	Next step
E0	Applying for MS (2) Identifier	Start	Identity matching	-	-	Person with MS (1) eID	1.
1.	Authentication	Task	Identity matching	Local e-service; eIDAS node	-	Identifier issuing MS (2)	1.1
1.1	Requesting personal data for identification	Task	Identity matching	-	-	Identifier issuing MS (2)	E1
E1	Consent is given	Event	Identity matching	-	-	Person with MS (1) eID	2.
2.	Providing required personal data for application	Task	Identity matching	eID provider MS (1); eIDAS node	-	Person with MS (1) eID	3.
3.	Validating personal data	Task	Identity matching	Validation related data source in MS(x)	eIDAS eID identifier/ ID document	Identifier issuing MS (2)	4.
4.	Initial identity matching	Task	Identity matching	Local identifier database	-	Identifier issuing MS (2)	G1
G1	"Any doubts?"	Gate	Identity matching	-	-	Identifier issuing MS (2)	4.1;4.3; G2
4.1	Requesting for more attributes from country that issued ID presented by person (MS1)	Task	Identity matching	-	G1 "YES"	Identifier issuing MS (2)	4.2
4.2	Sharing or additional attributes	Task	Identity matching	Local identifier database MS (1)	-	e-service from MS(x)	5.
4.3	Requesting for more data from person	Task	Identity matching	-	G1 "YES"	Identifier issuing MS (2)	4.4

4.4	Sharing additional data	Task	Identity matching	-	-	Person with MS (1) eID	5.
5.	Identity matching	Task	Identity matching	-	G1 "NO"	Identifier issuing MS (2)	G2
G2	"Match found?"	Gate	Identity matching	-	-	Identifier issuing MS (2)	
5.1	Creating new local identifier and connecting identities	Task	Identity matching	Local identifier database	Gate: "NO"; eIDAS eID identifier/ ID document; New local identifier	Identifier issuing MS (2)	6.
5.2	Connecting provided and existing identities	Task	Identity matching	Local identifier database	Gate: "YES"; eIDAS eID identifier/ ID document; Existing local identifier	Identifier issuing MS (2)	6.
6.	Providing identifier (new or existing one)	Task	Identity matching	-	-	Identifier issuing MS (2)	6.1
6.1	Receiving identifier	Task	Identity matching	-	MS (2) identifier	Person with MS (1) eID	7.
7.	Requesting service from foreign MS	Task	e-service usage	-	MS (xx) identifier	Person with MS (1) eID	8.
8.	Authentication	Task	e-service usage	eIDAS node	-	e-service from MS(x)	8.1
8.1	Matching with local identifier	Task	e-service usage	Local identifier database MS(x)	-	e-service from MS(x)	8.2
8.2	Receiving service request	Task	e-service usage	Local e-service	Service request	e-service from MS(x)	G3
G3	"Service specific data needed?"	Gate	e-service usage	-	-	e-service from MS(x)	E2;10.
E2	Request for service specific data is sent out	Event	e-service usage	-	G3 "YES"	e-service from MS(x)	G4

G4	"Digital e-service channel available?"	Gate	e-service usage	-	-	Person with MS (1) eID	8.3;8.4
8.3	Providing requested data to receive service	Task	e-service usage	-	G4 "NO"	Person with MS (1) eID	9.
8.4	Giving consent	Task	e-service usage	Local e-service of MS (xx)	G4 "YES"	Person with MS (1) eID	9.
9.	Validating dataset	Task	e-service usage	-	Additional attributes MS (xx)	e-service from MS(x)	10.
10.	Providing service	Task	e-service usage	-	G3 "NO"	e-service from MS(x)	10.1
10.1	Using service	Task	e-service usage	-	-	Person with MS (1) eID	10.2;10.3; E3
10.2	Providing/ creating new data	Task	Record matching	-	Personal data related to service use	Person with MS (1) eID	E4
E3	End of service use	End	Record matching	-	-	Person with MS (1) eID	-
E4	New personal data received	Event	Record matching	-	Service records	e-service from MS(x)	11.
10.3	Providing/ creating records	Task	Record matching	-	-	e-service from MS(x)	11.
11.	Record matching with local identity	Task	Record matching	-	-	e-service from MS(x)	12.
12	Storing records	Task	Record matching	Local e-service	-	e-service from MS(x)	E5
E5	End of service case	End	Record matching	-	-	e-service from MS(x)	-

\*Relying parties in this process are Identifier issuing MS (2) ; e-service from MS(x) and service user: Person using eID provided by MS(1).



**Figure 10** Graphical notation of Identity and record matching process Happy Path, generalized across member states. Based on interviews and process analysis of Spain (ES), Luxembourg (LU), Netherlands (NL), Norway (NO) and Estonia (EE). Text in ***Bold Italic*** refers to the identity or record matching activities that are not fully digital in countries referred. \*Happy path is an ideal and less complicated version of the process, where no interruptions or (almost none) terminations occur.

## 2.4 Common issues and difficulties

During the analysis different countries were analyzed from different aspects (see Table 18 in [Ch. 4.5](#)) and therefore issues and difficulties are described from two different angles: related to processes (see [Ch. 2.3](#)) and related to structural challenges (described below).

### 2.4.1 Description of the structural difficulties in Nordic-Baltic countries

Identity matching is difficult with the data currently available via eIDAS authentication. All the countries agree that there is no easy way to solve this issue. Most of the Nordic-Baltic countries already have the current eIDAS in use. However, it is not federated and requires additional steps to confirm authentication in cross-border situations. Identity matching of returning citizens in cross-border situations is not currently possible in most of the countries, but many of the countries are building national solutions to enable identity matching and reliable authentication, and there are authorities who already have built their own systems.

#### Denmark

Denmark has taken the current eIDAS in use for its own citizens with level of assurance (latvi) substantial and high. The country has an e-Identification system in which foreign users register remotely with an eID and a passport. They may also need to provide some additional attributes. Returning users can be matched, but the current method requires manual work, and, in some cases, matching is not possible. An automated process for identity matching has been available since October 2023.

The **CPR number** is unique to the person and is used in Denmark as an ID number. The CPR number consists of ten digits. The first six digits are date of birth (day, month, and year) while the last four digits provide a unique identification number for all citizens in Denmark. The CPR number is referred any time the person uses state-provided services. The CPR number can only be obtained on site in Denmark. <sup>[84]</sup>

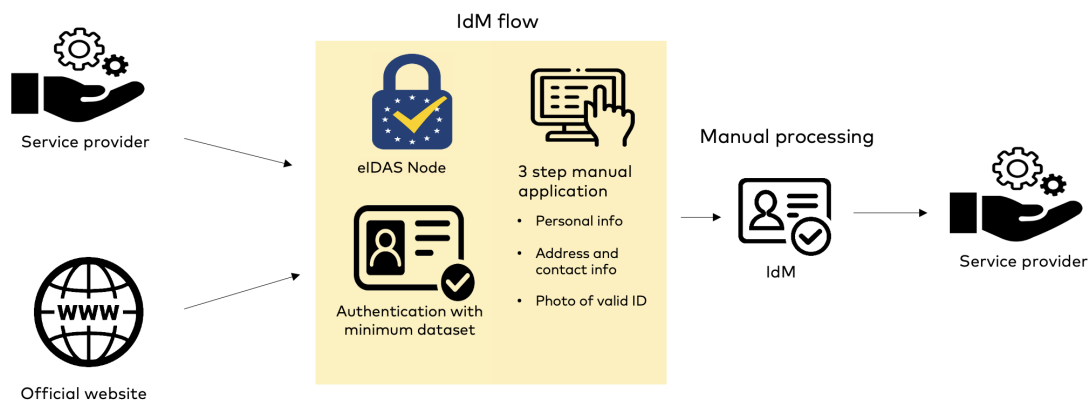
In case of identity matching, CPR number acts as a user provided attribute, which is used to start a search in the registry. The ID number was not initially considered as sensitive information, but it has been realized over time that it can be misused. Therefore, it is now personal sensitive information.

Currently, two different processes are being used for identity matching: manual and automatic. The manual process works as follows:

---

84. <https://international.kk.dk/live/cpr-registration-and-documents/cpr-number>

- Requesting a connection of CPR number and eID through DK Connect service (IdM).
- Login with national eID through eIDAS node.
- Information from national eID, self-type information and identity documents are being compared before IdM.



**Figure 11** Danish manual identity matching process. The Danish Agency for Digital Government.

#### Challenges of the manual process:

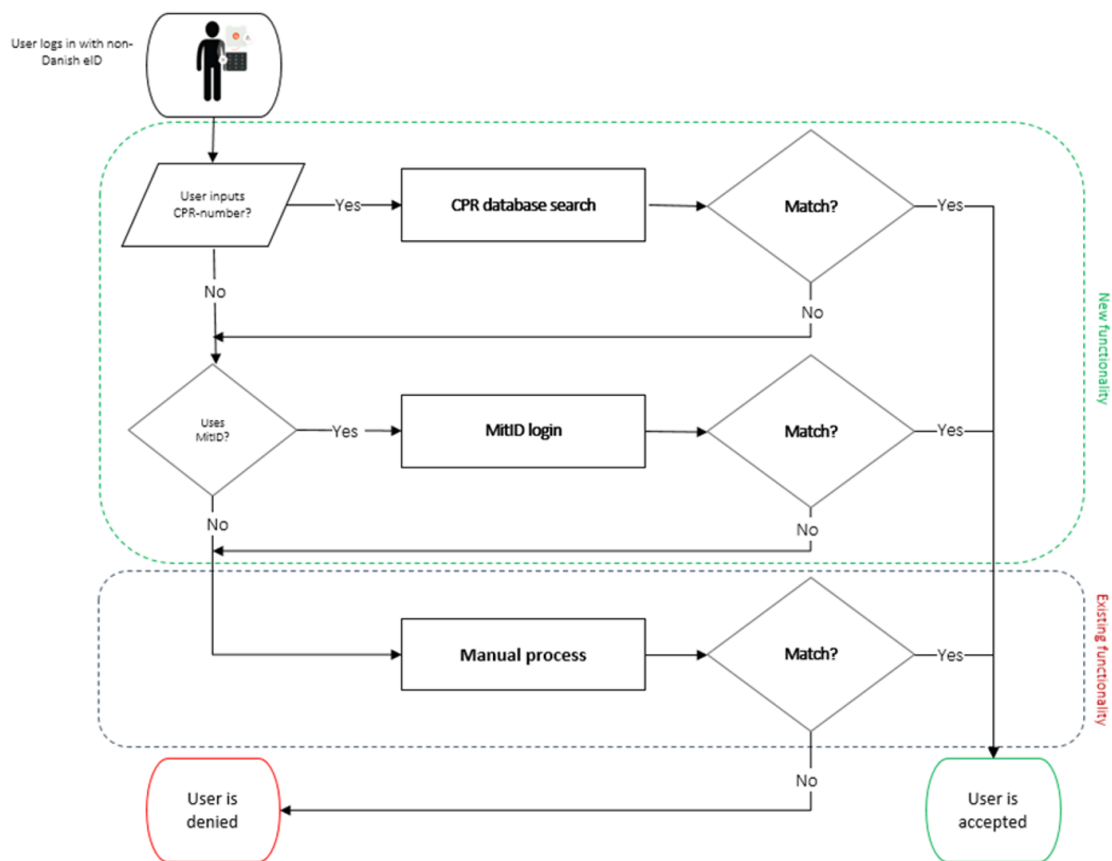
- Troublesome for users to register in IdM solution due to the complex user journey.
- Several sites and systems connected to the solution – long journey with many clicks and redirects.
- Too many steps and the requirement of photos of ID documents.
- Processing IdM applications manually demands resources, which makes it difficult to use on a large scale.

**Prerequisite:** Foreign citizen must have a notified eID from another member state that is connected to the Danish gateway, as well as a Danish CPR number. If the automatic match fails, the user will be prompted to match with their Danish eID that includes a CPR number, if they have one. If the user cannot or does not want to match with their Danish eID, they will be directed to the manual application for IdM. Automatic matching is only done if the cross reference with the CPR register with date of birth, given name and family name gives one result that matches with the CPR number. If zero or more than 1 match is found, automatic IdM will not be done.



### The automatic process works as follows:

- The user will provide their Danish CPR number (in addition to the automatically provided attributes from the eID).
- If the family name, given name and birthdate match with the information from the CPR-register, it will be automatically matched, and the user is redirected automatically to the self-service they were attempting to access.
- Names are concatenated and algorithms for transliteration is applied. If the eIDAS attribute for nationality is available, it is also be used for matching the datasets.
- If matching is successful, the user is redirected automatically to the self-service to be accessed.
- If step 1 of matching fails or is skipped, the user can provide their CPR number by logging in with their Danish eID, if they possess one.
- If both steps fail, they will be redirected to the manual identity matching process, where they will fill out the application.



**Figure 12** Danish automatic identity matching process.

Source: The Danish Agency for Digital Government.

### Challenges of the automatic process:

- Names are registered differently across systems and countries. E.g., cross reference between foreign eID and CPR register fails, due to middle name(s) being omitted in either.
- Accents and dialectic names (e.g., Cyrillic).
- First name and last name attributes can change.
- Common names increase risk of >1 matches.
- Few mandatory attributes to mitigate this.



For service providers, the main problem is still with foreign service users. The linking of registers to identify the user is highly regulated and, in many cases, even requires the user's approval before any data can be accessed. For some private service providers, user's CRM numbers are not automatically shared by the state but require the user's consent. The State has a service that allows private service providers to verify the accuracy of the individual's data. For example, when a person wants to open a bank account or draw up an insurance policy, most service providers are obliged to check the CRM number of the service user from the register. Many private service providers have access to the population register, but there are restrictions on the data that can be seen and used.

According to the interviewees, one of the biggest future problems regarding identity matching will probably be the complexity of the user journey, which from the user's perspective can lead to lower satisfaction of the services. The process can become even more complicated when new eIDAS attributes are required. Another challenge is related to resources: as processes are growing safer and more regulated, it requires more workforce to process the requests and avoid false positive and false negative matches.

### Faroe Islands

The Faroe Islands is an autonomous territory within Denmark. Although most inhabitants are Danish citizens, a Faroese inhabitant does not possess a Danish national ID number (CPR number) unless the person additionally fulfils the requirements for registration in the Danish population register.

In the Faroese P-System (Civic Registration Number System) a person is registered if

- the person is born in the Faroe Islands or has moved to the Faroe Islands as a resident or
- the person according to the Faroese Tax Administration is taxable to the Faroe Islands.

The Faroese P Number (p-tal) is used in almost all communication with public authorities. The p-tal consists of nine numbers. The first six numbers are a person's date of birth, and the remaining three numbers are private and only known to the individual.<sup>[85]</sup>

In cases where a person is not a Faroese resident, but where the Faroese Tax Administration at the same time finds the person taxable to the Faroe Islands, e.g., as an employee, the Faroese Tax Administration issues an identification number (v-number). The structure and format of this Identification number is similar, but not identical to the P number issued by the National Registration Office.<sup>[86]</sup> In the Faroe Islands the legal persons TIN equals the V number issued by the Faroese Tax Administration.



As Faroe Islands is not part of eIDAS scheme, identity data is moving through different service providers. Electronic ID solutions are mostly needed by Tax Authority and banks, which have working solution in place to interact with Danish CRM system. According to interviewees, since 95% of cross-border interactions are related to Denmark, eIDAS unnotified status is only a theoretical problem.

The population register is separate from the Danish jurisdiction. There is currently no solution to match cross-border service users with the population register. There have been plans for banks to allow a local identity for all cross-border service users, but this process would be quite cumbersome, so it has not been taken forward. The number of use-cases is too small considering the costs that could be involved.

According to interviewees, eID implementation is still in early phase, starting in 2020, so there are no major reform plans besides improving the infrastructure. The system was built from scratch with both public and private funding. Best practices were considered when building the solution, the solution is audited, so there are no major security risks.

## Greenland

Greenland is an autonomous territory within Denmark. All residents in Greenland get a CPR number (the same as in Denmark) that is used for almost all communication with public authorities and therefore also in tax matters. The CPR number is also issued for all non-residents in Greenland where the Greenlandic Tax Administration finds the person is taxable to Greenland.

The GER number for non-natural persons and legal entities is issued according to different tax- and excise laws. The GER number is administrated by Skattestyrelsen (The Greenlandic Customs and Tax Administration) placed under the Greenlandic Ministry of Finance.<sup>[87]</sup>

---

85. <https://www.taks.fo/en/individuals/tax/p-tal#:~:text=The%20p%2Dtal%20consists%20of,only%20known%20to%20the%20individual.&text=When%20you%20are%20born%20in,to%20receive%20wages%20or%20salaries>.

86. <https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/tax-identification-numbers/Faroe-islands-TIN.pdf>

87. <https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/tax-identification-numbers/Greenland-TIN.pdf>

As a local eID solution, MitID<sup>[88]</sup> has been implemented as the successor to NemID.<sup>[89]</sup>

MitID, can be obtained through local banks, by contacting a citizen service centre in person or at [www.nemid.nu](http://www.nemid.nu). The Digital Agency of Greenland is the authority in acquiring eID-s and assists the municipalities in administration of the MitID scheme.

Population operations in Greenland are conducted using the Danish population register. However, information about residents in Greenland is maintained as a separate copy in Greenland. The use of e-services, including identity matching, is like in Denmark, and it relies on Danish infrastructure. Greenland has a single point of contact for e-services, such as hunting license, residence certificate and digital mail.<sup>[90]</sup>

During the interview, it was emphasized that, due to Greenland's vast size and sparse population, the presence of eID and the accessibility of e-services are considered crucial because they enable service usage in regions where it would not be possible without eID. According to the interviewee, approximately 2,000 individuals (out of a total population of around 57,000)<sup>[91]</sup> currently do not have eID. However, identity matching is not considered a priority now, as the risk of identity misuse in Greenland is very low due to its limited accessibility. It was mentioned during the interview that even if the risk of data misuse arises, face-to-face identification is currently sufficient since people are familiar with each other in the community.

## Estonia

Estonia also has the current eIDAS eID means in use for its own citizens with level of assurance high. Citizens from other member states can sign into some of the Estonian public e-services with eIDAS if the member state has a notified eID means. **As the attributes of the current eIDAS do not enable reliable identification, most of the e-services cannot be fully accessed** (there are currently only a few SDG online procedures that can be accessed with eIDAS in EE). Estonia is also missing a central identity matching process for public e-services. Therefore, many digital services in Estonia require local authentication that uses the national ID number. The underlying issue, as in Finland, is that most online services cannot handle the foreign identifiers since they are dependent on the Estonian national identity code format to identify the user. Therefore, even if the authentication service passes the eIDAS eID attributes to the e-service application, the e-service might not recognize or accept eIDAS authentication or the eIDAS eID user will be forwarded to a manual process for identity matching and verification.

---

88. <https://lifeindenmark.borger.dk/apps-and-digital-services/mitid>

89. <https://lifeindenmark.borger.dk/apps-and-digital-services/nemid>

90. [https://www.sullissivik.gl/?sc\\_lang=da](https://www.sullissivik.gl/?sc_lang=da)

91. <https://www.worldometers.info/world-population/greenland-population/>

To simplify the adoption of eIDAS for relying parties, RIA operates a government authentication gateway service (TARA) that translates eIDAS SAML protocol to OpenID Connect (OIDC). For cross-border eID interoperability within the EU, RIA operates a centralized eIDAS Node services (eIDAS Proxy Service and eIDAS Connector) that use the TARA interface which translates eIDAS SAML protocol to OIDC. The eIDAS-Node application in the Estonian eIDAS-Node implementation is part of the European Commission's eIDAS-Node sample software that is responsible for a secure communication between member states eIDAS-Nodes using the eIDAS SAML protocol. On the authentication with Estonian eID means in eIDAS Network, the eIDAS minimum data set (MDS) for a natural person contains current family name(s), current first name(s), date of birth and unique persistent identifier (Estonian personal identification code). The minimum data set for a legal person contains current legal name, Business Registry code (identifier for a legal person in Estonia). MDS attributes for a natural person are fully based on data on the Estonian eID certificate, for legal person the MDS attributes are requested from Estonian e-Business Registry using X-Road data exchange layer.

Authorization/access to Estonian e-services are based on a unique identifier (see more in [Ch. 2.3.1 "Estonia \(EE, interviewed\)"](#)).

The population register is a database which unites the main personal data on Estonian citizens, citizens of the European Union who have registered their residence in Estonia, and e-residents who have been granted a residence permit or right of residence in Estonia.

Personal identification code is always formed in the population register. However, **minimum set of data** needed for formation of the PIC (name, date of birth, gender, place of birth and citizenship) can move to population register in different cases by following authorities:

- Vital statistics office (local authority, notary, Foreign Ministry/representation): registration of a vital statistics event in Estonia or data entry from foreign vital statistics document.
- Police and Border Guard Board: issuing an identity document/residence permit or other proceedings provided by law.
- Health care provider: for new-born children's medical birth certificate.
- County town local authority: for entry into a database based on a person's application.
- Local authority: entering of residence of European Union citizen in the population register.

- Other agency for public duties (Foreign Ministry, Maritime Administration, etc.): performing their duty of entering the personal identification code in a state database.



Data exchange between population registers is in place with Finland, Latvia, and Lithuania. However, with Finland, data is exchanged without a personal identification code, which means that the exchange is semi-manual. It is also possible to enter foreign personal identity code in the population register, which can be used for searching (e.g., Finnish personal identity code in addition to Estonian). However, the data cannot only contain a foreign country code, but also an Estonian one. Services do not use foreign ID codes. This is a free text field, as there are no rules for data processing now.

## Finland

Most Finnish public eServices have eIDAS authentication as part of Suomi.fi authentication but as it does not contain enough information it cannot be used as authentication as such. Most competent authorities require more information from the user to be able to use their eServices. Many digital services in Finland still require local authentication in the form of the Suomi.fi-authentication that uses the national ID number. The underlying issue is that most online services in Finland still only accept a Finnish national identity code to identify the user. Therefore, even if the authentication service passes the eID to the application, the other application may not recognize or accept eIDAS authentication. This prevents the authentication and use of Finnish digital public services with any other authentication identifiers, which hampers the use of services across borders.<sup>[92]</sup>

In Finland, identity management is based on the **idea that a person has only one identity, to which all transactions are attached**. This is important, for example, from the point of view of paying benefits or pensions, as well as from the point of view of taxation. The problem is solved by asking as much information as possible about the person, either from an official document or by asking the person himself. This information is used to ensure that the identity is not already found in the Finnish population information system. If no information is found, one's identity can be registered in the population information system. However, it currently requires face-to-face identification.

The problem is that a person can have multiple identities. **Connecting these identities requires a lot of manual work by the officials**. There is also a problem with eIDAS authentication, which provide too little information. People must be directed to a service where they will be asked for more information. In Finland, only a few organizations have built eIDAS support into their services, that is, few organizations can process a person's data with an eIDAS personal identifier.

---

92. <https://pub.norden.org/temanord2021-547/#88558>

According to Finnish legislation, a **person cannot be registered in the Finnish population information system remotely**. When a person is registered in the population information system for the first time, the person must be met face-to-face. In Finland, there was a draft law regulating remote registration (HE 132/2022) under consideration by the government, but the government did not have time to process it. A new government has been formed and according to the government's program, there is no intention to promote remote registration.

- For example, according to current legislation, a person must generally have a residence permit before a person can be registered in the population information system.
- For asylum seekers, it can take months, even years, before registration can be done. However, events related to a person must be processed by different organizations, and for processing to be possible, an organization-specific identifier is created for the person in the systems for processing.
- This **organization-specific identity will later be manually associated with the centralized identity when it can be created**. In the bill, which did not have time to be discussed, it was suggested that a centralized identity could be created earlier, e.g., when applying for a residence permit.

From the state perspective, the major challenge is that it cannot be ascertained whether the person has a centralized identity in the population information system and the systems of organizations. However, from the user's perspective, the main difficulty is that the **person must be asked for more information to find the identity information and it slows down the service**.

In Finland, a study is underway on how eIDAS identifiers could be linked to a national identity, if such exists. If, on the other hand, there is no identity, the person could be registered remotely in the centralized population information system. However, all of these require a legislative change and, according to the government's program, at least remote registration will not be promoted.



According to interviewees, one possibility could be that between the Nordic countries, information transmitted in connection with migration agreements and the national ID included in the information would be used. There is a migration agreement between the Nordic countries, where the information of the person moving to another Nordic country is sent. In connection with migration information, a national personal identification number is also transmitted, which is also stored in the population information system in Finland as a foreign personal identifier. The assumption is that the eIDAS code in the Nordic countries consists of national personal identifiers, and the information stored in the population information system in connection with migration could be used to link identities. Also, through the agreement related to data exchange between Estonia and Finland, the foreign

place of residence will be forwarded to the other country's population information system. However, the new foreign identification number issued to the person will not be forwarded.

## Latvia

Latvia has eIDAS in use for its own citizens with LoA high. Identity matching in case of one person with few Member State identities is considered problematic also in Latvia and a need for a Europe-wide unique person identifying mechanism or solution is recognized. Pre-analysis shows that standard attributes may be enough to identify a person in case the central permanent IDs implementation is going to be made or cross-country IDs relation scheme will be established. Decentralized or country-specific intention to match identities will complicate an OOTS system development and successful identity matching.

For now, the country has a unique and persistent identifier in use for the nationals, but due to a renewal project any person is currently allowed to change the identifier once, if they have the old form of the identifier. However, according to the interviewee, due to the change in the personal identification code format, there have been no insurmountable problems. Compatibility with the old personal identification code is ensured, and there is a system in place to verify the linkage between the new and old codes.

Citizens from other member states can sign into some of the Latvian Procedure portals and complete an eIDAS compatible services, but data or services provided may be imprecise or non-relevant for user because of already defined identity matching issues and unavailability to identify single person with multiple IDs.

State services operate with a personal identification code. When interacting with the government, registration in the Register of natural persons is required. The eIDAS authentication user is assigned a personal code in the Register of Natural Persons automatically.

In case of eIDAS authentication users, there may be duplicate records; for example, when a person arrives from Germany with an Estonian personal identification code, these records cannot currently be matched. Matching may also encounter issues when individuals arrive at different times with various documents issued by foreign countries. The foreign country's identification code is primarily used for information exchange and filtering with other nations, but currently, it is not machine-readable.

Data exchange using personal identification codes currently only works with Estonia (Population Register). Data exchange with Scandinavia or Lithuania does not function, and the matter is not particularly on the agenda now. Most cross-border users are mainly connected to the Baltic states, Sweden, or Norway.

According to interviewee, Latvia is not yet ready for everyday use of biometrics. Biometrics have a separate register that communicates with, among others, the driver's license register, and the population register. With biometrics, it is possible



to perform searches, but it is not used daily because records cannot be matched one-to-one, and the search consumes a significant number of resources.

Main challenges include:

- When registering a company, it is not necessary to provide all the attributes that would be required for registration in the population register when registering the owner.
- There is a desire to create new e-services continuously, but often they are not developed from the users' perspective.
- The use of biometrics could increase, but currently, there are not very good solutions. To ensure consistent data quality in the population register, people's biometrics should be collected when recording personal data. Once this is achieved, viable solutions can be developed.

## Lithuania

Lithuania has the current eIDAS in use for its own citizens with LoA high. The e-services are designed for nationals of the country whose national personal identification codes are connected to the public registries and databases. Foreigners (not only EU residents) need to apply for a resident ID („eRezidentas“) to get access to electronic services and a visit to the authority is required.

There is a central identity matching process for public e-services. Data of foreigners is stored in foreigner's registry and linked with Lithuanian identity code. The same matching process is applied to foreigners with resident ID and the ones who are coming through eIDAS. The process may still require some manual work.

Identity matching service is performed at the information system of Electronic Migration Services (MIGRIS). MIGRIS is managed by Migration Department under the Ministry of the Interior of the Republic of Lithuania. eIDAS node is at The State Information Resources Interoperability Platform (SIRIP).

When foreigner initiates **log in directly from SIRIP via eIDAS**, SIRIP webservice sends a data request to MIGRIS for checking if in the register of foreigners, the person has assigned ILTU code.

- If foreigner has assigned ILTU code, then personal profile is updated.
- If foreigner hasn't assigned ILTU code, then MIGRIS creates a new one.

When a foreigner comes directly to SIRIP and logs in for the first time, the new user is asked to provide contact information as phone no., email address.

When a foreigner initiates **log in from another procedure portal** (external system) then the portal redirects the person for identification to SIRIP via eIDAS node. SIRIP WS sends a data request to MIGRIS for checking if in the register of foreigners, a person has assigned ILTU code.

- If foreigner has assigned ILTU code, then a personal profile is updated at SIRIP and eIDAS personal data + ILTU code are transferred to the requesting Procedure portal.
- If foreigner hasn't assigned ILTU code, then MIGRIS WS creates a new one then personal profile is updated at SIRIP and eIDAS personal data + ILTU code are transferred to the requesting Procedure portal.

In this case, the person does not need to provide contact information: foreigner comes to SIRIP just for identification service from another Procedure Portal. In all cases ILTU code is provided with eIDAS data attributes.

Identity matching is performed by using the following attributes: name, date of birth and nationality. However, nationality attributes are calculated from the eIDAS code (PersonIdentifier) since for now there are no other working solutions.

## Norway

Norway has the current eIDAS in use with LoA high. Norway's situation similar as in other Nordic-Baltic countries: even though eServices are widely used among nationals, identity matching of foreign users is difficult (see Ch. 2.3.1 Norway).

The Norwegian Tax Administration is responsible for the Norwegian National Population Register and the registration of residents living in Norway. This register is used as the basis for the registration for an electronic identification means.

Norway has bilateral and multilateral agreements between governments and authorities on population registration - E.g., the agreement between Denmark, Finland, Iceland, Norway, and Sweden. Exchanging the country's national ID numbers with authorities in other countries is allowed between the Nordic countries to identify a person, and as documentation if someone asks and has got a legal reason to ask for it. Foreign eID codes and corresponding national ID numbers are registered in a separate register.<sup>[93]</sup>

## Sweden

Sweden also has eIDAS in use for citizens with LoA substantial. In Sweden, UID from other Nordic countries is stored in population register for residents that have moved to Sweden (from e.g., Norway, Denmark, and Finland). However, eUID is not stored in the Swedish population register. So, if a Nordic member state uses an identifier that is different in format as eUID compared to the holder's UID, the match is unsuccessful.

---

93. <https://pub.norden.org/temanord2021-547/#88558>

Sweden defines matching based on three different confidence levels: A; B; C; The C level is the lowest confidence. The C level is possible to achieve if the UID provided by the user (that has been identified through eIDAS) is found as single hit in population register and person is registered as emigrated. If there are more than one person with the same name and birthday in the population register, then C level is not possible. The data is stored in a service that is integrated to the Swedish eIDAS node. Data is created based upon request by user. Sweden widely uses BankID, Freja and Svenska Pass<sup>[94]</sup> for verifying digital identity.

The Swedish Tax Agency is responsible for the population register and the registration of residents living in Sweden. This register is used as the basis for the registration for an electronic identification means. As set out in the Population Registration Act (1991:481), The Swedish Tax Agency is responsible for the civil registry of Sweden. Persons permanently living in Sweden are registered in the population register with a unique identifier (Swedish personal identity number). Normally a person keeps this identifier their whole life, only under very rare conditions can someone change their personal identity number. Persons not permanently living in Sweden receive a unique coordination number.

A **personnummer** (Swedish UID) is a 10-digit number (YYMMDD-XXXX)<sup>[95]</sup> that has different parts with specific meanings. The first 6 digits represent date of birth, followed by a hyphen.<sup>[96]</sup> Among the four last digits, the three first are a birth number (serial number). Odd number for males and even number for females. The last digit is a checksum calculated using the [Luhn algorithm](#).<sup>[97]</sup>

**Coordination numbers** are used for persons who need to interact and/or live in a short period of time (less than a year). Coordination numbers expire. If a person stays for example a year or longer, then she will get a personnummer that replace her coordination number. Coordination numbers are also found in the Swedish population register. However, if a person is subsequently listed in the Swedish Population Register and receives a personal identity number, this will be linked with the coordination number. Coordination numbers are structured in a similar way to personal identity numbers, but 60 is added to the day on which an individual was born. So, someone born on 24 September 1990 would be given the coordination number 900984, followed by four digits. In coordination numbers for men, these four digits are odd numbers. For women, they are even numbers.<sup>[98]</sup>

Coordination numbers can be requested in two ways<sup>[99]</sup>:

---

94. Passport or confirmation by relatives are used to create a match on A level. I.e., to strength the proof of being the holder of the national UID.

95. When stored or handled in a structured way, the law states handling it with the full length of the year:

YYYYMMDDBBBC

96. The year a person turns 100 the hyphen is replaced with a plus sign.

97. <https://www.geeksforgeeks.org/luhn-algorithm/>

98. <https://www.skatteverket.se/servicelankar/otherlanguages/inenglishengelska/individualsandemployees/livinginsweden/personalidentitynumberandcoordinationnumber.4.2cf1b5cd163796a5c8b4295.html>

99. A third way is that an employer can request a coordination number for an employee.

- Usually, a public authority will request a coordination number for an individual if it is needed for its own activities or to coordinate with other public authorities. If this is the case, the public authority in question will manage all interaction with the Swedish Tax Agency.
- If a person has no contact with any public authority but still needs a coordination number, the person can apply for one by visiting a Swedish state service centre.<sup>[100]</sup> The application must include details of connections to Sweden, the need for a coordination number, and a valid proof of identity document. Also, a contact address needs to be provided, which can be either in Sweden or abroad.

Moreover, Sweden has a new system that creates coordination numbers on all 3 different levels of confidence for identity proofing. To get the highest level of confidence, the person must visit the Swedish state service center and have necessary records for identification.

Sweden does not issue eID means to legal persons, however a natural person can be authorized to represent a legal person. Sweden has an eID system that can provide a pseudonym unique identifier for a person that acts in his/her job position and not as a private legal person. The attribute is in the format of uid@oid.

To simplify the handling of users and identities in Swedish services the Swedish eIDAS node generates a standardized identity attribute for users that have been authenticated using a foreign eID, a so-called *Provisional ID* (PRID). The eIDAS node will also create an attribute that declares which persistence, or lifetime, the PRID attribute has. The PRID attribute is generated based on attributes values received from the foreign authentication according to specific methods for each country. Every combination of country and method a graded based on expected persistence, i.e., how likely it is that an identity for a person is changed over time. This makes it possible for Swedish services to customize the communication with the user and to proactively provide features for a user whose identity has changed and make it possible for this user to access his or her account.

In some cases, a person that has been authenticated using a foreign eID may hold a Swedish personal identity number. It can, for example, be a Swedish citizen that has moved abroad and obtained a foreign eID, or a foreign citizen that is, or has been, registered (folkbokförd) in Sweden and has been assigned a Swedish personal identity number.<sup>[101]</sup>

---

100. Which is a public authority that make an assessment on the need for requesting a coordination number.  
 101. <https://docs.swedenconnect.se/technical-framework/latest/00 - Swedish eID Framework - Introduction.html>

**According to interviewees, the main challenges regarding identity and record matching include:**

- few valuable digital solutions that in reality work with only eIDAS. Public relying parties have a strong tradition on building systems based on identifiers managed in the Swedish population register. Individuals and information about individuals are identified via Swedish identification number.
- no digital solution for onboarding new people to the Swedish identification system, i.e., during the period that starts with the first contact to the point when person receives PID or a Swedish coordination number.
- Lack of governance that would bridge the digital and physical world. A good example is the challenge of providing a digital support for onboarding people to Sweden.
- Legal challenges, especially when several governments are involved in building a common system.
- Bad user experience and difficulties in understanding whom to contact for support. Users must use interfaces provided by different relying parties, eIDAS-nodes, eID provider, and soon also an identity matching system.

According to interviewees, in most cases today where relying parties attempt to authenticate the user through eIDAS, the user is authenticated, but relying party doesn't know how to connect the user to records and information in their business processes. From a user point of view, also it would be important to be able to use identity matching across all Swedish public organizations.



It would mean that different governments and municipalities had to trust the matched records, even if the matching was not performed within their internal processes. However, as the situation is today, individuals that do not have a Swedish *personnummer* must perform identity matching at every contact with a public sector organization. This could include going through different processes that involve paper and sometimes a physical visit at a local office.

Today, the Swedish population register has access to the Nordic countries' personal identification numbers for citizens who live in Sweden. If there was an agreement between the Nordic countries to provide such attribute through the eIDAS nodes, identity matching could be performed with a higher confidence, i.e., when the eIDAS assertion contains an identification number that also exists in the Swedish population register.

## Iceland

In Iceland, persons and enterprises are issued a unique identification number (kennitala) which is recorded in the national register and register of enterprises. ID numbers are composed of ten digits. The first six of these are the individual's date of birth in the format DDMMYY. The seventh and eighth digits are randomly chosen when the ID number is allocated (ranging from 20 to 99), the ninth is a check digit and the tenth indicates the century of the individual's birth: '9' for 1900–1999, '0' for 2000 and beyond. ID numbers are often written with a hyphen following the first six digits, e.g., 120174-3389. The ID number from national registry is the main unique identifier used in Iceland.<sup>[102]</sup>

In Iceland, foreigners who come to work or relocate for various reasons are assigned a System ID, which is structured similarly to the personal ID number.<sup>[103]</sup> However, the key distinction is that System IDs are stored in a separate database. To acquire a System ID, you need to submit an application along with a copy of your identity document. Once you are physically in Iceland, you must visit Registers Iceland in person to complete the identification process. Individual is registered in the system ID register which is a centralized register that is disseminated to Icelandic legal entities on the assignment of a system ID No. The purpose of the system ID No. is to provide public authorities with a unique number to differentiate between individuals and to be able to exchange information about the individuals, for example due to tax payments. One can utilize the System ID to access services in Iceland and even obtain digital certificates from Audkenni. These certificates allow the person to log in to various services and digitally sign documents (they can even vote in e-voting). Therefore, the time required to obtain the official ID number does not impede persons access to services in Iceland. As individuals spend more time in Iceland and complete the necessary identification procedures, their System ID eventually becomes their official ID number.

Personal ID numbers are issued at birth to all children born in Iceland and Icelandic citizens born abroad. Personal ID numbers are also assigned to all individuals who register their domicile in Iceland. When domicile is registered in Iceland a personal ID number is assigned in the national register, or in cases where individual is already registered in the system ID register, the system ID no. is moved from register of System ID No. to the National register. Entitlement to public services and assistance is generally dependent on having a registered legal domicile. It is therefore recommended that individual register their legal domicile as soon as possible.<sup>[104]</sup>

---

102. <https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/tax-identification-numbers/iceland-tin.pdf>

103. Process has started to make a new version of the System ID which will look different from the kennitala - it will be a random number, which starts with 8.

104. <https://www.skra.is/english/people/my-registration/id-numbers/>

Audkenni is the only issuer of eID means today and the company is 100% owned by the state.

One issue is that having an ID number is usually a prerequisite to accessing most government services, banking services and even some businesses transactions. This can be a hinderance to newly settled residents, as it takes some time to apply and be issued a new ID number. Employers typically apply for System IDs on behalf of their foreign workers before they arrive in Iceland, because these IDs are a prerequisite for starting work.

The following table (Table 12) gives an overview of different personal identification codes used in Nordic-Baltic countries, current eIDAS status and main challenges that emerged from the analysis of the current situation.

**Table 12** Used PIC(s), Uniqueness Identifier,<sup>[105]</sup> eIDAS status, LoA and main challenges regarding identity and record matching by country

Country	Used PIC(s)	Uniqueness Identifier	eIDAS status	LoA	Main challenges
Estonia	personal identification number ( <i>isikukood</i> )	Estonian personal identification code	notified	high	<ul style="list-style-type: none"> <li>Population register has no automated process for identity matching.</li> <li>Manual work: for example, Police and Border Guard Board takes an application from the person and then tries to identify them, sends an application to the population register and asks for a new ID number, but the operation reveals that person is already on the register.</li> <li>Using local services very often requires Estonian PIC.</li> </ul>
Finland	personal identity code ( <i>henkilötunnus</i> or <i>hetu</i> )	–	un-notified	–	<ul style="list-style-type: none"> <li>Face-to-face identification required to be registered in the population register.</li> <li>Few organizations can process a person's data with an eIDAS personal identifier.</li> <li>Organization-specific identifiers need to be connected manually</li> </ul>
Norway	national identity number ( <i>fødselsnummer</i> ) D-number (issued to people with temporary connection to Norway)	Derived from the Norwegian Personal Identification Number	notified	high	<ul style="list-style-type: none"> <li>Enrolment for ID cannot be done digitally today. Physical appearance is required to receive the ID document.</li> <li>Current legislation does not comply with the identity matching solutions connected to biometric data.</li> <li>People come with a minimum data set from abroad or with a passport. And data quality differs a lot.</li> </ul>
Sweden	personal identity number ( <i>personnummer</i> ) coordination number (issued to people who need to interact with public authorities, but have never been listed in the population register)	Derived from the Swedish Personal Identification Number	notified	substantial	<ul style="list-style-type: none"> <li>Few valuable digital solutions that in reality work with only eIDAS.</li> <li>No digital solution for onboarding new people to the Swedish identification system, i.e., during the period that starts with the first contact to the point when person receives PID or a Swedish coordination number.</li> <li>Bad user experience and difficulties in understanding whom to contact for support.</li> </ul>

105.Describes how the PIC is made visible to other countries via eID.



Iceland	System ID number Personal ID number	-	un-notified	-	<ul style="list-style-type: none"> <li>Having an ID number is usually a prerequisite to accessing most services, banking services (incl. private) in Iceland. This can be a hinderance to newly settled residents, as it takes some time to apply and be issued a new ID number.</li> </ul>
Faroe Islands	civil registration number ( <i>p-ta</i> ) V number (for legal persons)	-	un-notified	-	<ul style="list-style-type: none"> <li>There is currently no solution to match cross-border service users with the population register.</li> <li>As Faroe Islands is not part of eIDAS scheme, identity data is moving through different service providers.</li> </ul>
Denmark	personal identification number ( <i>personnummer</i> or <i>CPR-nummer</i> )	Derived from DK's unique PID number	notified	substantial	<ul style="list-style-type: none"> <li>Names are registered differently across systems and countries. E.g., cross reference between foreign eID and CPR register fails, due to middle name(s) being omitted in either.</li> <li>Troublesome for users to register in IdM solution due to the complex user journey.</li> <li>Processing IdM applications manually demands resources, which makes it difficult to use in large scale.</li> </ul>
Lithuania	Personal code ( <i>asmens kodas</i> )	Personal ID number	notified	high	<ul style="list-style-type: none"> <li>Nationality attributes are calculated from the eIDAS code (PersonIdentifier) since for now there are no other working solutions.</li> </ul>
Latvia	Personal code ( <i>personas kods</i> )	The new type of personal code consists of eleven digits, ensuring the non-repetition of personal codes. The first digit of the personal code is "3", the second digit is an automatically generated random number from "2" to "9" by the system, and the remaining digits are automatically generated random numbers from "0" to "9" by the system.	notified	substantial and high	<ul style="list-style-type: none"> <li>When registering a company, it is not necessary to provide all the attributes that would be required for registration in the population register when registering the owner.</li> <li>There is a desire to create new e-services continuously, but often they are not developed from the users' perspective.</li> <li>The use of biometrics could increase, but currently, there are not very good solutions. To ensure consistent data quality in the population register, people's biometrics should be collected when recording personal data. Once this is achieved, viable solutions can be developed.</li> </ul>
Greenland		-	un-notified	-	

## 2.4.2 Overview of data's quality and trustworthiness in the Nordic-Baltic region

Nordic-Baltic region countries are following the same principles in terms of how data about country's population is maintained. All Nordic-Baltic countries have implemented centralized digital solution for population registry, which assures common practice of population management, reliability of data and high system availability.

The framework and implementation of population registries is stipulated by respective law and implementing acts. Legal acts stipulate the composition of data in the population registry and the procedure for maintaining the population registry, entering data to registry, ensuring access to data, and supervising these activities. Any activities within population registry must be in line with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR). It is common to have a single authority who is responsible for the maintaining of population registry.

Population registry's main purpose is to keep population records and by this assist governmental authorities, local authorities, and other legally entitled entities to perform their duties. Population registry is the tool for identity management, as correctness of personal identifiable information entered therein is assumed. In addition to personal identifiable information and persons' statuses (i.e., alive or dead) the population registry may contain data about marital status, kinship, education, etc.

Nordic and Baltic countries have established data exchange amongst themselves for managing population migration. The receiving country does notify the country of origin about residence settlement if respective agreements have concluded between two countries. Not all Nordic-Baltic countries have concluded such agreements that can lead to outdated of persons' residence data in population registry of country of migration origin.

Population registries operate based on primary key identifier, which is the personal identification number issued to a person. Some population registries also contain personal identification numbers assigned to persons by foreign countries or data about ID-document issued to population registry's subject by foreign countries. These named records may have only informative value.

Given the above-described circumstances it can be stated that data quality and trustworthiness is well handled by population registries of Nordic-Baltic countries. Potential identity and record matching solutions can incorporate and rely on personal identifiable information stored in population registries. On the other hand, depending on identity and record matching solutions, the population registries might be subject to further development in terms of composition of data in registries and new application programming interfaces (APIs) for data exchange and handling between identity and record matching actors/components.

For clarification the identifiers are described in Table 13 below.

**Table 13** Uniqueness and data structure of local identifier (PIC) per country.

Country	PIC derive	Digits	1	2	3	4	5	6	h	7	8	9	10	11	12	13
Estonia	+	11	G/Cn	Y	Y	M	M	D	-	D	Sq	Sq	Sq	Ch	-	-
Finland	+	11	D	D	M	M	Y	Y	+/-/A	Sq	Sq	G	V	-	-	-
Norway	+	11	D	D	M	M	Y	Y	+	Sq	Sq	Sq	Ch	Ch	-	-
Sweden	+	11	Y	Y	M	M	D	D	+	Cn	Sq	Sq	G	Ch	-	-
Iceland	+	10	D	D	M	M	Y	Y	+	R	R	Ch	Cn	-	-	-
Denmark	+	10	D	D	M	M	Y	Y	+	Cn	Sq	Sq	G	-	-	-
Faroe Islands	+	9	D	D	M	M	Y	Y	+	V	V	G	-	-	-	-
Lithuania	+	11	G/Cn	Y	Y	M	M	D	-	D	Sq	Sq	Sq	Ch	-	-
Latvia	-	11	3	R	R	R	R	R	-	R	R	R	R	R	-	-
Greenland	+	10	D	D	M	M	Y	Y	+	Cn	Sq	Sq	G	-	-	-

"+" = yes, "-" = no

\* DD-day, MM- month, YY-year, G-gender, Cn-century, Sq-sequence, R-random, Ch-check, H-hyphen, V-verification.

### 2.4.3 Joint difficulties to tackle in collaboration

Through the whole AS-IS analysis five main issues popped out more often and were associated with most impact by most countries interviewed (see Table 14):

**Table 14** Five main issues with most impact on achieving the common vision

Description of the issue	Problem area
A. <b>Recurring work</b> is done for identity verification and matching. If a person's activities engage different domains, then <b>identity matching results are not shared</b> within the state. Moreover, the identity matching results are not shared between the states.	Scope
B. There are <b>differences in PII</b> (Personal Identifiable Information) <b>datasets operated by states</b> due to their legal and cultural particularities (e.g., place of birth logic, contact address obligation, facial biometric data storage/usage, derived PNOs towards other states, pseudonyms). Therefore, common best practices are hard to be defined.	Principles
C. <b>Motivation for changing status quo is low</b> due to high initial investment costs, even though risks associated with potential identity mismatch are serious. Current fragmented processes allow also to keep the scope of any error clearly local.	Principles
D. <b>Low capability of Population Registries to adapt to any changes in PII dataset</b> or modifications/improvements in processes of PII handling. As central repositories with also crucial national importance Population Registries primary responsibility is to each Member State, persons currently not residents of MS may not get attention and budget.	Technology
E. Identity verification and matching is <b>manual work</b> performed by personnel who are not trained/experts in ID-management (healthcare, educational personnel, etc.).	Scope

Those issues were validated in a physical workshop, which brought together respective parties of Nordic-Baltic countries. Every issue was analyzed from different angles, considering countries perspectives (see 2.4.4.

## Vision

Main issues above should be solved by achieving a "Happy Day" vision for different stakeholders. And a future solution must be designed accordingly for those (three main) stakeholders:

- A person with positive intentions towards use of identity and record matching services can easily connect all one's identities and relating records in any information system across Nordic States.
- A person with negative intentions towards use of identity and record matching services cannot hide one's other identities across Nordic States and their related records.
- States can find duplicated identities from Population Registries across Nordic States, and match records accordingly.

## Difficulties causing issues



Those five main issues are related to, or directly caused by joint difficulties identified during analysis of the AS-IS situation. These should be tackled in collaboration to solve the main issues and to achieve a "Happy Day" for stakeholders (see Table 15):

Those fifteen difficulties are **resulting in unwanted situations** regarding either service user or the services itself:

- user is denied access to cross-border services.
- user is not matched to identity.
- records are not matched to the user.
- cross-border services are not used or developed.

All those elements described above "vision for stakeholders + situations + difficulties + problem area" are joint together in Table 16 to illustrate the complexity of the situation that future Nordic-Baltic identity and record matching solution must unravel.

**Table 15** Fifteen difficulties that are causing five main issues.

Description of the difficulties to be tackled in co-operation	Where the Problem MAINLY LIES? *
1. eIDAS fully not working as intended (functionally and coverage of member states);	Technology
2. cross-border e-services require person to have local (e-service's country of location) personal identifier, which can be obtained through physical process;	Scope
3. reduced economic benefit (investment vs usage volume) in smaller countries;	Principles
4. national registries and their conformity with international technical standards/national legislation varies;	Principles
5. SLD access might be restricted;	Technology
6. every MS does not have notified eID scheme;	Technology
7. personal identifiers of other countries are not stored in registries;	Technology
8. varying country or sectorial specific requirements/acceptance for level of assurance in identification process;	Scope
9. extending scope of attributes available through eID schemes beyond the defined minimum data set is practically impossible;	Scope
10. unique identifiers may contain derived personal identifiers;	Scope
11. cross-border personal identifier sharing can have national restrictions;	Technology
12. manual processing of IdM applications is resources demanding and imposes limitation for scaling the solution	Scope
13. no solution available for e-services to match cross-border users with local identities	Technology
14. countries issue their national Registry number (PIC) through physical process	Scope
15. not all organizations can process a person's data with an eIDAS UID, i.e. without local personal identifier	Principles

\* The problem can manifest in more than one area, but here the main issue is highlighted.

**Table 16** Summary of difficulties in regard to Single Digital gateway vision<sup>[106]</sup>

Single digital gateway use vision:1		Fully digital process and uninterrupted customer journey		Unified maturity level		Set of attributes ensures compatibility with relying parties	
Concerning:		Scope (States: internal or cooperation)		Technology and infrastructure		Principles and Regulations	
Situation caused by difficulties:		user is denied of access to cross-border services	duplicated ID-s	user is not matched to identity	records are not matched to user	Cross-border services are not used or developed	
Impact on:	Person with positive intentions	...can easily connect all one's identities in any information system across Nordic States	8. varying country or sectorial specific requirements/ acceptance for level of assurance in identification process	2. cross-border e-services require person to have local (e-service's country of location) personal identifier, which can be obtained through physical process	5. SLD access might be restricted	11. cross-border personal identifier sharing can have national restrictions	15. not all organizations can process a person's data with an eIDAS UID, i.e. without local personal identifier
	Person with negative intentions	...cannot hide one's other identities and related records across Nordic States	9. extending scope of attributes available through eID schemes beyond the defined minimum data set is practically impossible	10. unique identifiers may contain derived personal identifiers	13. no solution available for e-services to match cross-border users with local identities	7. personal identifiers of other countries are not stored in registries	4. national registries and their conformity with international technical standards/ national legislation varies
	States	...can find a duplicated identities from Population Registries across Nordic States, and match records accordingly	14. countries issue their national Registry number (PIC) through physical process	12. manual processing of IdM applications is resources demanding and imposes limitation for scaling the solution	1. eIDAS fully not working as intended (functionally and coverage of member states)	6. every MS does not have notified eID scheme	3. reduced economic benefit (investment vs usage volume) in smaller countries

106. Difficulties (in the middle of this matrix) are numbered the same, as it was done previously in Table 15

#### 2.4.4 Summary of common issues and input to solutions

On joint seminars 5 previously mentioned issues (from A. to D. at Table 14) were analyzed and possible solutions were discussed. Most importantly, the question “**What could be the solutions to overcome the problem?**” was asked. The following lists present the results from the seminar, and therefore gave a direct input to TO-BE analysis.

- A. **Recurring work** is done for identity verification and matching if person’s activities engage different domains as **identity matching results are not shared within the state**. Moreover, the identity matching results are not shared between the states.
  - Why is this a problem in the first place (what consequences may arise from it)?
    1. Clients must re-identify themselves (inconvenience)
    2. No overview of the person on country level
  - What does this mean (what might accompany this problem)?
    1. Possibility of fraud
  - How has this problem arisen (for what reasons)?
    1. Needs for different sectors are different.
    2. High-level of match making is not necessary for all
  - Why is the problem unresolved (for what reasons)?
    1. Whose responsibility it is?
    2. Decentralization
    3. Lack of regulations
  - **What could be the solutions to overcome the problem?**
    1. National ID solutions
    2. Common framework for ID matching in EU level
  
- B. There are differences in PII (Personal Identifiable Information) **datasets operated by states** due to their legal and cultural particularities (e.g., place of birth logic, contact address obligation, facial biometric data storage/usage, derived PNOs towards other states, pseudonyms).
  - Why is this a problem in the first place (what consequences may arise from it)?
    1. We need solutions for eIDAS and SDG.



- What does this mean (what might accompany this problem)?
    1. Problems in providing e-services.
    2. Problems in e-identification
  - Why is the problem unresolved (for what reasons)?
    1. GDPR restrictions (conflict with identity matching goals)
    2. It's a new problem.
    3. No agreement on datasets
    4. Legal and cultural background is different.
  - **What could be the solutions to overcome the problem?**
    1. Common rules on datasets; in ID numbers
    2. Data from passports
    3. Passports mandatory
- C. Risks associated with potential identity mismatch and the economic benefits of enhanced/automated processes are small/minimal. Thus, **motivation for changing the status quo is low.**
- Why is this a problem in the first place (what consequences may arise from it)?
    1. Nothing changes
    2. No e-services and no clear ownership
    3. What does this mean (what might accompany this problem)?
    4. Low usage of cross-border e-services
    5. Low eID means usage.
  - How has this problem arisen (for what reasons)?
    1. Not doing anything is less of a burden.
    2. No value in resolving (lack of motivation)
  - Why is the problem unresolved (for what reasons)?
    1. GDPR conflict
    2. Mistrust of governance
    3. Low nr of (cross-border) e-services
    4. Low volume of users
    5. Too few attributes (risk of mismatch)

- **What could be the solutions to overcome the problem?**
  1. More attributes mandatory
  2. Data sharing agreement in NBC
  3. Store eID dataset in registries
  4. NBC voluntary identifier
  5. Biometrics
  6. Fingerprint as a minimum dataset
  7. Have a friend in every country to validate you as a person.
  
- D. **Low capability of Population Registries to adapt to any changes in PII dataset** or modifications/improvements in processes of PII handling.
  - Why is this a problem in the first place (what consequences may arise from it)?
    1. Old registries
    2. Any changes are large-scale ones.
  - What does this mean (what might accompany this problem)?
    1. Changes can brake systems.
    2. How has this problem arisen (for what reasons)?
    3. Motivation is low.
    4. The cost of changes is high.
    5. No small things and quick fixes
  - **Why is the problem unresolved (for what reasons)?**
    1. Low motivation
    2. What could be the solutions to overcome the problem?
    3. Cooperation on NBC level
    4. Sharing data between population registries
    5. piloting

Identity verification and matching is **manual work** performed by personnel who are not trained/experts in ID-management (healthcare, educational personnel, etc.)

- Why is this a problem in the first place (what consequences may arise from it)?
  1. Manual work takes time and workforce.
  2. What does this mean (what might accompany this problem)?
  3. Time, cost
  4. Can't access services.

- How has this problem arisen (for what reasons)?
  1. you need to have an eID.
  2. Why is the problem unresolved (for what reasons)?
  3. Low motivation
  4. Population registries capability
- **What could be the solutions to overcome the problem?**
  1. financing

According to the vision and to address today's difficulties (see [2.4.3](#)), 10 possible solutions for Nordic-Baltic identity and record matching were derived, which were also validated on the joint workshop.



These options will be described, and one from these will be selected, or some other solution will be developed during the TO-BE analysis.

# 3. TO-BE

## 3.1 Overview of possible solutions

Now that we know, what the main issues in identity and data matching are, and what problems should and could be tackled together in the region, we conducted 10 preliminary solutions what were presented in a live workshop on 12<sup>th</sup> and 13<sup>th</sup> September in Tallinn. These solutions were described on high level through story telling method involving personas, epic, user stories and use cases. In the following chapter high level description are presented outlining their strengths and weaknesses.

### Process and thought behind 3 types of personas

We brought in 3 scenarios based on main persona:

1. **Willing to cooperate, active person.** With scenario 1 we may assume that we are living in an abundance of information if such information exists or can be created. A person is willing to share information necessary to make decision on the identity matching and is also assumed to be active in sharing that information. In this scenario the risk of NOT matching is leaving a person without their right to access the data about them and exercising their rights on that data.
2. **Unwilling to cooperate, passive and resisting person.** In scenario 2 we imagined an actor who does not actively want to connect identities one has in different countries. This may be for simple privacy concerns one has or that such matching would harm a person's ability to perform intended actions now or in the future. Therefore, the identity matching decision might need to be made in lack of data. User intent on not cooperating may be not detected and even if detected the motivation will not be clear. The biggest risk in this scenario is NOT matching person to existing records and giving them unearned clean start.
3. **State who is interested to have up to date records in their registries** (population registry, social benefits applicants, tax declarations, etc.). The third scenario is meant to allow Member States to perform their duties and serve their residents. Law may either grant some benefits of take them away based on individual's activities and if these activities are performed in different Member State may not matter. People are either unaware that they should report something to a Member State, or they refuse to report that knowingly. Thus, matching people's records bilaterally seems to include promise to mitigate several risks for states. The risk of incorrect matching

and the risk of not finding a match when there really is one both may have significant negative consequences due to the scale of the process.

The 10 possible solutions to address these three scenarios are as follows.

## Exresidence

Every country issue through digital process local eID mean (e.g., to EUDIW - EU Digital Identity Wallet, or a separate token) to cross-border users trying to access that country's e-services. This way a person gets eID mean that local e-service can operate with, and user will be enabled to enjoy e-services in other country and access his/her personal records. With this solution identity matching process for potential later cross-border identity or record matching remains unsolved, as no identity matching is performed.

- + User can swiftly access cross-border e-services.
- Most countries must develop digital issuance process for their eID mean(s), which requires also principal legal changes.
- **The problem of identity matching is not solved but pushed one step further.**

## QuickFix

Convert personal identification number's physical issuance process into digital remote video identity verification process and integrate this process into current business flow of e-services' usage. Proposed digital identity creation (personal identification number issuance) is based on combination of eID authentication and capture of biometric identifier (facial image). Processing facial images depends on country's practices. The process ends with establishing connection between two countries' personal identification numbers in local population registry.

- + Users can access cross-border e-service through purely digitally provided workflow.
- + Remote video identity solutions can be designed to meet every country's requirement.
- + Physical process can be replaced by a digital one – potential efficiency.
- Countries must develop new digital business processes and create respective legal framework influencing existing principles.

- Technologically more complex process, which requires involvement of knowledge from additional fields of expertise.

## Hard\_EAA

Country of an e-service provider concludes identity matching using eID mean from other country and data from local population registry. Output of identity matching process is delivered in format of electronic attestation of attributes (EAA), which includes link between personal identification numbers of two countries and other necessary PII. EAA is delivered to e-service that is being accessed by user. In addition, EAA is delivered to the user, so a person can use it as identity matching evidence during future interactions with e-services.

- + Users can access cross-border e-service through purely digitally provided workflow.
- + Minor or no changes to user experience, as process is based on regular usage of eID mean.
- Countries must establish a framework for legal recognition of EAAs, their technical format, exchange/storage mechanisms and validation principles.

## Easy\_EAA

Service, which allows "pairing" of eID means of two countries. Country of an e-service provider concludes identity matching using eID means at person's hand. Identity matching service establishes a link between two identities based on attributes received from eID means of both countries. Ground for match bases on uninterrupted process performed by authoritative party during which authentication with both eID means is performed, thus identities of two countries can be linked.

Output of identity matching process is delivered in format of electronic attestation of attributes (EAA), which includes link between personal identification numbers of two countries and other necessary PII. EAA is delivered to e-service that is being accessed by user. In addition, EAA is delivered to the user, so a person can use it as identity matching evidence during future interactions with e-services.

- + Users can access cross-border e-service through purely digitally provided workflow.
- + Minor or no changes to user experience, as process is based on regular usage of eID means.

- Not every user has eID meanings from two countries at hand.
- Countries must establish a framework for legal recognition of EAAs, their technical format, exchange/storage mechanisms and validation principles.

## eIDAS\_0

User is granted access to cross-border e-services based on eID mean of his/her country of residence. Identity matching is performed relying on attributes received from eID mean and PII coming from population registry of cross-border e-service location. Result of identity matching will have use for the countries general identity management purposes and is made available to e-services, whereas e-services operate in their internal processes based on personal identification number delivered by eID mean of other country. E-services must be able to operate with a foreign personal identification number.

- + No changes to user experience, as the process is based on regular usage of eID mean.
- **Significant impact (impossible to deploy) on business logic of e-services.**

## eIDASNode+

Every foreign identity will be assigned a local personal identification number. After authentication with eID mean through eIDAS node e-services approach local identity matching service for retrieval of local personal identification number of user. E-services are required to implement in their user authentication flow an intermediate step for API request towards identity matching service for retrieval of local personal identification number. Identity matching service either finds a match form (population) registry or creates new local identity. Output of identity matching process includes link between personal identification numbers of two countries and other necessary PII.

- + Minor or no changes to user experience, as process is based on regular usage flow of eID means.
- + E-services can operate based on local personal identification number.

## E-services can operate based on local personal identification number.Defense

Biometric identity verification (1:1) is added to the eID authentication process to perform identity matching process. A person's facial image is captured during authentication step by identity matching service using remote video identity verification technology. Biometric verification is performed based on user facial images captured from video session and facial image retrieved from biometric database of e-service's country of location.

- + Usage of additional strong attributes, that provides required level of assurance for identity management that might not be achievable with eID mean's attributes only.
- **Not all countries store biometric data of residents.**
- Technologically more complex process, which requires involvement of knowledge from additional fields of expertise.
- Usage of biometric identifiers for identity verification in context of cross-border e-service usage can be legally challenging.

## Hinting

Identity matching is performed based on minimum mandatory data set provided by eIDAS node and using country specifically available additional attributes (in addition to 4 mandatory attributes) from eID means. Input for identity matching process is collected during eID authentication and matching system attempts to execute the process based on limited attributes and PII available in local population registry.

- + No changes to user experience, as the process is based on regular usage of eID mean.
- Limited number of attributes available, which probably require usage of supplementary procedures for establishing identity match.
- Usage of e-service might fall into physical process.
- **Current modus operandi, which does not work in practice.**



## Bonding

Process involving interaction of backend systems of two countries, where biometric verification (1:1) or identification (1:n) is part of identity matching process.

Proceedings between two countries are executed based on triggers, which are not related to direct activities of user during consuming of e-service (e.g., migration events, activities in non-residential country, etc.) whereas person him/herself is not involved in the matching process. Country in necessity for identity matching initiates procedure, where PII and facial images are retrieved from databases of both countries. Following steps on top of PII data matching include facial image verification/identification either by country in necessity or by both countries.

- + Usage of additional strong attributes, that provides required level of assurance for identity management that might not be achievable with PII only.
- **Not all countries store biometric data.**
- Technologically more complex process, which requires involvement of knowledge from additional fields of expertise.
- Usage of facial image for biometric verification/identification in context of cross-border e-service usage can be legally challenging.

## Binding

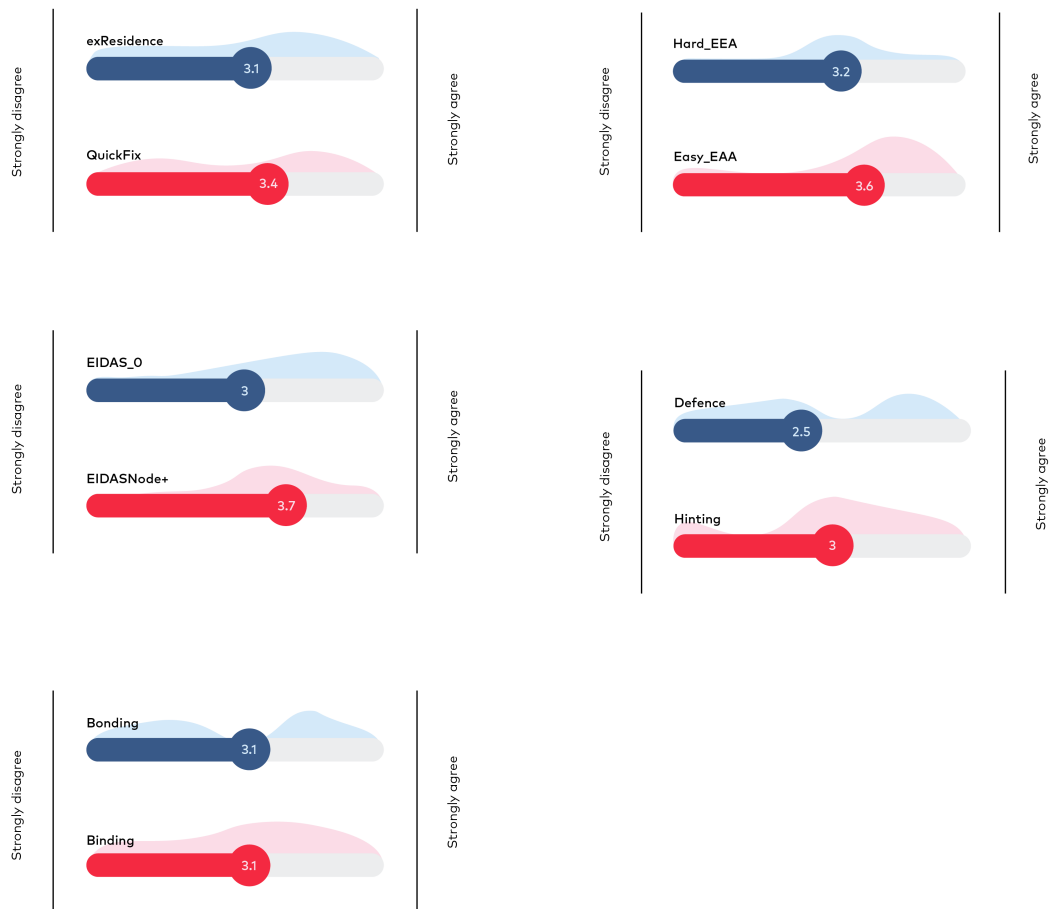
Process involving data exchange between population registries of two countries, which is followed by identity matching process. Proceeding is initiated by backends systems following defined triggers (e.g. migration events, activities in non-residential country, etc.) whereas person him/herself is not involved in the matching process. Country in necessity for identity matching initiates process for exchange of person's PII between two countries and executes identity matching.

- + Solution operates based on common PII used for identity management.
- **Reliability of matching outcome might be questionable, as partial matches are expected to have significant proportion due to person him/herself not being involved in proceedings.**
- **"Partial matches" require manual processing.**

**Evaluation of 10 preliminary solutions** was conducted by combining 2 methods. First the 10 possible solutions were introduced at a seminar, where the participants were asked to evaluate the suitability of each solution by rating them on a scale from 1 to 5. Before casting the votes, participants and solutions' presenters discussed each solution and questions from audience were answered or remarks taken. The results of voting are depicted on Figure 13, where average score and distribution of provided points are depicted for each solution. Score of voting is summarized in Table 17, showing the ranking of solutions.

Secondly, conductors of analysis evaluated the strengths and weaknesses of all 10 solutions. Based on identified substantial weaknesses (above marked bold) and low efficiencies 6 solutions were discarded from further analysis. It must be noted that the 4 most preferred solutions voted by participants of Tallinn workshop and selected through analysis did match 100%.

In [Ch. 3.2](#) the four most potential solutions will be described in more detail.



**Figure 13** Preferences of solutions from Tallinn workshop participants (average score and distribution of points)

**Table 17** Ranking of solutions based on poll with Tallinn workshop participants

Solution	Score
eIDASNode+	3,7
Easy_EAA	3,6
QuickFix	3,5
Hard_EAA	3,2
Bonding	3,1
Binding	3,1
exResidence	3,0
eIDAS_0	3,0
Hinting	3,0
Defence	2,5

## 3.2 Description of highest potential solutions

The four highest potential solutions are the following:

1. eIDASNode+
2. Easy\_EAA
3. QuickFix
4. Hard\_EAA

We will elaborate on these solutions in more detailed through personas, epic, user stories and use cases.

### 3.2.1 eIDASNode+

For every foreign identity a local personal identification number will be assigned. After authentication with eID mean through eIDAS node, e-services approach local identity matching service for retrieval of local personal identification number of user. E-services are required to implement in their user authentication flow an intermediate step for API request towards identity matching service for retrieval of

local personal identification number. Identity matching service either finds a match form (population) registry or creates new local identity. Identity matches can be already established during some administrative procedures undergone earlier (e.g. registering residence).

Output of identity matching process delivered to e-service includes link between personal identification numbers of two countries and other necessary PII. Exchange of data about matched identities between two involved countries is essential for successful deployment of once only principle and trustworthy identity management in Nordic-Baltic region.

Data exchange between countries can be performed based on to be established framework defining principles for identity matching process and acceptance of matched identities between countries in Nordic-Baltic region.

E-services in receiving country continue operating with local personal identification number.

## Personas

John

- is a resident of country\_A,
- has eID\_A mean from country\_A,
- has been awarded bachelor's degree (diploma) at university\_B located in country\_B,
- wants to apply for master's degree at university\_A in country\_A,
- is eager to improve his educational qualification and is thereof very co-operative (has no problem with submitting PII beyond eID scheme content).

University\_A

- has e-service for submitting applications for admission to university,
- e-service users can authenticate with eID means supported by eIDAS node,
- must verify holding of bachelor's degree,
- must match the identity of diploma holder with the identity of authenticated user.

University\_B

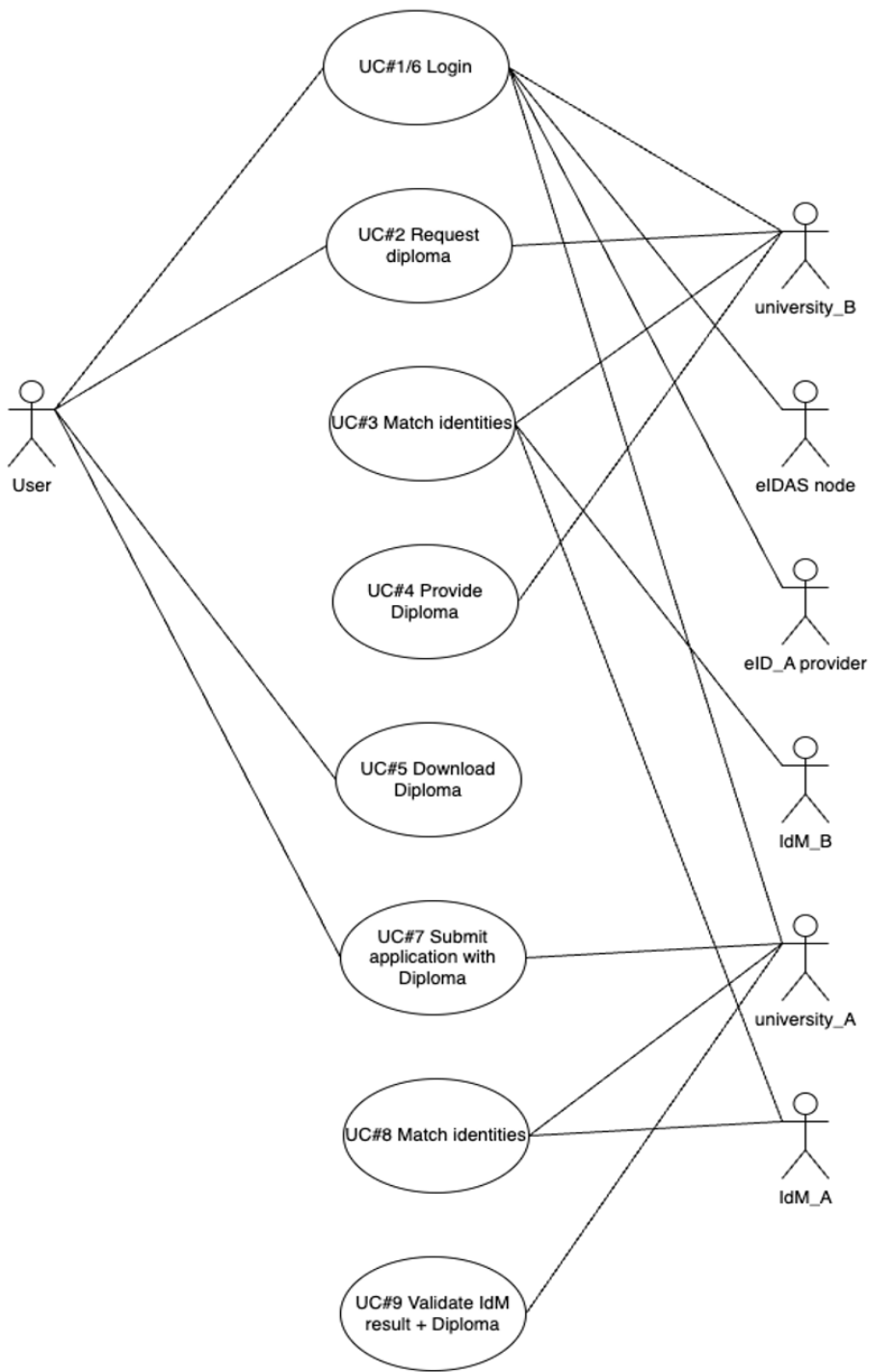
- has e-service, which provides access to diploma records,
- e-service users can authenticate with eID means supported by eIDAS node,
- must match the identity of diploma holder with the identity of authenticated user.

#### Country\_A IdM service provider (IdM\_A)

- has access to PII data of country\_A residents,
- has processes and logic in place for IdM,
- has access to data of matched identities, authority to create matches between identities and create new identity in country\_A,
- has data exchange with IdM\_B for sharing matching results involving identities of country\_A and country\_B,
- accepts and trusts matching results delivered by IdM\_B, which involve identities of country\_A and country\_B.

#### Country\_B IdM service provider (IdM\_B)

- has access to PII data of country\_B residents,
- has processes and logic in place for IdM,
- has access to data of matched identities, authority to create matches between identities and create new identity in country\_B,
- has data exchange with IdM\_A for sharing matching results involving identities of country\_A and country\_B,
- accepts and trusts matching results delivered by IdM\_A, which involve identities of country\_A and country\_B.



**Figure 14** Use case on EIDASNODE+

## Epic

As John, I want to prove the obtaining of bachelor's degree in university\_B to apply for master's degree in university\_A.

## User stories

As John, I want to retrieve and present my diploma through e-services of universities to facilitate the process.

As John, I want to identify myself with my eID\_A to provide assurance of my identity.

As John, I want diploma to be matched with my identity\_A to prove obtaining of bachelor's degree.

As university\_A/B, I want to provide e-services for document/process management for optimizing workload.

As university\_A/B, I want to enable access to e-services with eID means supported by eIDAS node for reliable authentication of users.

As university\_A/B, I want to rest assured that identities of diploma holder and authenticated user are matching for avoidance of misuse/fraud.

## Use cases

UC#1 User authenticates with eID\_A to university\_B e-service.

- University\_B e-service authenticates user through eIDAS node and eID\_A provider and receives identity attributes for eID\_A.

UC#2 User submits request for collecting the bachelor's degree diploma.

UC#3 University\_B e-service interacts with IdM\_B for establishing the alumni identity.

- University\_B e-service delivers eID\_A attributes to IdM\_B.
- IdM\_B searches for existing matches between Id\_A and Id\_B.
- If not found, then IdM\_B searches from Country\_B registry match for Id\_A. Match between Id\_A and Id\_B is created in Country\_B registry and stored with Id\_A attributes. IdM\_A is notified about created match of identities and data is stored in Country\_A registry.
- If no match is found, then IdM\_B creates new Id\_B in Country\_B registry. Match between Id\_A and Id\_B is created in Country\_B registry and stored with Id\_A attributes. IdM\_A is notified about created match of identities and data is stored in Country\_A registry.
- IdM\_B provides Id\_B attributes to University\_B e-service.

UC#4 University\_B e-service displays to user diploma evidence.

UC#5 User downloads the diploma evidence.

UC#6 User authenticates with eID\_A to university\_A e-service.

UC#7 User submits application for admission to master's programme.

- User uploads the diploma as attachments to application.

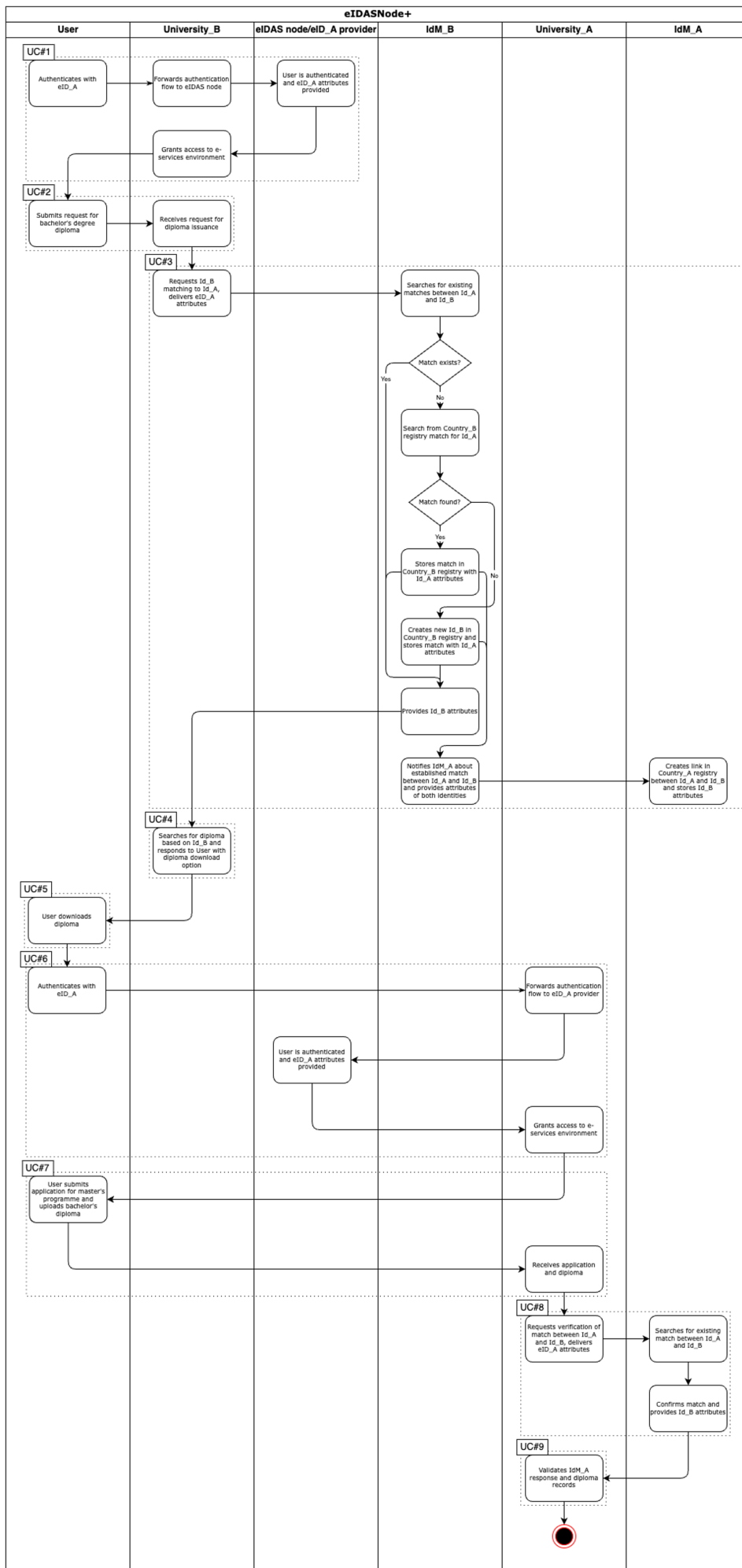
UC#8 University\_A e-service interacts with IdM\_A for verifying match between Id\_A and Id\_B.

- University\_A e-service delivers eID\_A attributes to IdM\_A.
- IdM\_A searches for existing matches between Id\_A and Id\_B.
- Existing match is found due to IdM\_B having shared result of earlier matching process conducted with User's identities.
- IdM\_A confirms match of two identities and provides Id\_B attributes to University\_A e-service.

UC#9 University\_A e-service validates IdM\_A response and diploma records.

- Upon successful validation of IdM\_A response and diploma records, User's application is accepted.





**Figure 15** eIDASNode+ detailed WORKFLOW

### 3.2.2 Easy\_EAA

Service, which allows "pairing" of eID means of two countries. Country of e-service provider concludes identity matching using eID means at person's hand. Identity matching service establishes a link between two identities based on attributes received from eID means of both countries. Ground for match bases on uninterrupted process performed by authoritative party during which authentication with both eID means is performed, thus identities of two countries can be linked.

Output of identity matching process is delivered in format of electronic attestation of attributes (EAA), which includes link between personal identification numbers of two countries and other necessary PII. EAA is delivered to e-service that is being accessed by user. In addition, EAA is delivered to the user, so a person can use it as identity matching evidence during future interactions with e-services.

#### Personas

John

- is resident of country\_A,
- has eID\_A mean from country\_A,
- has eID\_B mean from country\_B,
- has been awarded bachelor's degree (diploma) at university\_B located in country\_B,
- wants to apply for master's degree at university\_A in country\_A,
- is eager to improve his educational qualification and is thereof very co-operative (has no problem with submitting PII beyond eID scheme content).

University\_A

- has e-service for submitting applications for admission to university,
- e-service users can authenticate with eID means issued in country\_A,
- must verify holding of bachelor's degree,
- must match identity of diploma holder with the identity of authenticated user,
- has capability to process EAAs.

## University\_B

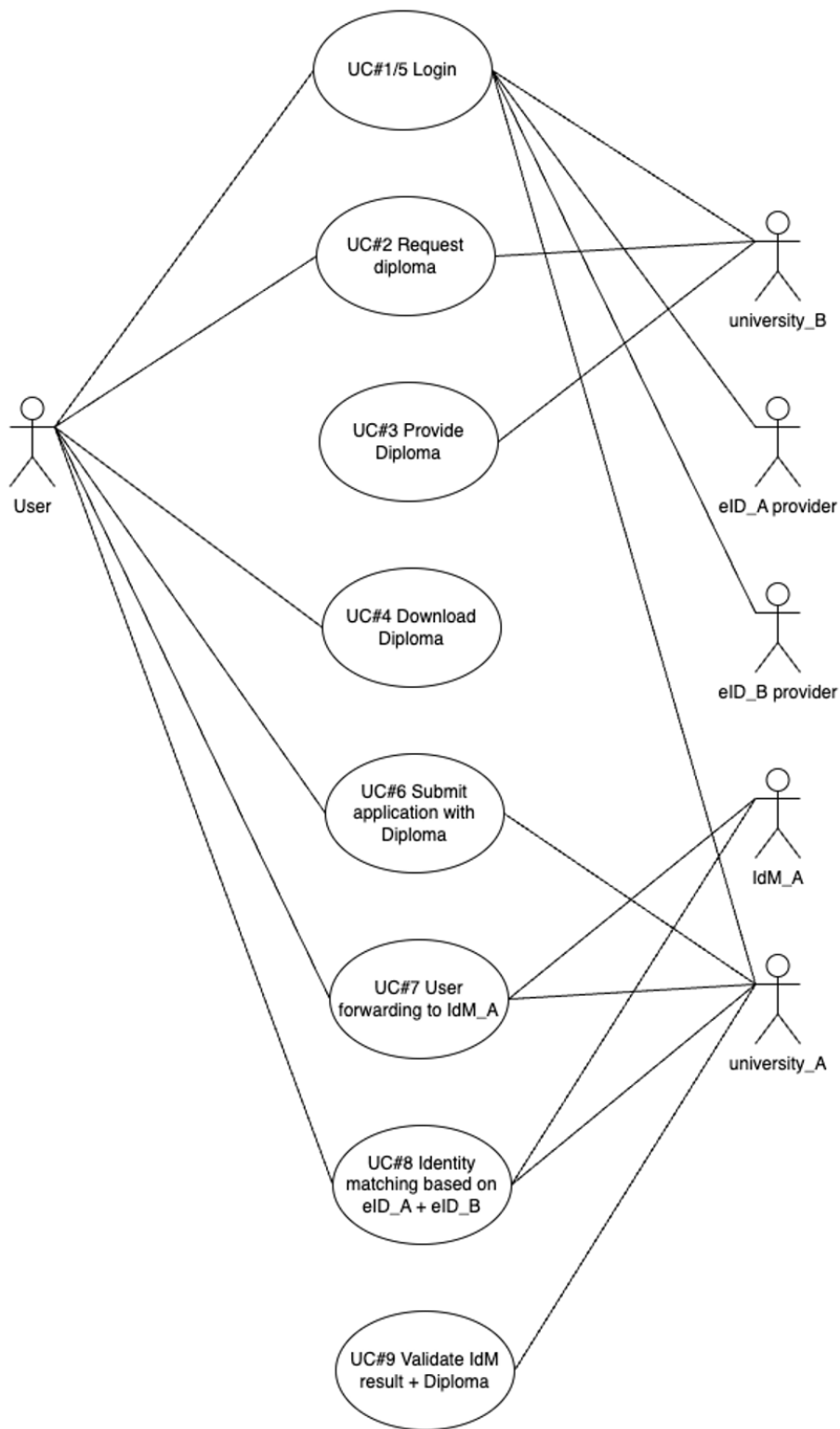
- has e-service, which provides access to diploma records,
- e-service users can authenticate with eID means issued in country\_B,
- must match identity of diploma holder with the identity of authenticated user,
- has capability to process EAAs.

## Country\_A IdM service provider (IdM\_A)

- has access to PII data of country\_A residents,
- has processes and logic in place for IdM,
- has process for reliably pairing of eID means of two countries,
- has access to data of matched identities, authority to create matches between identities and create new identity in country\_A,
- has data exchange with IdM\_B for sharing matching results involving identities of country\_A and country\_B,
- accepts and trusts matching results delivered by IdM\_B, which involve identities of country\_A and country\_B,
- issues matching results in format of EAAs.

## Country\_B IdM service provider (IdM\_B)

- has access to PII data of country\_B residents,
- has processes and logic in place for IdM,
- has process for reliably pairing of eID means of two countries,
- has access to data of matched identities, authority to create matches between identities and create new identity in country\_B,
- has data exchange with IdM\_A for sharing matching results involving identities of country\_A and country\_B,
- accepts and trusts matching results delivered by IdM\_A, which involve identities of country\_A and country\_B,
- issues matching results in format of EAAs.



**Figure 16** Use case for EASY\_EAA

## Epic

As John, I want to prove the obtaining of bachelor's degree in university\_B to apply for master's degree in university\_A.

## User stories

As John, I want to retrieve and present my diploma through e-services of universities to facilitate the process.

As John, I can identify myself with my eID\_A and eID\_B to provide assurance of my identity in both countries.

As John, I want diploma to be matched with my identity\_A to prove obtaining of bachelor's degree.

As university\_A/B, I want to provide e-services for document/process management for optimizing workload.

As university\_A/B, I want to enable access to e-services with eID means supported by eIDAS node for reliable authentication of users.

As university\_A/B, I want to rest assured that identities of diploma holder and authenticated user are matching for avoidance of misuse/fraud.

## Use cases

UC#1 User authenticates with eID\_B to university\_B e-service.

- University\_B e-service authenticates user through eID\_B provider and receives identity attributes for eID\_B.

UC#2 User submits request for collecting the bachelor's degree diploma.

UC#3 University\_B validates eID\_B attributes against diploma records and displays to user diploma evidence.

UC#4 User downloads the diploma evidence.

UC#5 User authenticates with eID\_A to university\_A e-service.

- University\_A e-service authenticates user through eID\_A provider and receives identity attributes for eID\_A.

UC#6 User submits application for admission to master's programme.

- User uploads diploma as attachments to application.

UC#7 University\_A e-service interacts with IdM\_A for verifying match between Id\_A and Id\_B.

- IdM\_A searches for existing matches between Id\_A and Id\_B.
- If not found, then IdM\_A searches from Country\_A registry match for Id\_B. Match between Id\_A and Id\_B is created in Country\_A registry and stored with Id\_B attributes. IdM\_B is notified about created match of identities in format of EAA and data is stored in Country\_B registry.
- If no match found, then IdM\_A requests User through open session with University\_A to authenticate with eID\_B and eID\_A in sessions under control of IdM\_A. Once User has authenticated with both eID\_B and eID\_A in the session created by IdM\_A the match between both identities is created. IdM\_B is notified about created match of identities in format of EAA and data is stored in Country\_B registry.
- IdM\_A confirms match of identities and provides Id\_B attributes to University\_A e-service in format of EAA.

UC#8 University\_A e-service validates IdM\_A matching result EAA against diploma attributes.

- Upon successful validation of IdM\_A response and diploma records, User's application is accepted.

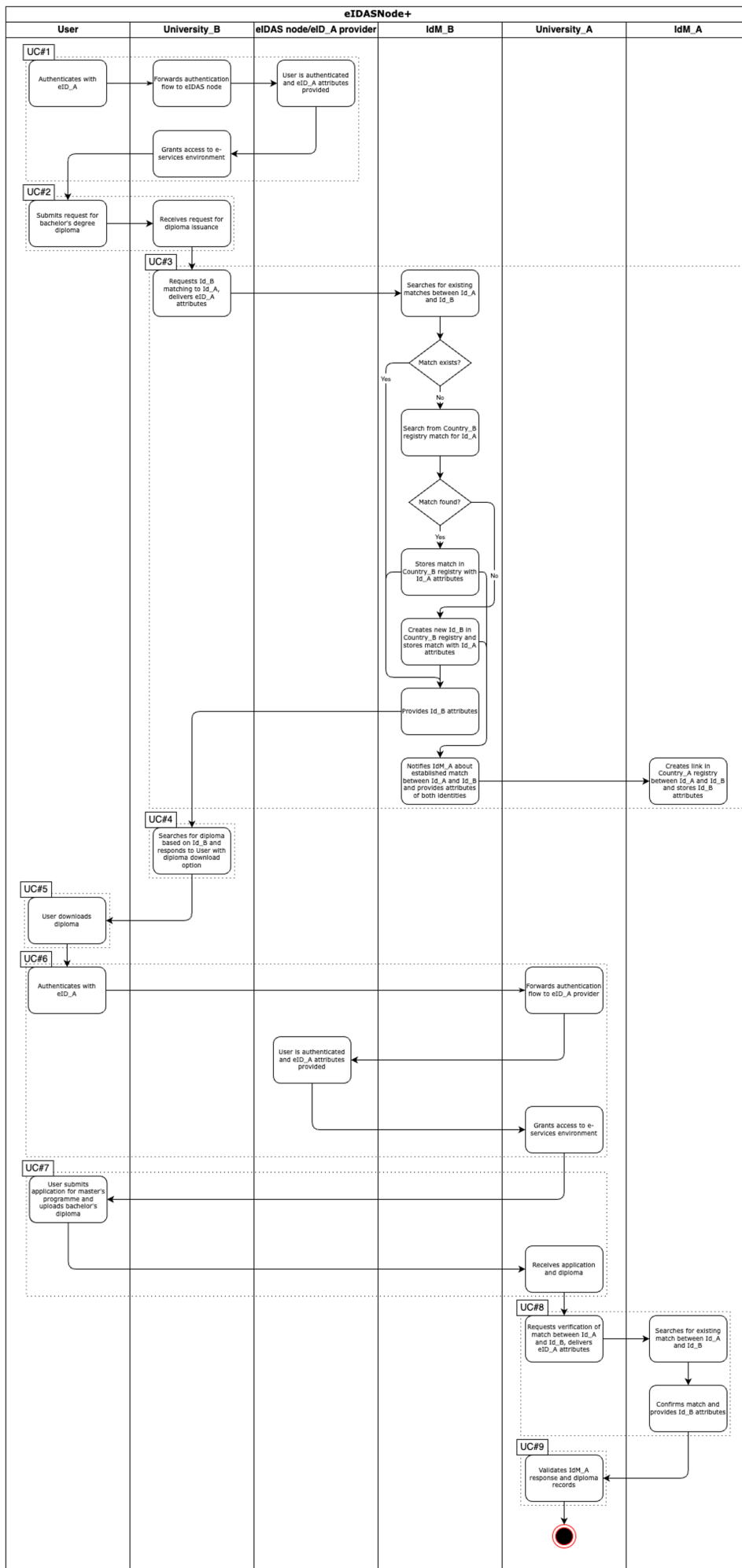


Figure 17 Easy\_EAA detailed WORKFLOW

### 3.2.3 QuickFix

Convert personal identification number's physical issuance process into digital remote video identity verification process and integrate this process into current business flow of e-services' usage. Proposed digital identity creation (personal identification number issuance) is based on combination of eID authentication and capture of biometric identifier (facial image). Processing facial images depends on country's practices. The process ends with establishing connection between two countries' personal identification numbers in local population registry.

#### Personas

John

- is resident of country\_A,
- has eID\_A mean from country\_A,
- has been awarded bachelor's degree (diploma) at university\_B located in country\_B,
- wants to apply for master's degree at university\_A in country\_A,
- is eager to improve his educational qualification and is thereof very co-operative (has no problem with submitting PII beyond eID scheme content).

University\_A

- has e-service for submitting applications for admission to university,
- e-service users can authenticate with eID means supported by eIDAS node,
- must verify holding of bachelor's degree,
- must match the identity of diploma holder with the identity of authenticated user.

University\_B

- has e-service, which provides access to diploma records,
- e-service users can authenticate with eID means supported by eIDAS node,
- must match the identity of diploma holder with the identity of authenticated user.

Country\_A IdM service provider (IdM\_A)

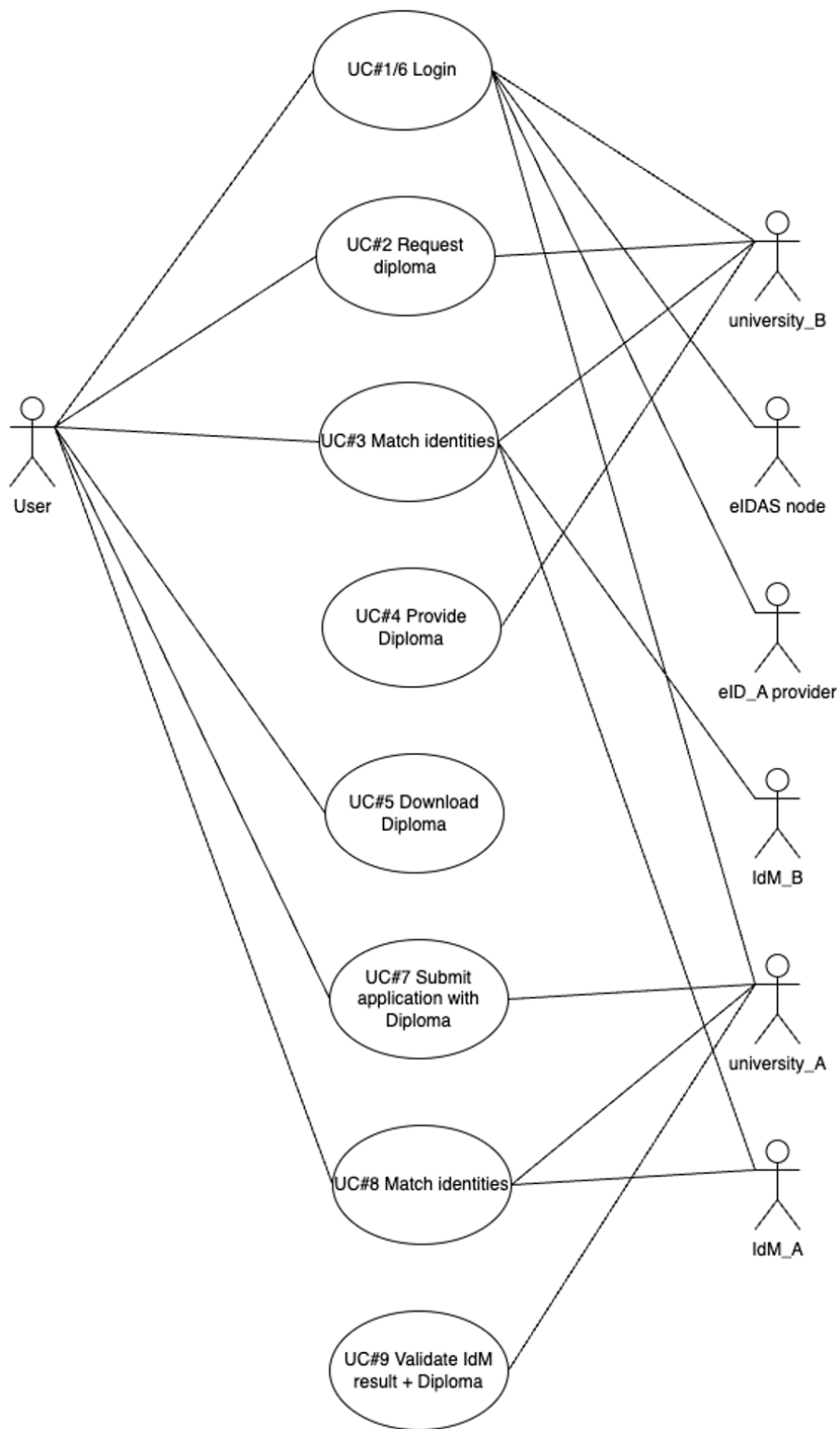
- has access to PII data of country\_A residents,
- has processes and logic in place for IdM,
- has access to data of matched identities, authority to create matches between identities and create new identity in country\_A registry,



- has data exchange with IdM\_B for sharing matching results involving identities of country\_A and country\_B,
- accepts and trusts matching results delivered by IdM\_B, which involve identities of country\_A and country\_B.

#### Country\_B IdM service provider (IdM\_B)

- has access to PII data of country\_B residents,
- has processes and logic in place for IdM,
- has access to data of matched identities, authority to create matches between identities and create new identity in country\_B registry,
- has data exchange with IdM\_A for sharing matching results involving identities of country\_A and country\_B,
- accepts and trusts matching results delivered by IdM\_A, which involve identities of country\_A and country\_B.



**Figure 18** Use case for QUICKFIX

## Epic

As John, I want to prove the obtaining of bachelor's degree in university\_B to apply for master's degree in university\_A.

### User stories

As John, I want to retrieve and present my diploma through e-services of universities to facilitate the process.

As John, I want to identify myself with my eID\_A to provide assurance of my identity.

As John, I want diploma to be matched with my identity\_A to prove obtaining of bachelor's degree.

As university\_A/B, I want to provide e-services for document/process management for optimizing workload.

As university\_A/B, I want to enable access to e-services with eID means supported by eIDAS node for reliable authentication of users.

As university\_A/B, I want to rest assured that identities of diploma holder and authenticated user are matching for avoidance of misuse/fraud.

### Use cases

UC#1 User authenticates with eID\_A to university\_B e-service.

- University\_B e-service authenticates user through eIDAS node and eID\_A provider and receives identity attributes for eID\_A.

UC#2 User submits request for collecting the bachelor's degree diploma.

UC#3 University\_B e-service interacts with IdM\_B for establishing the alumni identity.

- University\_B e-service delivers eID\_A attributes to IdM\_B.
- IdM\_B searches for existing matches between Id\_A and Id\_B.
- If not found, then IdM\_B searches from Country\_B registry match for Id\_A. Match between Id\_A and Id\_B is created in Country\_B registry and stored with Id\_A attributes. IdM\_A is notified about created match of identities and data is stored in Country\_A registry.
- If no match is found, then IdM\_B initiates remote video identification session and directs User to facial image capturing procedure.
- User presents facial image.
- IdM\_B system performs verification of captured facial image.
- IdM\_B engages human operator in necessity for clarification of additional information.

- IdM\_B creates new Id\_B in Country\_B registry. Match between Id\_A and Id\_B is created in Country\_B registry and stored with Id\_A attributes. IdM\_A is notified about created match of identities and data is stored in Country\_A registry.
- IdM\_B provides Id\_B attributes to University\_B e-service.

UC#4 University\_B e-service displays to user diploma evidence.

UC#5 User downloads the diploma evidence.

UC#6 User authenticates with eID\_A to university\_A e-service.

UC#7 User submits application for admission to master's programme.

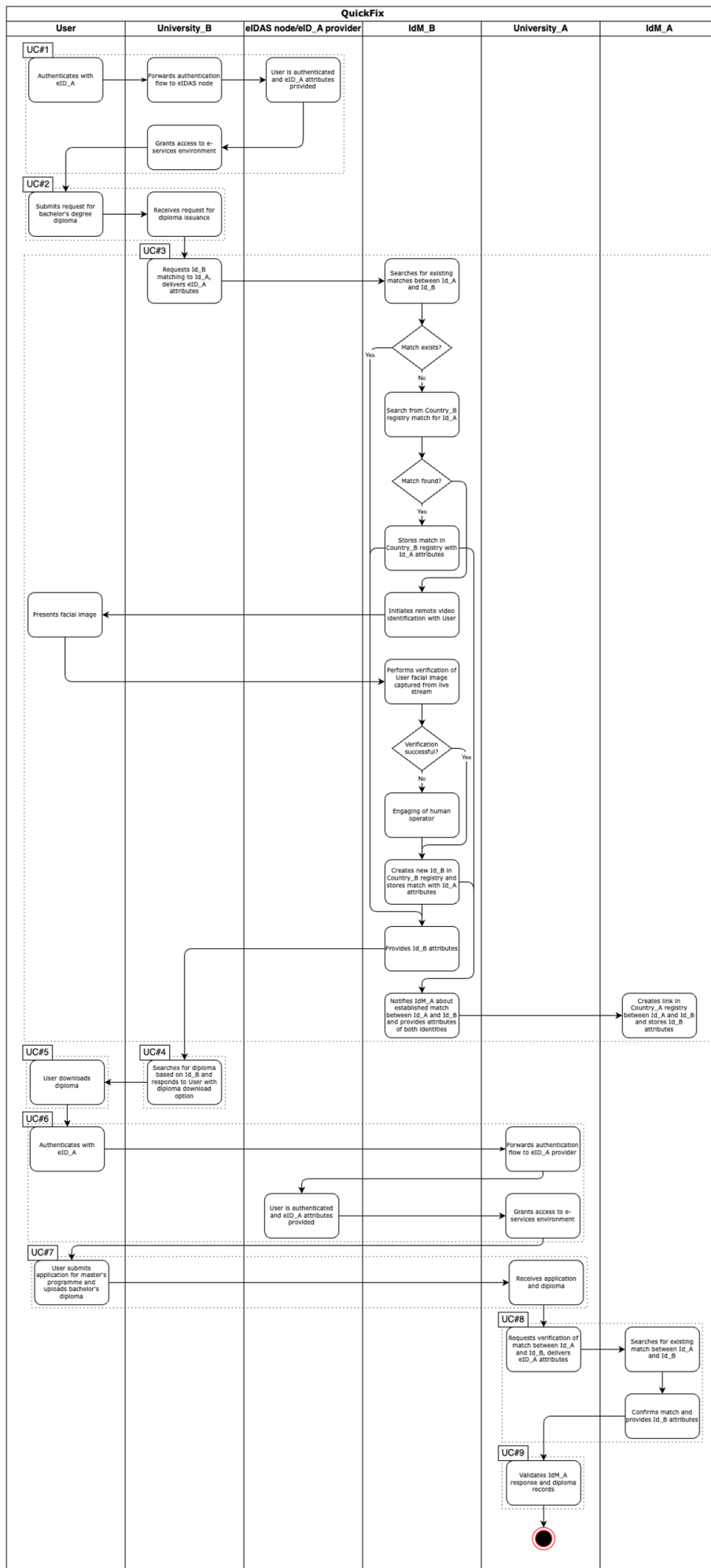
- User uploads the diploma as attachments to application.

UC#8 University\_A e-service interacts with IdM\_A for verifying match between Id\_A and Id\_B.

- University\_A e-service delivers eID\_A attributes to IdM\_A.
- IdM\_A searches for existing matches between Id\_A and Id\_B.
- Existing match is found due to IdM\_B having shared result of earlier matching process conducted with User's identities.
- IdM\_A confirms match of two identities and provides Id\_B attributes to University\_A e-service.

UC#9 University\_A e-service validates IdM\_A response and diploma records.

- Upon successful validation of IdM\_A response and diploma records, User's application is accepted.



**Figure 19** Quickfix detailed WORKFLOW

### 3.2.4 Hard\_EAA

Country of e-service provider concludes identity matching using eID mean from other country and data from local population registry. Output of identity matching process is delivered in format of electronic attestation of attributes (EAA), which includes link between personal identification numbers of two countries and other necessary PII. EAA is delivered to e-service that is being accessed by user. In addition, EAA is delivered to the user, so a person can use it as identity matching evidence during future interactions with e-services.

#### Personas

John

- is resident of country\_A,
- has eID\_A mean from country\_A,
- has been awarded bachelor's degree (diploma) at university\_B located in country\_B,
- wants to apply for master's degree at university\_A in country\_A,
- is eager to improve his educational qualification and is thereof very co-operative (has no problem with submitting PII beyond eID scheme content).

University\_A

- has e-service for submitting applications for admission to university,
- e-service users can authenticate with eID means supported by eIDAS node,
- must verify holding of bachelor's degree,
- must match identity of diploma holder with the identity of authenticated user,
- has capability to process EAAs.

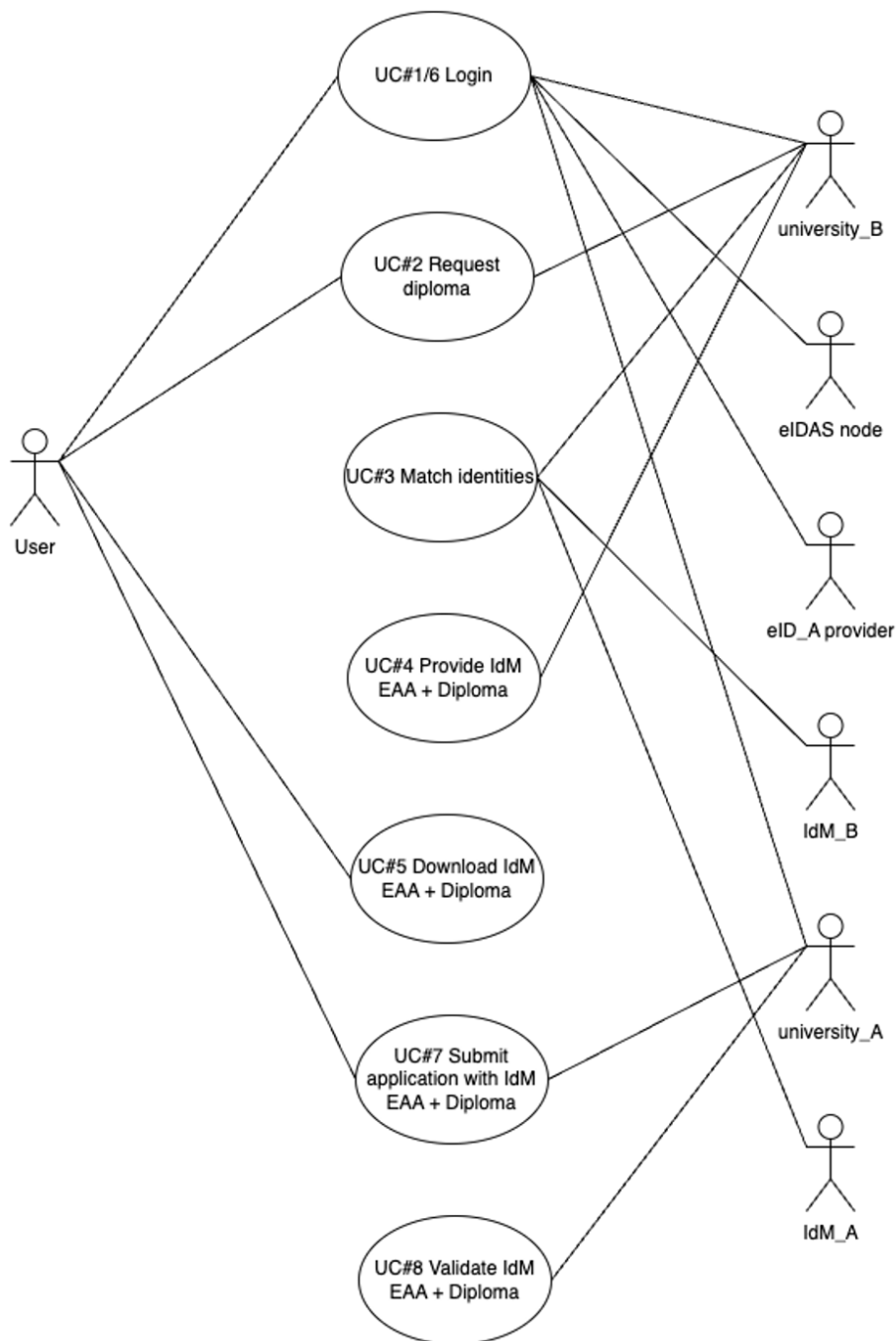
University\_B

- has e-service, which provides access to diploma records,
- e-service users can authenticate with eID means supported by eIDAS node,
- must match identity of diploma holder with the identity of authenticated user,
- has capability to process EAAs.

Country\_B IdM service provider (IdM\_B)

- has access to PII data of country\_B residents,

- has processes and logic in place for IdM,
- has access to data of matched identities, authority to create matches between identities and create new identity in country\_A,
- has data exchange with IdM\_B for sharing matching results involving identities of country\_A and country\_B,
- accepts and trusts matching results delivered by IdM\_B, which involve identities of country\_A and country\_B,
- issues matching results in format of EAAs.



**Figure 20** Use case for Hard\_EEA

## Epic

As John, I want to prove the obtaining of bachelor's degree in university\_B to apply for master's degree in university\_A.

### User stories

As John, I want to retrieve and present my diploma through e-services of universities to facilitate the process.

As John, I want to identify myself with my eID\_A to provide assurance of my identity.

As John, I want diploma to be matched with my identity\_A to prove obtaining of bachelor's degree.

As university\_A/B, I want to provide e-services for document/process management for optimizing workload.

As university\_A/B, I want to enable access to e-services with eID means supported by eIDAS node for reliable authentication of users.

As university\_A/B, I want to rest assured that identities of diploma holder and authenticated user are matching for avoidance of misuse/fraud.

### Use cases

UC#1 User authenticates with eID\_A to university\_B e-service.

- University\_B e-service authenticates user through eIDAS node and eID\_A provider and receives identity attributes for eID\_A.

UC#2 User submits request for collecting the bachelor's degree diploma.

UC#3 University\_B e-service interacts with IdM\_B for establishing the alumni identity.

- University\_B e-service delivers eID\_A attributes to IdM\_B.
- IdM\_B searches for existing matches between Id\_A and Id\_B.
- If not found, then IdM\_B searches from Country\_B registry match for Id\_A. Match between Id\_A and Id\_B is created in Country\_B registry and stored with Id\_A attributes. IdM\_A is notified about created match of identities in format of EAA and data is stored in Country\_A registry.
- If no match is found, then IdM\_B creates new Id\_B in Country\_B registry. Match between Id\_A and Id\_B is created in Country\_B registry and stored with Id\_A attributes. IdM\_A is notified about created match of identities in format of EAA and data is stored in Country\_A registry,
- IdM\_B confirms match of identities and provides Id\_B attributes to University\_A e-service in format of EAA.



UC#4 University\_B e-service displays to user identity matching EAA and diploma evidence.

UC#5 User downloads the identity matching EAA and diploma evidence.

UC#6 User authenticates with eID\_A to university\_A e-service.

UC#7 User submits application for admission to master's programme.

- User uploads the identity matching EAA and diploma as attachments to application.

UC#8 University\_A e-service validates provided identity matching to EAA and diploma.

- Upon successful validation of EAA and diploma records, User's application is accepted.

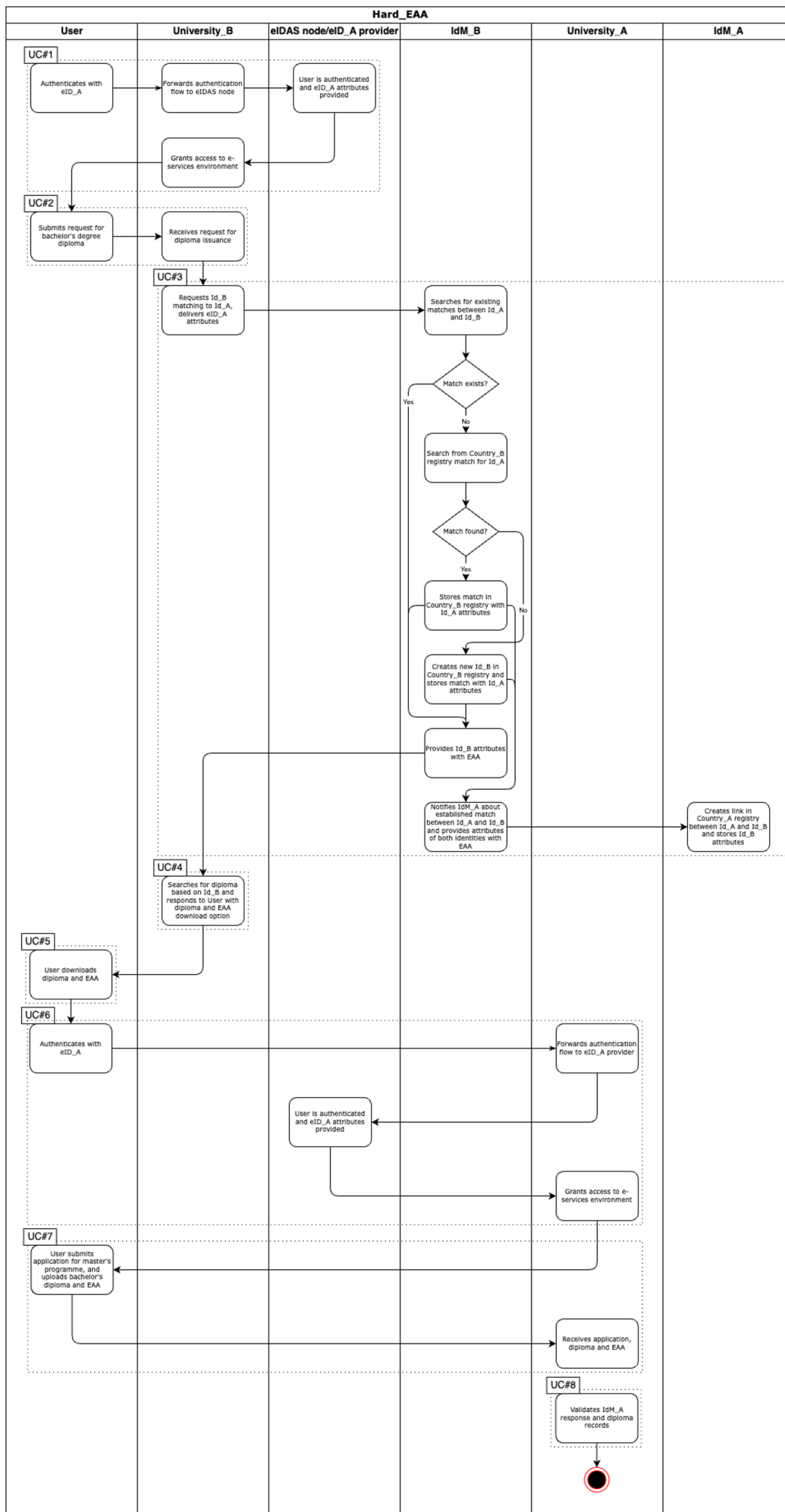


Figure 21 Hard\_EEA detailed WORKFLOW

### 3.3 Suggestions for Nordic-Baltic region

In general, our proposed solution consists of answers to two crucial questions:

1. How actually member state e-services would be able to smoothly start serving non-residents of a given member state regardless of the user being a returning user with changed residency or a new user?
2. How potential match between identities from different member states be made with the least amount of effort on the level of required assurance and following once only principle?

As we considered that member state services architecture will remain dependent on the local identity data structure for a while, then we deemed priority to implement "change on border" type of solution. This means everyone who enters e-service in a member state will be granted the ability to explain their identity in a format that is known in local ecosystems.

**For that to happen our suggestion is to change it through proxy like eIDAS Node that is described in detail in "eIDASNode+" scenario**, where we extend the existing framework to accommodate the multitude of identities. The implementation of identity matching solution must respect the fact that not all e-services require local identity. Named e-services should not be impacted by the change and must be able to operate with setup that corresponds to current eIDAS node and business logic.

**We still considered that direct connection to e-services should be regarded as well, and this can be done through EAA** (which is created through completing of "Hard\_EAA" or "Easy\_EAA" scenario) as part of authentication and authorization process.

Further, if a person has an EAA that connects different identities and that individual needs to prove some rights (eligibility) or needs to create connections to any dataset, then person will be enabled to present and prove that claim, even if through a manual process. With working eID and EAA all the evidence needed is immediately at persons disposal and ready to be presented for a decision.

Dependent of the agreed objectives, identity matching solution can be built up this way that "eIDASNode+" can be used as core solution or foundation for provisioning the service. There are several countries in Nordic-Baltic region, who either have deployed solution common to "eIDASNode+" or have made plans following mindset of "eIDASNode+". Other solutions can be incorporated into logic of "eIDASNode+" following the added value that they provide either by facilitating matching process (e.g., "Easy\_EAA" pairing of eID means, "QuickFix" digitizes process of new identity creation) or providing interoperable scheme in format of EAA ("Easy\_EAA", "Hard\_EAA") for distribution and further utilization of identity matching results.

Nevertheless, all 4 solutions do have properties that allow their deployment as standalone solutions.

To answer the second question, identity matching service availability together with ability to find existing and assign new member state specific identifiers is the cornerstone of the proposal. It must be noted, to fulfil targets of SDGR ability to assign new member state identifiers through digital process is of same importance as having capability to match identities of different members states.

In most countries such a service exists but is often not available remotely. **Our QuickFix scenario improves the availability of receiving member state specific identity attributes and produces. Also, the Easy\_EAA is easy to implement alongside any existing identity matching allowing most of the work to happen as self-service.** The Hard\_EAA model builds on the fact that e-Service user is known to have a high level of assurance for one member state and the next member state can rely on the first, therefore. That again improves the availability of identity matching services.

There is substantial potential for efficiency in sharing the matching service results to the member state from where the matched identity is from. Matching made in one country should not be contested by another country and both countries could use the match for translating identity in their member state services. EAA format allows data to be shared and checked for validity in quite a general sense whereby the integrity and authenticity of data is well protected. Solution for exchange and recognition of EAAs between registries of member states is subject for further design and agreement.

Common rules of making the match could also mean that matching will have its own "level of assurance" to indicate what process and data was used to match the identities. The highest level of assurance should mean that the matching could be trusted to hold true in any transaction regardless of the context. Lower levels could be appointed if the assurance holds true only in clearly one sector specific context (healthcare, construction, taxation, etc.) or where there was a need to make the match with clear lack of data and associated risks allowed still to pursue.

While dealing with data exchange between member states and ensuring the trustworthy results of matching process, the necessity for data sharing between member states' registries during identity matching process must be noted. During interviews with Nordic and Baltic countries the need to extend scope of attributes available for identity matching process was expressed multiple times. Not limiting to but attributes like 'nationality' and 'place of birth' have been regarded as records what would facilitate matching process and provide required trustworthiness. Although eIDAS node has several attributes (incl. 'place of birth') that may be distributed, then due to their optional nature these attributes are mostly not available to relying parties. Accordingly, such additional attributes could be shared

through data exchange of registries in countries whose identities are involved in a particular matching process.

## Actionplan to implement suggestions

The following must be done, to implement proposed solutions:

- Define EAA standard to use and specify content (e.g. OpenID Connect for Verifiable Credentials (OIDC-VC) for electronic usage, but we do recommend PDF to support F2F interactions as well). Although the content of the attestation is not too complex, issues like data minimization and privacy preservation may lead to some difficulties. Standards that exist allow interpretations that do not guarantee interoperability on attribute level, so specific implementation must be agreed. Also, we note that the agreement must be ready to be changed as the maturity of eIDAS defined attribute attestation service evolves in coming years.
- Create common extension or use existing one to allow eIDAS Node to replace incoming identity with local one before reaching e-Service provider. Organizationally the identity matching data and the service that translates the foreign eID's into locally acceptable ones, does not need to be bundled with eIDAS Node hosting, but that might ease the implementation. It is important that the service is usable by eIDAS Node and that is supported in the product lifecycle as an extension. This may need cooperation agreement with European Commission that is responsible for the building blocks development.
- Review national legislations for processing of personal data in terms, that would support deployment of once only principle and in justified use cases facilitate identity management processes in a user controlled manner. Initiate legal changes necessary for introduction of proposed procedural and technical activities.
- Agree on NBCM level that electronic identification of one's resident on "high" level of assurance must be accepted as proof of identity on the same level as using physical identity documents from that country and to identify physical person, countries grant to each other similar rights and obligations what are contextually needed.
- Formalize sharing of the matched identity data between countries. Establish framework defining principles for identity matching process and acceptance of matched identities in Nordic-Baltic region. It should give requirements for:
  1. Accepted sources for identity attributes (e.g., eID means, identity documents, cross-border data exchanges between registries),
  2. Handling identity attributes (e.g., minimum data set, encoding of characters),

3. Defining the level of assurance for results of identity matching process dependent of identity attributes' sources and procedures in involved case,
4. Data governance rules, protection, and mechanisms for supervision for data handling (e.g., notification to matched identity about established cross-border connection with other identity, enable users to view events accessing their data).

Harmonized and enforced requirements allow participants of framework to trust each other's matching results and enhance identity management in region through cost-effective approach.

- Enable data exchange of attributes between countries, deemed necessary for identity matching process.
- Address the issue of derived personal identification number usage as value for person's unique identifier delivered by eID schema in a cross-border context. Following EC published information there are several countries in Nordic-Baltic region, who implement such practice. Handling of derived personal identification numbers adds remarkable complexity layer to identity matching process and to usage of matching results, if created evidence does not contain personal identification number values that are operated domestically or communicated to other countries (i.e., receiving country specific derivation).
- Amend domestic legislation and processes so that creation of identities through digital process would be allowed. Currently persons accessing cross-border e-services without having an e-service provider's domestic country's personal identification number are queued in virtual "waiting rooms". Passage through a virtual waiting room is granted only after completion of specific physical activities in receiving country. Digital transformation of physical procedures meets the aim of SDG regulation. Dependent of country specifics, the identities created through digital processes could have dedicated level of assurance or status in country's identity management system.

### **What will the future safety concerns be for identity matching?**

Identity matching, if done incorrectly, may leak data of a person and create constant backdoor to their records. If matching is done in a very privacy preserving, non-linkable, non-traceable manner then catching the fact that something has at all happened may be hard, but also investigation on the topic would be hard.

Identity matching not done where needed leaves people without access to their records, for which they have legitimate rights to. This may hinder a person's most basic functions such as health, ability to earn income or have access to their loved ones.

## What will the future need for identity matching be and are the suggested solutions scalable?

EUDIW is identity matching machine – withing single EUDIW person is meant to generate as many pseudonyms as they wish, and service providers must accept these if law is not directly forcing people to reveal their actual personal data. Our solution does introduce EAA concept that is external proof of identities that can be matched, however given the nature of eIDAS and EUDIW ARF we do see that we are bound to have much more orphaned accounts to which the original owner will be unable to get access to even if they want to.

## Suggestions on how quality of data across countries can be improved

Only used data is accurate and it is accurate because something depends on it. Therefore, link the data and use the linked data and show that to data subjects and make their life depend on it. We also believe that sharing the data about matches created will improve data quality and allow quicker error spotting.

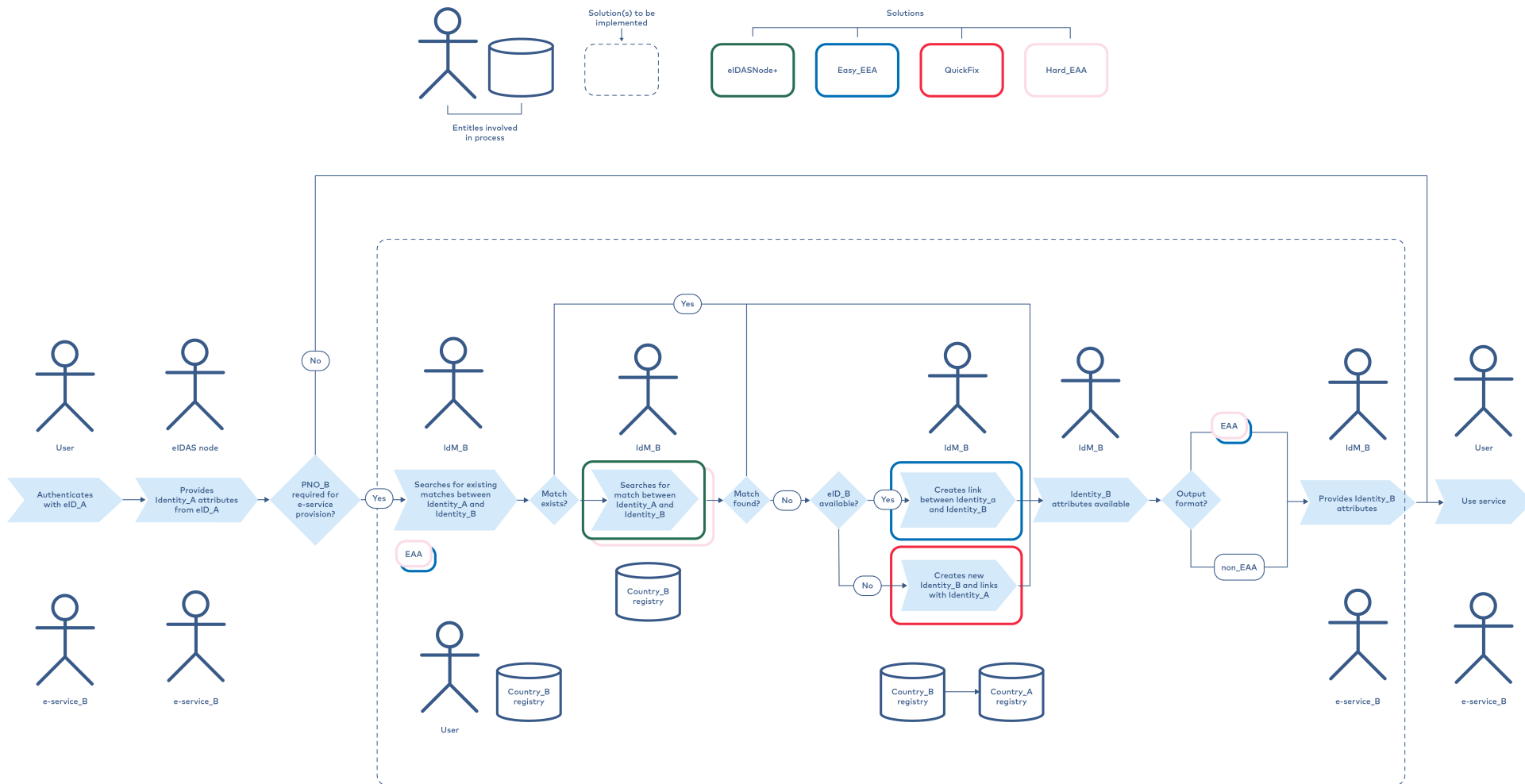
## eIDAS revision implications

At the point of report writing eIDAS revision still has not finished. However, the discussions and released versions of the text bring in several changes relevant to this report and we would like briefly to touch on the following:

- **Electronic Attestation of Attributes.** Electronic Attestation of Attributes is seen as Trust Service in regulation, and it will create greater clarity on organizational and technical requirements for such services and attestations themselves. However, nothing prohibits Nordic and Baltic countries to use such methods already now. In principle this is document with e-seal confirming that identity data set of one member state belongs to the same person as identity data set from another member state. These e-seals must be trusted by the NBCM community. As there is e-seal issuance and handling in current regulation then agreement can be made based on this. It is important to note that lifecycle management of such attestations must be well thought through. Although it is assumed that identity matching is done once and the link between identities is persistent forever, then as the process is open to errors of different kinds, the need to revoke this link must be foreseen. Attestation is a digital document and is living independently of its issuer. The other attestation related concern might be data privacy. Attestation should include only a minimal set of user data, but enough that it is unique to the member state it originates from. Additionally, it is possible to create attestations that would only be usable to validate the claim of identity matching and that cannot be used to derive the identities it connects. We do see that such discussions must take place before launching the system, but there are solutions that allow to implement a politically agreed solution.

- **eID scheme notification obligation.** eIDAS' new version foresees that all member state will have to notify an identity scheme and at least one such scheme should be on the level of assurance high. Although this statement may change but it at least now gives hope that there is a way to authenticate from every member state using the highest level of assurance through eIDAS node infrastructure. There is no statement however how many citizens of any country such scheme should cover, but in our proposals, we can assume that for willing participant such mechanism is available, and it is not discriminatory to request using such scheme to interact with identity matching service.
- **Introduction of EU Identity Wallet.** The introduction of the EU Identity Wallet (EUDIW) will change the landscape of e-services in coming years and may well compete for attention and budget for most other issues either this report or any other may address. Therefore, alignment of this change has been a burning issue for the research. Introduction of EUDIW as mandatory tool for authentication for public and private sector services creates incentives to leave central identity brokers such as eIDAS Nodes infrastructure. We have therefore envisaged the EAA model alongside the eIDAS Node extension. We see that the proposal allows smooth transition from one model to another. However, we do see that the shift that is planned creates an environment without identity data that could be matched, rather a lot of pseudonyms and only claims about attributes existence. That leaves the active and cooperative participant sometimes without proper support - because data is not available to help then but even more it hides the traces of these who did not want to be matched in the first place. It leaves no room for state-to-state cooperation. So based on that we also feel that our focus on the scenario of helping a person who seeks help and is supportive on the identity matching is best suited.





**Figure 22** General overview of the proposed solution

## 3.4 Suggestions for Member States

We will now bring out country specific recommendations, that will ensure smooth implementation of our suggested solutions. General recommendations made by consultants have taken into account all the input gathered from every Nordic-Baltic country. Still, by mutual agreement, this report does not include recommendations concerning the identity matching solutions in Sweden, as their applicability would need a broader legal analysis, which was not within the scope of this study.

### Denmark

Suggested solution: eIDASNode+

Reasoning: Denmark has identity matching solution in place, which aligns with eIDASNode+ principles. After piloting with manual process, Denmark has deployed automated process from October 2023.

Challenges/changes:

- Creation of new Danish identities during digital process of identity matching is not supported and requires longer term principal preparations in legal and organizational aspects. Currently creation of new identities requires physical presence in Denmark. In addition, feasibility of this change is questioned, because in practice persons requiring Danish personal identification number (CPR) are usually already residing in Denmark.
- Easy\_EAA could be complimenting eIDASNode+, as in use cases of migration persons can have eID means of two countries at their hand.
- Retrieval of additional attributes besides eID 4 mandatory ones deemed to be necessary.

### Faroe Islands

Suggested solution: eIDASNode+

Reasoning: Feasible approach from process and technical point of view.

Challenges/changes:

- No EU notified eID scheme and has not integrated with eIDAS node yet.
- Creation of new identity requires change in identity management ecosystem.
- Retrieval of additional attributes besides eID 4 mandatory ones deemed to be necessary.

## Greenland

Suggested solution: eIDASNode+

Reasoning: Greenland has identity management setup following Denmark's approach and is relying on Danish system.

Challenges/changes:

- Return on investment will have a very poor score due to the very limited number of transactions that might require identity matching.

## Estonia

Suggested solution: eIDASNode+

Reasoning: Estonia is currently designing identity matching system, that aligns with eIDASNode+. Extending the solution with EAAs (Hard\_EAA) is favorable. In addition, QuickFix could be deployed for subprocesses, where new identity is created.

Challenges/changes:

- Adjusting legal framework.
- Integration works of API between identity matching solution and e-services.
- Handling of identity matching results with lower level than 'High' in terms of LoA.

## Finland

Suggested solution: eIDASNode+

Reasoning: Finland internal proposals for identity matching system are targeting same kind of solution.

Challenges/changes:

- Retrieval of additional attributes (e.g., citizenship, ID-document number) besides eID 4 mandatory ones deemed to be necessary.
- Changes in legislation and development of systems is necessary. In addition, topics needs prioritization for resources to be allocated.
- Handling of derived personal identity numbers increases identity matching complexity.

## Latvia

Suggested solution: eIDASNode+

Reasoning: Technologically most suitable for deployment.

Challenges/changes:

- Retrieval of additional attributes (e.g., citizenship, ID-document number) besides eID 4 mandatory ones deemed to be necessary.
- Creation of new identity during identity matching process requires legislative changes.
- Conclude data exchange agreements with most countries' population registries.

## Lithuania

Suggested solution: eIDASNode+

Reasoning: Follows best established Lithuanian identity matching solution.

Challenges/changes:

- Accepting the identity matching results of other countries requires legislative and technological amendments.
- Levels of assurance for identity matching results require further analysis.
- e-services require significant time for adjustment to changes.

## Norway

Suggested solution: eIDASNode+

Reasoning: Norway's current outlook with identity matching solution aligns with principles of eIDASNode+.

Challenges/changes:

- Creation of identities for persons not residing in Norway requires changes in population registry.
- Appointing the owner of identity matching solution.

## Iceland

Suggested solution: eIDASNode+

Reasoning: Technologically most suitable for deployment.

Challenges/changes:

- Legislation changes required.
- Creation of new identities during the identity matching process.
- e-services must adapt their business logic if matching results will have several levels of assurance, that do not align with currently established levels.

# Summary

EU has initiated several initiatives to support services both in public and private sector to be available cross border and in personalized manner where that is preferred or necessary. However, as eIDAS implementation report<sup>[107]</sup> showed, the actual usage of cross-border services is low, and the availability is not reachable for most of the EU residents. Moreover, **there are currently no cross-border processes at EU level to avoid the situation where one person owns multiple eIDs issued or assure that a person is successfully matched to correct eID under different notified eID schemes.** This can lead to denial of access to services in cases where the receiving Member State cannot exclude duplication or match multiple legitimate eIDs from different eID schemes.

Nordic and Baltic countries differ heavily from most of the EU by having strong public sector data registries that are used to provide a rich selection of services for their residents. This region has so far had also a common approach in most countries that an individual is recognized in different datasets through commonly agreed unique identifiers or data sets. But even in the Nordic-Baltic region, there are still differences and deviations regarding identity and record matching.

**The aim of this analysis** was to conduct region-wide recommendations that would help person to interact in meaningful manner with all the Member States in the region, but also produce Member State (MS) specific policy suggestions to pave the way for that vision to be implemented in specific Member State regarding identity and record matching.

To develop possible solutions and formulate recommendations, a current situation analysis (AS-IS) was first conducted, consisting of four main parts:

- Analysis of the main EU-level requirements and their relevance to identity and record matching.
- Assessment of the existing processes and solutions for identity and record matching within the EU/EEA region
- Mapping of the data requirements necessary for identity and record matching across three service areas (banking, health, academia) within the Nordic-Baltic countries.
- Overview of structural challenges encountered by the Nordic-Baltic countries regarding identity and record matching.

---

107. <https://www.enisa.europa.eu/publications/eidas-overview-on-the-implementation-and-uptake-of-trust-services>

**The analysis of EU-level requirements** concluded that Nordic-Baltic countries are following the same principles in terms of how data about country's population is maintained. All Nordic-Baltic countries have implemented centralized digital solution for population registry, which assures common practice of population management, reliability of data and high system availability.

**The analysis of best practices for identity and record matching in EU/EEA** countries concluded that different strategies are used by countries, like:

- One central database of all identities (including a small amount of available information about foreign identities connected to the local ones).
- Video identification.
- Central passports register stores photo and fingerprints, which can be checked, to make sure that no duplicate identities are created.
- Manual supervision over connecting duplicated identities (same person with more than one match from the database).
- Name details are coded to match language specific changes in the surname.
- Infinite shelf life of ID number (= identity) with added status (like "living" or "deceased").
- Using digital signature together with ID number for making any commitments.

**The analysis of data requirements in three different sectors** (banking, health, and academia) concluded that one can see remarkable challenges to be tackled if cross-sectoral data availability and data machine-readability would be targeted. For example:

- Implemented systems do vary from country-to-country dependent on availability of resources and/or volumes of cases. In addition, within the country implementations in sub-domains of specific domain may have significant discrepancies.
- Rules for identifying persons can be missing although the domain is regulated on EU-level, and matching identity with record is crucial.
- Domain specific data is not deployable for cross-sectorial usage, as it is commonly prohibited due to data protection constraints, data can be non-disclosable for reason of being a business/bank secret.

**The analysis of structural challenges in Nordic-Baltic region** revealed five main problems with the most significant impact that need to be addressed collaboratively:

- Recurring work is done for identity verification and matching if person's activities engage different domains as identity matching results are not shared within the state. Moreover, the identity matching results are not shared between the states.
- There are differences in PII (Personal Identifiable Information) datasets operated by states due to their legal and cultural particularities (e.g., place of birth logic, contact address obligation, facial biometric data storage/usage, derived PNOs towards other states, pseudonyms).
- Risks associated with potential identity mismatch and the economic benefits of enhanced/automated processes are small/minimal. Thus, motivation for changing the status quo is low.
- Low capability of Population Registries to adapt to any changes in PII dataset or modifications/improvements in processes of PII handling.
- Identity verification and matching is manual work performed by personnel who are not trained/experts in ID-management (healthcare, educational personnel, etc.).

These five main challenges served as the basis for developing the TO-BE solutions and recommendations. 10 potential solutions were identified and four of them proved higher potential:

1. **eIDASNode+**, where for every foreign identity a local personal identification number will be assigned. After authentication with eID mean through eIDAS node, e-services approach local identity matching service for retrieval of local personal identification number of user. E-services continue operating with local personal identification number.
2. **Easy\_EAA**, which allows "pairing" of eID means of two countries. Country of e-service provider concludes identity matching using eID means at person's hand. Identity matching service establishes a link between two identities based on attributes received from eID means of both countries. Ground for match bases on uninterrupted process performed by authoritative party during which authentication with both eID means is performed, thus identities of two countries can be linked. Output of identity matching process is delivered in format of electronic attestation of attributes (EAA), which includes link between personal identification numbers of two countries and other necessary PII. EAA is delivered to e-service that is being accessed by user. In addition, EAA is delivered to the user, so a person can use it as identity matching evidence during future interactions with e-services.



3. QuickFix, where converting personal identification number's physical issuance process into digital remote video identity verification process and integrate this process into current business flow of e-services' usage. Proposed digital identity creation (personal identification number issuance) is based on combination of eID authentication and capture of biometric identifier (facial image). Processing facial images depends on country's practices. The process ends with establishing connection between two countries' personal identification numbers in local population registry.
4. Hard\_EAA, where a country of e-service provider concludes identity matching using eID mean from other country and data from local population registry. Output of identity matching process is delivered in format of electronic attestation of attributes (EAA), which includes link between personal identification numbers of two countries and other necessary PII. EAA is delivered to e-service that is being accessed by user. In addition, EAA is delivered to the user, so a person can use it as identity matching evidence during future interactions with e-services.

In conclusion, eIDASNode+ should be implemented in all Nordic-Baltic countries, as a common approach, adding the other three described possibilities to that, depending on country specific needs.

# 4. Appendixes


## 4.1 Terms and abbreviations

TERM	ABBREVIATION	EXPLANATION
<b>The citizen service number</b>	BSN	The citizen service number (BSN) is used once only in the registration process, to generate a unique number.
<b>A certificate authority</b>	CA	Trusted entity that issues digital certificates to authenticate content sent from web servers
<b>Citizen Service Number</b>	CSN	The Citizen Service Number (CSN) is a unique identification number assigned to residents of the Netherlands for the purpose of accessing government services and benefits. The CSN is issued by the Dutch government and is similar in function to a social security number or national identification number in other countries.
<b>Country of Treatment</b>		Country where the patient receives treatment.
<b>Danish CPR number</b>	CPR	The CPR number is unique to the person and is used in Denmark as an ID number.
<b>Data sharing "on paper"</b>	-	means that at least once in the process some data are shared in any other form than digitally, e.g., verbally, printed, e-mail etc. (digital data sharing is in a machine-readable way).
<b>Digitize</b>	-	Transforming analogue information to digital form.
<b>Digitalize</b>	-	Transforming processes to digital form.
<b>Digital Service Infrastructure</b>	DSI	Digital Service Infrastructure is an Application Component enabling networked services to be delivered electronically, typically over the internet, providing trans-European interoperable services of common interest for citizens, businesses and/or public authorities, and which are composed of core service platforms and generic service
<b>eID infrastructure</b>	-	An eID infrastructure is a technical framework that enables electronic identification (eID) systems to operate securely and efficiently. An eID infrastructure typically includes a set of hardware and software components, as well as standards and protocols for interoperability, security, and privacy.

<b>eIDAS minimum data set</b>	PID	The eIDAS minimum data set (MDS) or Personal Identity Data (PID) is a standardized set of personal data attributes that are required to be included in electronic identification (eID) documents issued by member states of the European Union (EU) in compliance with the eIDAS regulation. The purpose of the MDS is to ensure that eIDs issued by different member states are interoperable and can be used to authenticate users across borders. The eIDAS MDS includes essential information about the individual or entity using the eID, such as their name, date of birth, and a unique identifier.
<b>eIDAS network</b>	-	The eIDAS network is a technical infrastructure that enables electronic identification (eID) and trust services to be provided across the European Union (EU) in compliance with the eIDAS regulation. The eIDAS network consists of a set of interconnected national eID systems and trust service providers (TSPs) that provide secure and reliable cross-border eID and trust services.
<b>eIDAS node</b>	-	An eIDAS node is a software component that provides a secure and standardized interface for communication between electronic identification (eID) systems and other trust services across different member states. eIDAS nodes are used to facilitate cross-border transactions, allowing individuals and businesses to use their electronic identities to access online services in other EU countries.
<b>eIDAS SAML Attribute Profile</b>	-	eIDAS SAML Attribute Profile is a specification that frames how identity transaction (the assertion) shall be managed between the member states (eIDAS nodes) – thus, it leaves it open to each country to decide how eID and node shall communicate.
<b>eIDAS scheme</b>	-	An eIDAS scheme is a framework for electronic identification (eID) and authentication that complies with the requirements of the eIDAS regulation.
<b>eIDAS Unique Identifier</b>	eUID	(eUID) is a unique identifier assigned to each electronic identification (eID) issued by a member state of the European Union (EU) in compliance with the eIDAS regulation. The eUID is a critical component of the eIDAS framework, as it allows different eID systems to identify and authenticate users across different member states.
<b>EUDI-Wallet</b>	-	EUDI wallets provide users with a secure interface to interact with their devices, allowing them to store money or other data. These wallets can also be used as a payment platform by supporting online access from different merchants and transferring funds from one device to another.

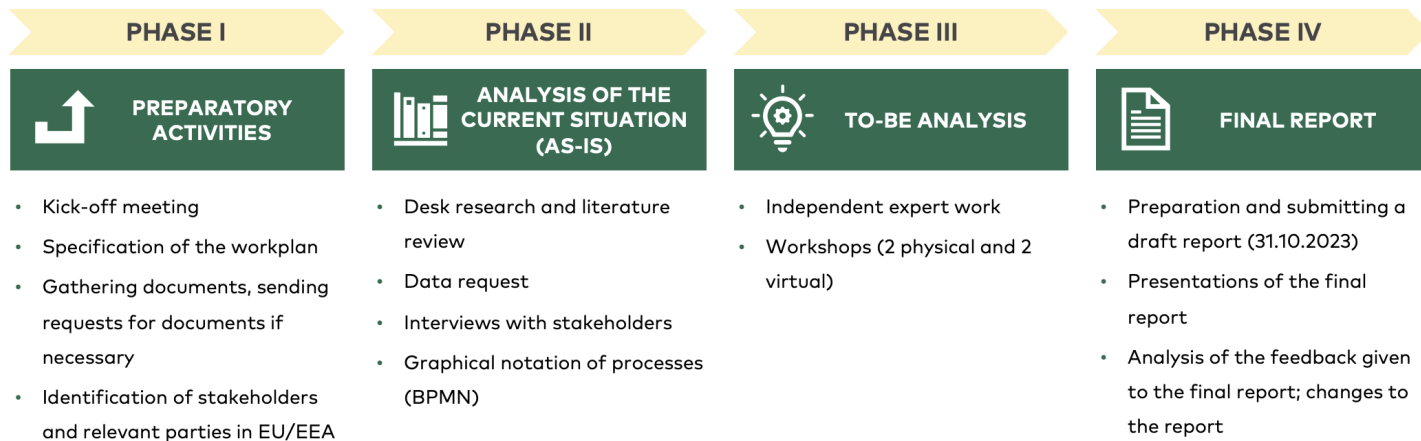
<b>Evidence provider</b>	EP	A system, service, or component that supplies evidence or proof of a particular event, transaction, or action. This evidence is often used to verify and validate specific activities, such as user actions, system events, or data transactions.
<b>General Data Protection Regulation</b>	GDPR	The General Data Protection Regulation is a Regulation in EU law on data protection and privacy in the EU and the European Economic Area. The GDPR is an important component of EU privacy law and of human rights law, in particular Article 8 of the Charter of Fundamental Rights of the European Union.
<b>Health Care Provider Organization</b>	HCPO	An individual health professional or a health facility organization licensed to provide health care diagnosis and treatment services including medication, surgery, and medical devices.
<b>Health professional</b>	HP	A health professional, healthcare professional, or healthcare worker is a provider of health care treatment and advice based on formal training and experience.
<b>Identity Matching</b>	-	In this context, identity matching is to be understood as the process when the identity of a person, when using a digital service abroad, is verified through previously registered data in that country.
<b>Internal Market Information System</b>	IMI	The Internal Market Information System (IMI) is a secure, multilingual online tool that facilitates the Exchange of information between public authorities involved in the practical implementation of EU law.
<b>Level of Assurance</b>	LoA	In the European Union, the eIDAS definition of LoA is used as a criterion to evaluate the strength of authentication methods used to verify a user's digital identity. eIDAS definition outlines three levels of identity assurance: Low, Substantial, and High.
<b>The eIDAS minimum data set</b>	MDS	Set of attributes that every country must supply for authenticated users and legal entities. Each country must provide a unique identifier per eID that represents a natural person.
<b>Member State</b>	MS	A member state is a state that is a member of an international organization or of a federation or confederation. In this analysis, Member State is a country or overseas territory within Nordic-Baltic region.
<b>Electronic Migration Services</b>	MIGRIS	MIGRIS is managed by Migration Department under the Ministry of the Interior of the Republic of Lithuania.
<b>National Contact Points</b>	NCP	European networks enabling healthcare providers to mutually exchange medical details. This exchange takes place through a secure connection.

<b>NOBID group</b>		Nordic-Baltic eID (NOBID) is a project that is focused on enabling the use of national eID solutions across the Nordic and Baltic regions. The NOBID Group is made up of appointed representatives of the eIDAS implementation in the participating countries.
<b>Nordic Council of Ministers for Digitalization</b>	MR-DIGITAL	The Nordic Council of Ministers for Digitalization (MR-DIGITAL) consists of ministers and representatives from the Nordic and Baltic countries and works to promote digitalization in and between the countries in the region.
<b>Nordic Council of Ministers</b>	NCM	The Nordic Council of Ministers is the official body for inter-governmental co-operation in the Nordic Region. It seeks Nordic solutions wherever and whenever the countries can achieve more together than by working on their own.
<b>Once-only principle</b>	OOP	The once-only principle is an e-government concept that aims to ensure that citizens, institutions, and companies only must provide certain standard information to the authorities and administrations once.
<b>Once-Only Technical System</b>	OOTS	OOTS enables the sharing of information between public administrations across borders between EU countries. It is cross-sectorial and can be expanded beyond the current scope of life events set out in the Single Digital Gateway Regulation. It puts into practice the Once-Only Principle, which states that citizens should not be forced to provide information to authorities if another authority already holds that information in electronic format.
<b>Physical process</b>	-	in this report is referred as the one which requires physical presence/contact of parties in any point of the process
<b>Personal Identification Code</b>	PIC	A unique code assigned to an individual, often used for identification and official purposes.
<b>Process Happy Path</b>	-	is an ideal and less complicated version of the process, where no interruptions or (almost none) terminations occur.
<b>Public Relying Party</b>	Public RP	is a third-party entity that relies on an electronic identification (eID) system or trust service provider (TSP) to authenticate and verify the identity of its users. In the context of the eIDAS regulation, a Public RP is typically a service provider that offers online services to citizens or businesses, such as financial institutions, e-commerce websites, or government agencies.
<b>Record matches</b>	-	Record matches refer to the process of identifying and validating a user's identity or access privileges based on information stored in a database or system. When a user attempts to access certain resources or perform specific actions, their provided credentials or attributes are compared with the records in the authorization database to determine if they are allowed to proceed.

<b>Returning user</b>	-	An individual who has previously visited and interacted with a particular website, application, or system and is accessing it again for subsequent use.
<b>Security Assertion Markup Language</b>	SAML	In the eIDAS context, SAML is a critical protocol used for exchanging authentication and authorization data between different identity providers (IdPs) and service providers (SPs).
<b>The Single Digital Gateway Regulation</b>	SDGR	SDGR is a European Union regulation aimed at improving the access of citizens and businesses to information, procedures, and assistance services in the EU's Single Market. The regulation was officially adopted by the European Parliament and the Council on November 20, 2018, and it came into force on December 11, 2018.
<b>System Landscape Directory</b>	SLD	is the central source of information on systems in relevant IT landscape.
<b>State Information Resource Interoperability Platform</b>	SIRIP	SIRIP is the Lithuanian interoperability platform that offers an easy way for public authorities to design, deliver and manage e-services. Many e-services can be streamlined and made available in a user friendly one-stop-shop portal to citizens, business entities and civil servants.
	Icon	This icon is used to highlight information in the content
<b>Tax Identification Number</b>	TIN	A Tax Identification Number is a unique identification number used by tax authorities to track and identify individuals and entities for tax purposes. It is also known as a Tax ID or Taxpayer Identification Number, depending on the country.
<b>Two factor authentication</b>	2FA	Two-factor authentication is a security process that requires users to provide two different forms of identification before gaining access to an account, system, or service. It adds an extra layer of security beyond just a username and password, making it more challenging for unauthorized individuals to access sensitive information.

## 4.2 Methodological approach

According to the aims of the study, the analysis was conducted in 4 phases (see Figure 23).



**Figure 23** Methodological approach

The objective of the **first phase** was to align the Tenderer's and the Client's visions regarding the project's goals and methodology. During the preparatory activities, the alignment of expectations and understandings between the Client and the Tenderer project teams took place at the kick-off meeting, along with the development of a detailed project action plan. The project objectives were also presented to the NOBID group.

In the **second phase** of the analysis, data collection was conducted, and the current situation was mapped (see also Ch 4.5 "Aspects analyzed per country").

- The scope of **document analysis** included several previous studies as well as relevant materials available from public sources (such as documents describing the eID status of member states). The focus of the document analysis was to understand the state of play of processes and solutions for identity and record matching in the EU/EEA.

- The purpose of the **data inquiries** was to ascertain the current state of identity matching in the EU/EEA. Additionally, it aimed to determine whether the solutions being used could be applicable in the Nordic-Baltic region. To achieve this, letters were sent to all EU/EEA countries, requesting information about their current solutions and future plans regarding identity matching. From the countries that responded, those with initial descriptions that appeared promising in the context of the Nordic-Baltic region were selected, and **interviews** were conducted with them to gather further information. For three countries not interviewed (PL, DE, MT), summary information is provided based on a data request for broader perspective.
- Based on the interviews, descriptions of the best practices used in the field were compiled. Additionally, **process descriptions and diagrams** were created based on the input gathered from the interviews. The Bizagi Process Drawer was utilized to generate visual representations of the processes. In addition to one generalized identity and record matching process to describe its three phases, separate sub-process descriptions were prepared.
- As part of the current situation analysis, **interviews** were conducted with representatives from all Nordic-Baltic countries (10) to gain insights into the solutions currently being used, challenges faced, and future perspectives. The input gathered from these interviews was primarily utilized to describe an overview of the structural issues in the Nordic-Baltic region. See the overview of all analysed aspects per country in chapter 4.5.

**It is crucial to emphasize that despite the phase's title suggesting a focus solely on the current situation, this phase encompassed a wealth of valuable input for TO-BE analysis.** This includes gathering best practices from EU/EEA countries, considering stakeholders' expectations, and identifying and addressing structural challenges that necessitate specific country-based recommendations. The comprehensive nature of this phase ensured that the ensuing analysis will be well-informed and encompass a broader perspective of the topic.

In the **third phase** of the analysis, the information collected in the previous phase was validated, descriptions of identity matching solutions were prepared, and recommendations were developed for both the Nordic-Baltic region and on a country-specific basis.

- For validating the information collected and the issues identified in the second phase of the analysis, a **physical workshop** was organized with representatives from the interviewed countries (a total of 21 participants from 7 different Nordic-Baltic countries). During the workshop, the participants were presented with the results of the AS-IS analysis and 10 initial identity matching solutions, which were developed because of **individual expert work**. To gather feedback on the initial solutions, workshop participants were asked to vote for each solution using a 5-point rating system.



- Considering the feedback from the physical workshop, the project team, because of individual expert work, selected four out of the initial ten solutions. The chosen solutions chosen by the expert team also had the highest scores based on the **feedback collected** during the physical workshop. To gather feedback and confirm the most promising solutions for further in-depth analysis, a **virtual workshop** was conducted (with a total of 25 participants from 9 different countries). The input gathered during the workshop was also used to develop Nordic-Baltic region-wide recommendations.
- To develop country-specific recommendations and to gain a better understanding of the situation in each member state, **separate interviews** were conducted with representatives from **all member states**. During the interviews, the four most promising solutions were presented, and feedback was collected regarding the feasibility of implementing these solutions on a country-by-country basis.
- During the third phase of the analysis, the information collected was used as a basis for providing more **detailed descriptions of the identity matching solutions**. As a result of independent expert work, comprehensive descriptions of the most promising solutions were prepared. Additionally, **recommendations were developed for the use of the described solutions**, both at the Nordic-Baltic regional level and separately for individual member states. The descriptions of the solutions and the developed recommendations were structured in the "TO-BE" chapter (Ch 3) of the final report.

In the fourth phase of the analysis, the **final report** was compiled, and **feedback** was collected on it. Additionally, the **results of the analysis were presented** at a physical CBDS seminar.

## METHODOLOGICAL PRINCIPLES



**Figure 24** Logical flow of information

To ensure the high quality of the research results, **the principles of logical flow and triangulation**<sup>[108]</sup> have been followed when conducting the research and creating conclusions and recommendations.

The principle of logical flow ensures that the research report is logically structured and does not contain irrelevant information. Each conclusion must be based on the analysis, and each recommendation must address at least one conclusion (see Figure 24. Logical flow).

### 4.3 Sources

1. *Article 12B (2014) Art. 12b Regulation (EU) No 833/2014*. Available at: [https://lexparency.org/eu/32014R0833/ART\\_12b/](https://lexparency.org/eu/32014R0833/ART_12b/) (Accessed: 04 August 2023).
2. Leyen, U. von der (2020) *European Digital Identity, European Commission*. Available at: [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en) (Accessed: 04 August 2023).
3. *Glossary: european economic area (EEA) (no date) Glossary: European Economic Area (EEA) - Statistics Explained*. Available at: [https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary%3AEuropean Economic Area %28EEA%29](https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary%3AEuropean+Economic+Area+%28EEA%29) (Accessed: 04 August 2023).
4. European Parliament (2022) *Revision of the eIDAS Regulation Findings on its implementation and application*. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS\\_BRI\(2022\)699491\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf) (Accessed: 04 August 2023).
5. *Report from the Commission to the European Parliament and the council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) (2021b) EUR*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0290> (Accessed: 04 August 2023).
6. *Report from the commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) (2021) EUR*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021SC0130> (Accessed: 04 August 2023).
7. *The Nordic-Baltic Eid Project (NOBID) (no date) Digdir*. Available at: <https://www.digdir.no/digdir/nordic-baltic-eid-project-nobid/1342> (Accessed: 04 August 2023).

---

108.Triangulation in research means using multiple datasets, methods, theories, and/or investigators to address a research question.

8. *Single Digital gateway- once only proof of concept pilot project* (no date) *Nordic cooperation*. Available at: <https://www.norden.org/en/project/single-digital-gateway-once-only-proof-concept-pilot-project> (Accessed: 04 August 2023).
9. Federal Office for Information Security (2017) *German EID based on extended access control V2 - BSI*. Available at: [https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German\\_eID\\_Whitepaper.pdf?\\_\\_blob=publicationFile&v=5](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper.pdf?__blob=publicationFile&v=5) (Accessed: 04 August 2023).
10. Schroers, J. (2023) *A unique identification number for every European citizen: The proposal for a European digital identity regulation and what it entails*, *Verfassungsblog*. Available at: <https://verfassungsblog.de/digital-id-eu/> (Accessed: 04 August 2023).
11. Rafael Campillol am a Computer Engineer who loves Marketing (2023) *Spanish ID cards, evolution and meaning of DNI 3.0 Fields*, *Mobbeel*. Available at: <https://www.mobbeel.com/en/blog/spanish-id-cards-evolution-and-meaning-of-dni-3-0-fields/> (Accessed: 04 August 2023).
12. *Spain foreigner identity card (tie) - visaguide.world*. Available at: <https://visaguide.world/europe/spain-visa/foreigner-identity-card/> (Accessed: 04 August 2023).
13. Bremmers, B. (2023) *2.1 - identity and record matching - Q1 2023, 2.1 - Identity and Record Matching - Q1 2023 - OOTS Technical Design Documents -*. Available at: <https://ec.europa.eu/digital-building-blocks/wikis/display/TDD/2.1+-+Identity+and+Record+Matching+-+Q1+2023> (Accessed: 04 August 2023).
14. Sparks, T. (2020) *How to get your spanish digital ID, (barcelona-metropolitan.com)*. Available at: <https://www.barcelona-metropolitan.com/living/settling-in/how-to-get-your-spanish-digital-id/> (Accessed: 04 August 2023).
15. Ministerio de Asuntos Exteriores, Unión Europea y Cooperación (no date) *Digital Certificate*. Available at: <https://www.exteriores.gob.es/Consulados/toronto/en/ServiciosConsulares/Paginas/Consular/digital-certificate.aspx> (Accessed: 04 August 2023).
16. Age in Spain Team. (2022) *Digital Certificate - A How to guide*. Available at: <https://www.ageinspain.org/post/digital-certificate-guide> (Accessed: 04 August 2023).
17. Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. *Employee visa*. Available at: <https://www.exteriores.gob.es/Consulados/londres/en/ServiciosConsulares/Paginas/Consular/Visado-de-trabajo-por-cuenta-ajena.aspx> (Accessed: 04 August 2023).

18. *A full guide on residency and Nationality Options in Spain* (2023) CostaLuz Lawyers. Available at: <https://costaluzlawyers.es/for-you/a-full-guide-on-residency-and-nationality-options-in-spain/> (Accessed: 04 August 2023).
19. Castro, M.L. (2023) *FAQ Guide to the new digital nomad visa in Spain*, CostaLuz Lawyers. Available at: <https://costaluzlawyers.es/blog/faq-guide-to-the-new-digital-nomad-visa-in-spain/> (Accessed: 04 August 2023).
20. Chamber of Deputies (2013) *Law of 19 June 2013 relating to the identification of natural persons*. Available at: <https://legilux.public.lu/eli/etat/leg/loi/2013/06/19/n3/jo> (Accessed: 04 August 2023).
21. Lemoine, F., Bellwald, C. and Keereman, C. (2022) *Registration of luxembourg national identification numbers (Numéro de matricule) with the Luxembourg Register of Commerce and companies - shareholders - Luxembourg, Registration Of Luxembourg National Identification Numbers (Numéro De Matricule) With The Luxembourg Register Of Commerce And Companies - Shareholders - Luxembourg*. Available at: <https://www.mondaq.com/shareholders/1190004/registration-of-luxembourg-national-identification-numbers-numro-de-matricule-with-the-luxembourg-register-of-commerce-and-companies> (Accessed: 04 August 2023).
22. eIDAS.eID Network. *Information about the national identification number*. Available at: [https://eIDAS.services-publics.lu/cisie-sp/initRegistration?req\\_lang=en](https://eIDAS.services-publics.lu/cisie-sp/initRegistration?req_lang=en) (Accessed: 04 August 2023).
23. Council of the European Union (2023) *PRADO - Public Register of Authentic identity and travel Documents Online*. Available at: <https://www.consilium.europa.eu/prado/en/prado-start-page.html> (Accessed: 04 August 2023).
24. European e-Justice Portal (2020) *Interconnection of EU Business Registers, Business registers at European level*. Available at: [https://e-justice.europa.eu/content\\_business\\_registers\\_at\\_european\\_level-105-en.do](https://e-justice.europa.eu/content_business_registers_at_european_level-105-en.do) (Accessed: 04 August 2023).
25. Welling de Arruda, A. (2022) *Dutch identity matching: The Devil's in the details*, TU Delft Repositories. Available at: <https://repository.tudelft.nl/islandora/object/uuid%3A5d52babb-c6b0-4c96-8f93-8f3129ba448d> (Accessed: 04 August 2023).
26. The Norwegian Tax Administration. *Id checks*. Available at: <https://www.skatteetaten.no/en/person/national-registry/identitetsnummer/id-kontroll/> (Accessed: 04 August 2023).
27. Finanstilsynet (2022) *The AML legislation and requirements for valid proof of identity*. Available at: <https://www.finanstilsynet.no/en/topics/money-laundering-and-financing-of-terrorism/the-aml-legislation-and-requirements-for-valid-proof-of-identity/> (Accessed: 04 August 2023).

28. The Norwegian Tax Administration. *National Identity Numbers*. Available at: <https://www.skatteetaten.no/en/person/national-registry/identitetsnummer/fodselsnummer/> (Accessed: 04 August 2023).
29. The Norwegian Tax Administration. *Changing information regarding your identity in the National Population Register*. Available at: <https://www.skatteetaten.no/en/person/national-registry/change/information-regarding-your-identity/> (Accessed: 04 August 2023).
30. Fahle, C. (2021) *ID control for foreign employees in Norway*, *Magnus Legal Bloggen*. Available at: <https://blogg.magnuslegal.no/en/id-control-for-foreign-employees-in-norway> (Accessed: 04 August 2023).
31. EASi ja KredExi ühendatud (2022) *Residency - e-estonia*. Available at: <https://e-estonia.com/solutions/e-identity/e-residency/> (Accessed: 04 August 2023).
32. Siseministerium (2023) *Personal Identification Code, Estonian Population Register*. Available at: <https://www.siseministerium.ee/en/activities/population-procedures/population-register#personal-identificat> (Accessed: 04 August 2023).
33. Republic of Estonia e-residency (2023) *Who is eligible – knowledge base*. Available at: <https://learn.e-resident.gov.ee/hc/en-us/articles/360000625078-Who-is-eligible> (Accessed: 04 August 2023).
34. Police and Border Guard Board. *Frequently asked questions - E-resident's digital ID*. Available at: <https://www.politsei.ee/en/instructions/e-resident-s-digital-id/frequently-asked-questions> (Accessed: 04 August 2023).
35. Shabbir, N. (2014) *Estonia offers e-residency to foreigners*, *The Guardian*. Available at: <https://www.theguardian.com/world/2014/dec/26/estonia-offers-e-residency-to-world-what-does-it-mean> (Accessed: 04 August 2023).
36. Republic of Estonia e-residency. *How to apply + FAQ – knowledge base*. Available at: <https://learn.e-resident.gov.ee/hc/en-us/articles/360000633237-How-to-apply-FAQ> (Accessed: 04 August 2023).
37. Republic of Estonia e-residency (2023) *Become an E-resident of Estonia: How to apply*. Available at: <https://www.e-resident.gov.ee/become-an-e-resident> (Accessed: 04 August 2023).
38. European Commission (2023) *Eidas regulation, Shaping Europe's digital future*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/eIDAS-regulation> (Accessed: 04 August 2023).
39. European Parliament (2022) *Revision of the eIDAS Regulation: Findings on its implementation and application*, *Think Tank | European Parliament*. Available at: [https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_BRI\(2022\)69\\_9491](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)69_9491) (Accessed: 04 August 2023).

40. Vihma, P. (2022) *The (bumpy) road to european digital identity - e-estonia, e-Estonia*. Available at: <https://e-estonia.com/the-bumpy-road-to-european-digital-identity> (Accessed: 04 August 2023).
41. Vercruyssen, W. (2023) *2.1 - identity and record matching - Q3 2022, OOTS Technical Design Documents*. Available at: <https://ec.europa.eu/digital-building-blocks/wikis/display/TDD/2.1+-+Identity+and+Record+Matching+-+Q3+2022> (Accessed: 04 August 2023).
42. Ministry of Finance (2021) *Single Digital Gateway, Ministry of Finance - gov.pl website*. Available at: <https://www.gov.pl/web/finance/single-digital-gateway> (Accessed: 04 August 2023).
43. Information System Authority (2022) *Your Europe and the Single Digital Gateway of the European Union, Single Digital Gateway of the European Union (SDG)*. Available at: <https://www.riaa.ee/en/state-information-system/data-exchange-platforms/single-digital-gateway-european-union-sdg> (Accessed: 04 August 2023).
44. TOOP Project (2018) *Single Digital Gateway comes into force!, TOOP.EU*. Available at: <https://toop.eu/node/280> (Accessed: 04 August 2023).
45. Agency for Digital Government. *Single Digital Gateway Regulation*. Available at: <https://en.digst.dk/systems/single-digital-gateway-regulation/> (Accessed: 04 August 2023).
46. European Commission (2020) *The once only principle system: A breakthrough for the EU's Digital Single Market, Directorate-General for Informatics*. Available at: [https://commission.europa.eu/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-11-05\\_en](https://commission.europa.eu/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-11-05_en) (Accessed: 04 August 2023).
47. Krimmer, R. et al. (2017) 'Exploring and demonstrating the once-only principle', *Proceedings of the 18th Annual International Conference on Digital Government Research* [Preprint]. doi:10.1145/3085228.3085235.
48. Directorate-General for Informatics (European Commission). (2011) *European Interoperability Framework (EIF), Publications Office of the EU*. Available at: <https://op.europa.eu/en/publication-detail/-/publication/c8d6514e-e729-45a1-81c1-ea3ee811d7a6/language-en/format-PDF/source-search> (Accessed: 04 August 2023).
49. Copenhagen Citizen Service. *CPR number, International.kk.dk*. Available at: <https://international.kk.dk/live/cpr-registration-and-documents/cpr-number> (Accessed: 04 August 2023).
50. Dahl, A. et al. (2021) *Baseline study of cross-border data exchange in the Nordic and Baltic countries, pub.norden.org*. Available at: <https://pub.norden.org/temanord2021-547/#88558> (Accessed: 04 August 2023).

51. Gupta, V.K. (2022) *Luhn algorithm*. Available at: <https://www.geeksforgeeks.org/luhn-algorithm/> (Accessed: 04 August 2023).
52. Skatteverket. *Personal identity number and coordination number*. Available at: <https://www.skatteverket.se/servicelankar/otherlanguages/inenglishengelska/individualsandemployees/livinginsweden/personalidentitynumberandcoordinationnumber.4.2cf1b5cd163796a5c8b4295.html> (Accessed: 04 August 2023).
53. Registers Iceland. *Id numbers, ID numbers | Þjóðskrá*. Available at: <https://www.skra.is/english/people/my-registration/id-numbers/> (Accessed: 04 August 2023).
54. TAKS. *P-Tal, Taks*. Available at: <https://www.taks.fo/en/individuals/tax/p-tal#:~:text=The%20p%2Dtal%20consists%20of,only%20known%20to%20the%20individual.&text=When%20you%20are%20born%20in,to%20receive%20wages%20or%20salaries>. (Accessed: 04 August 2023).
55. Environment agency National Registration Office and TAKS. *Information on Tax Identification Numbers – Faroe Islands*. Available at: <https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/tax-identification-numbers/> (Accessed: 04 August 2023).
56. Agency for Digital Government (2022) *Introduction to the Swedish eID Framework*. Available at: <https://docs.swedenconnect.se/technical-framework/latest/00 - Swedish eID Framework - Introduction.html> (Accessed: 04 August 2023).
57. Directorate of Internal Revenue. *Iceland - Information on Tax Identification Numbers*. Available at: <https://www.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/tax-identification-numbers/> (Accessed: 04 August 2023).
58. Nordic Statistics database (2022) *Who goes where in the Nordic region?* Available at: <https://www.nordicstatistics.org/news/who-goes-where-in-the-nordic-region/> (Accessed: 04 August 2023).
59. European Network of Information Centres in the European Region (ENIC) and National Academic Recognition Information Centres in the European Union (NARIC). *Professional recognition - Enic-Naric*. Available at: <https://www.enic-naric.net/page-professional-recognition#:~:text=Professional%20recognition%20is%20the%20recognition,regulated%20in%20the%20host%20country> (Accessed: 04 August 2023).
60. The European Parliament and The Council of the European Union (2005) *DIRECTIVE 2005/36/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 September 2005 on the recognition of professional qualifications*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0720> (Accessed: 04 August 2023).

61. European Network of Information Centres in the European Region (ENIC) and National Academic Recognition Information Centres in the European Union (NARIC). *about the ENIC-NARIC networks*. Available at: <https://www.enic-naric.net/page-homepage> (Accessed: 04 August 2023).
62. European Commission. *Internal Market Information System, IMI-Net Homepage*. Available at: [https://ec.europa.eu/internal\\_market/imi-net/index\\_en.htm](https://ec.europa.eu/internal_market/imi-net/index_en.htm) (Accessed: 04 August 2023).
63. Council of Europe. *Lisbon recognition convention, Higher education and research*. Available at: <https://www.coe.int/en/web/higher-education-and-research/lisbon-recognition-convention> (Accessed: 04 August 2023).
64. Hännikäinen, H. *et al.* (2019) *Nordic Work Mobility and Labour Market – for Professional Scientists*. Available at: [https://www.fin.is/media/utgafa/Nordic\\_Work\\_Mobility\\_190628\\_Norden.pdf](https://www.fin.is/media/utgafa/Nordic_Work_Mobility_190628_Norden.pdf) (Accessed: 04 August 2023) doi:10.6027/tn2010-515.



## 4.4 Participants in workshops and interviews

During the analysis, a total of 46 representatives from 26 different organizations and 13 different countries participated in interviews and workshops.

Name	Country	Organization
Emilie Kristin Pedersen, Sven Rostgaard Rasmussen, Linh Signe Tran Nygaard	Denmark	Danish Agency for Digital Government
Tiiia Raudma	Estonia	Estonian Ministry of Education and Research
Katre Pruul	Estonia	Estonian Health and Welfare Information Systems Centre
Enel Pungas, Carolyna Maidla	Estonia	Estonian Population Register
Mark Erlich, Helen Raamat, Silvia Lips	Estonia	Estonian Information System Authority
Stina Avvo, Mait Heidelberg	Estonia	Ministry of Economic Affairs and Communications
Jónsvein Simonsen, Janus Helgi Læarsson	Faroe Islands	The National Digitalization Programme of the Faroe Islands
Mervi Kylmänen-Paakki, Kirsi Mikkonen	Finland	Development and Administrative Services Centre (KEHA Centre)
Anneli Kupari	Finland	Finnish Digital and Population Data Services Agency
Erik Frydensberg-Holm	Greenland	The Greenlandic Agency for Digitization
Haraldur Bjarnason, Erna Birgisdóttir, Arnaldur Axfjörð	Iceland	Auðkenni ehf
Jens Svansson	Iceland	Icelandic Tax Authority
Einar Gunnar Thoroddsen	Iceland	Ministry of Finance and Economic Affairs

Halldor B. Hreinsson, Júlía Þorvaldsdóttir, Soffía Felixdóttir, Bryndís Bjarnþórsdóttir, Gunnar Geir Johannsson	Iceland	Registers Iceland
Uldis Apsitis	Latvia	Register of Natural Persons
Linda Mikelsone	Latvia	Ministry of Environmental Protection and Regional Development
Vytautas Krasaukas	Lithuania	Information Technology and Communications Department under the Ministry of the Interior of the Republic of Lithuania
Egle Simukenaite, Jevgenij Višniakov	Lithuania	Lithuanian Information Society Development Committee
Liudas Kanapienis	Lithuania	Ondato
Lionel Antunes	Luxembourg	The Government of The Grand Duchy of Luxembourg
Frans Rijkers	Netherlands	Dutch National Office for Identity Data, Ministry of the Interior and Kingdom Relations
Tor Alvik, Ismail Yasir Özcan, Stig Slaatto-Hornnes, Herman Walby, Runar Ugelstad, Oskar Drastrup-Fjordbak	Norway	Norwegian Digitalisation Agency
Jan Olnes	Norway	Signicat
Antonio Skarmeta	Spain	University of Murcia
Maria Engström, Aras Kazemi	Sweden	Swedish Agency for Digital Government

## 4.5 Aspects analyzed per country

**Table 18** Overview of analyzed aspects per country

Country	Processes	Best practices	Data requirements	Structural challenges
Germany		x		
Poland		x		
Malta		x		
Spain	x	x		
Luxembourg	x	x		
Netherland	x	x		
Norway	x	x		x
Estonia	x	x	x	x
Finland			x	x
Iceland				x
Latvia				x
Denmark				x
Faroe Islands				x
Sweden			x	x
Lithuania				x
Greenland				x

# About this publication

## IDENTITY MATCHING IN THE NORDIC BALTIC-REGION

*This analysis has been compiled by Civitta Estonia and SK ID Solutions on behalf of the Nordic Council of Ministers.*

*The proposed solutions in the analysis can be used as suggestions by the Nordic Council of Ministers for making further decisions.*

*Contributors to the analysis:*

- *Maari Helilaid (Civitta);*
- *Kenn Laas (Civitta);*
- *Rita Treimuth (Civitta);*
- *Annette Schultz (Civitta);*
- *Marit Napp (Civitta);*
- *Raul Eks (SK ID Solutions);*
- *Katrin Laas-Mikko (SK ID Solutions);*
- *Kalev Pihl (SK ID Solutions);*
- *Sigurður Másson (external expert).*

*We thank all the interviewed experts who contributed to the completion of the analysis.*

TemaNord 2024:511

ISBN 978-92-893-7851-2 (PDF)

ISBN 978-92-893-7852-9 (ONLINE)

<http://dx.doi.org/10.6027/temanord2024-511>

© Nordic Council of Ministers 2024

Cover photo: Greta Hoffman/Pexels

Published: 8/5/2024

## Disclaimer

This publication was funded by the Nordic Council of Ministers. However, the content does not necessarily reflect the Nordic Council of Ministers' views, opinions, attitudes or recommendations.

## Rights and permissions

This work is made available under the Creative Commons Attribution 4.0 International license (CC BY 4.0) <https://creativecommons.org/licenses/by/4.0>.

**Translations:** If you translate this work, please include the following disclaimer: This translation was not produced by the Nordic Council of Ministers and should not be construed as official. The Nordic Council of Ministers cannot be held responsible for the translation or any errors in it.

**Adaptations:** If you adapt this work, please include the following disclaimer along with the attribution: This is an adaptation of an original work by the Nordic Council of Ministers. Responsibility for the views and opinions expressed in the adaptation rests solely with its author(s). The views and opinions in this adaptation have not been approved by the Nordic Council of Ministers.

**Third-party content:** The Nordic Council of Ministers does not necessarily own every single part of this work. The Nordic Council of Ministers cannot, therefore, guarantee that the reuse of third-party content does not infringe the copyright of the third party. If you wish to reuse any third-party content, you bear the risks associated with any such rights violations. You are responsible for determining whether there is a need to obtain permission for the use of third-party content, and if so, for obtaining the relevant permission from the copyright holder. Examples of third-party content may include, but are not limited to, tables, figures or images.

### **Photo rights (further permission required for reuse):**

Any queries regarding rights and licences should be addressed to:  
Nordic Council of Ministers/Publication Unit  
Ved Stranden 18  
DK-1061 Copenhagen  
Denmark  
[pub@norden.org](mailto:pub@norden.org)

## **Nordic co-operation**

*Nordic co-operation* is one of the world's most extensive forms of regional collaboration, involving Denmark, Finland, Iceland, Norway, Sweden, and the Faroe Islands, Greenland and Åland.

*Nordic co-operation* has firm traditions in politics, economics and culture and plays an important role in European and international forums. The Nordic community strives for a strong Nordic Region in a strong Europe.

*Nordic co-operation* promotes regional interests and values in a global world. The values shared by the Nordic countries help make the region one of the most innovative and competitive in the world.

The Nordic Council of Ministers  
Nordens Hus  
Ved Stranden 18  
DK-1061 Copenhagen  
pub@norden.org

Read more Nordic publications on [www.norden.org/publications](http://www.norden.org/publications)