PROUD ENGINEERS

Study on Nordic-Baltic Trust Services

by Proud Engineers:

Hille Hinsberg, Kaspar Kala, Laura Kask and Andres Kütt

Study on Nordic-Baltic Trust Services

Table of Contents

Definitions

- "**Alternative trust services**" mean services which are not trust services according to eIDAS but aim to bring about the same legal effect – i.e. link the identity of a person to an action online. In the context of this study, such alternative trust services are authentication services which establish the persons' intent in online electronic services without the requirement for an e-signature or e-seal.
- "**CA**" means Certification Authority.
- "**Declaration**" means the Digital North Ministerial Declaration signed in 2017.
- "**eID**" means electronic identity.
- "**eIDAS gateway**" means the same as eIDAS node.
- "**eIDAS network**" means the interconnected eIDAS nodes.
- "**eIDAS node**" means the CEF eIDAS node software used for authentication.[1]
- "**eIDAS Regulation**" or "**eIDAS**" means the EU Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market
- "**Electronic signature**" or "**e-signature**" means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign as per article 3(10) of the eIDAS Regulation;
    - "advanced electronic signature" means an electronic signature which meets the requirements set out in article 26 of the eIDAS Regulation
    - "qualified electronic signature" means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures
- "**Electronic seal**" or "**e-seal**" means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity as per article 3(28) of the eIDAS Regulation;
    - "advanced electronic seal" means an electronic seal, which meets the requirements set out in article 36 of the eIDAS Regulation;
    - "qualified electronic seal" means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal.
- "**Electronic registered delivery service"** or "**e-delivery**" means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;
- "**Federated authentication services**" means services passing on and linking identity information between different service providers allowing an organisation to provide proof of a person being authenticated to other organisations.

[1] eIDAS eID Profile, Technical specifications v.1.2, https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile (accessed 7 October 2020).

- "**Identity carrier**" means a device by means of which a person can assert their identity in an online setting.
- "**LoA**" means level of assurance referencing the eIDAS Regulation's levels "low", "substantial" and "high".
- "**mID**" means an identity carrier based on a mobile device like a smartphone.
- "**NOBID countries**" refers to the eight Nordic and Baltic countries in scope of this study. Namely, Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden.
- "**NOBID**" refers to the Nordic-Baltic region.
- "**PSD2**" or "**PSD2 Directive**" means the EU Directive No 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.
- "**QSCD**" means qualified signature creation device.
- "**QTSP**" – means trust service provider meeting the requirements set for a qualified trust service provider within the meaning of the eIDAS Regulation.
- "**QWAC**" means qualified certificate for website authentication within the meaning of eIDAS Regulation.
- "**SDG**" or "**SDG Regulation**" means the EU Regulation No 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services.
- "**Trust services according to eIDAS**" refer to trust services as defined in article 3(16) of the eIDAS Regulation. See also section 4.1.2.

1. Introduction

This report captures the as-is overview of the trust services landscape in the eight Nordic-Baltic countries (NOBID countries), i.e. Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden. The study has been prepared by Proud Engineers OÜ at the request of the Nordic-Baltic eID Project[2], managed by the Norwegian Digitalisation Agency (Digdir).

Firstly, the report presents an overview of policy and regulatory context of each NOBID country (section 4). Although the overarching regulatory principles are similar and the adoption of the eIDAS Regulation has affected the national regulatory landscape in all NOBID countries, there are still many differences in terms of the level of assurance of electronic signatures which are mandated by law, what is deemed to be sufficient evidence of one's identity and how the eIDAS framework is applied in a country. Therefore, the barriers and differences arise not just from the national regulatory landscape but also the prevalent approaches to trust and identity that a country upholds. For these reasons, it is important to explore and understand the situation in the context of the NOBID region.

Secondly, the study describes what trust services (as defined in the eIDAS Regulation) as well as alternative trust services - services, which are not trust services according to eIDAS Regulation, but which aim to bring about the same legal effect as e-signatures and e-seals, i.e. link the identity of a person to an action online – are present in NOBID countries (sections 5.1-5.2). The study sought out qualified trust service providers, defined which non-qualified trust service providers are most dominant on the market and what are the authentication solutions that are mostly in use.

Thirdly, the study looks at the use of cross-border electronic services and how trust services and alternatives thereof are engaged in the service provision (section 5.3).

Fourthly, the study analyses barriers to the cross-border use of trust services and alternatives thereof both in and between NOBID countries in the findings section (section 6.1). Besides barriers, the study also discusses several enablers and drivers for further use of trust services between NOBID countries (section 6.2).

The study is accompanied by two appendices. "Appendix A: Interviewees" presents a list of the interviewees. These interviews formed the major source of information for the study. "Appendix B: The market of trust services and alternatives thereof in NOBID countries" presents a list of services provided, their roles in different countries as well as remarks on services provided and market focus.

No similar studies regarding trust services and alternatives thereof have been conducted in the NOBID region prior to this. However, in a different scope of thematic focus and regional coverage, the use of eID and cross-border services have been studied before.[3]

Facts, information and data is presented in the report as of September 2020.

[2] The Nordic-Baltic eID Project (NOBID), https://www.digdir.no/om-oss/nordic-baltic-eid-project-nobid/1342 (accessed 1 October 2020).
[3] D. Jaakkola, *e-ID and digital border obstacles in the Nordic region*, Nordic Council of Ministers, 2018 and K.Hansteen, J.Ølnes, T.Alvik, *Nordic digital identification,* TemaNord, 2016.

2. Executive summary

This study sought to investigate the landscape of trust services and their alternatives in NOBID countries as well as use of these services between the countries along with barriers or enablers for the use.

The research methods included conducting interviews with public and private sector representatives from all of the NOBID countries (see Appendix A: Interviewees). Based on the input from the interviews as well as other document-based sources, desk research was conducted investigating the policies in place in NOBID countries as well as the supply of identity and trust services on the market. The results of both streams of research were then combined and directed to the research group for feedback along with specific questions to be clarified. Further feedback rounds and comments submitted by interviewees resulted in the document at hand.

The study identified key policy and regulatory documents in the area of trust services and eID as well as policy owners. Despite a very similar shared legal context in terms of the eIDAS Regulation, the countries are remarkably different in terms of the specific ways the eIDAS Regulation has been implemented. Although requirements for trust services are regulated under the eIDAS Regulation, the legal meaning differs. In the Baltic region, a qualified e-signature is mostly required by law whereas the laws of other NOBID countries tend to be laxer on the issue and require the use of lower-level e-signatures (e.g. advanced electronic signatures). The private sector relies more on the principle of freedom of contract (including the freedom of format) and different means to express the intent online are used. Most public e-services might not even need e-signature and authentication is deemed sufficient. This is primarily the case in the Nordics; the Baltic region has a few examples, but most e-services require qualified e-signatures. Other trust services within the meaning of the eIDAS Regulation and their legal meaning are usually not defined. Although e-seals are used, their legal meaning is vague, or they are used within a specific service. Only Lithuania has defined the legal meaning of all trust services regulated in eIDAS Regulation. As eID is subject to national legislation, the legal frameworks differ between countries in that regard.

The research identified 35 organisations based in NOBID countries and operating in the multi-faceted international market of solving the problem of capturing the intent of a particular user in a legally valid fashion. In this market, banks appear to play a significant role. For example, they can be direct providers of digital identity as part of the BankID structures in Finland, Sweden, and Norway. Or they can be owners of major trust service providers like in Iceland and Estonia. Banking and financial transactions also occur as drivers of dominant use cases for various trust-related services. That said, telecom companies, private enterprises, and start-ups of varying levels of maturity also play a significant role. There certainly is no shortage of trust service providers and the supply of available services is wide in scope and variety.

On the demand side, there is still great potential for electronic identity and trust services in cross-border use (i.e. when a private person or a legal entity registered in one country needs to access services in another country, using one's own electronic means of identification).

All eight NOBID countries have a high level of digital maturity and have solid experience in doing business, conducting transactions, and using e-services online. However, there is considerable difference concerning how these actions are done. If the Baltic states are generally more dependent on qualified trust services and require a high level of assurance

of electronic identity, then Nordic countries use authentication solutions which are commonly on the substantial level for authentication and use advanced electronic signatures instead of qualified electronic signatures. Besides looking into how trust services and alternatives thereof are used in the NOBID countries, the study also looks at cross-border use of trust services and alternatives. There are market players who offer services in multiple countries, but these service providers tend to be either Nordic or Baltic in nature, not NOBID-wide.

The SDG Regulation defines services which are to be completed fully online. The volume of cross-border use cases, however, is reportedly low. Although the enabling eIDAS framework exists and all the NOBID countries have a national personal identification code which would in principle enable the cross-border interaction. The report concludes, however, that these enablers have not created sufficient cross-border online interaction.

Countries in the NOBID region have mostly established eIDAS nodes to comply with the eIDAS Regulation, to enable authentication with foreign means. However, mere identification does not fulfil the real purpose of using other countries' electronic services which would be the aim of the SDG Regulation. The access to electronic services is restricted because service providers, including public authorities and private providers, cannot establish a match of a foreign personal identification code with the person in a reliable way. Mostly, the services are designed for nationals of the country whose national personal identification codes are connected to the public registries and databases. Other nationals need to apply for a resident ID or obtain a local bank ID to get access to electronic services. As these options are available for private and corporate use, the motivation to use state-issued means of identification for cross-border electronic services in accordance with eIDAS requirements remains low.

Existing barriers to the use of electronic identity between NOBID countries were also highlighted. Some of the most significant ones of these are not directly related to trust services at all: semantics and format of the identity code, access to interoperability solutions and challenges in driving eID adoption were all cited as challenges to be surmounted.

In terms of potential for further use cases and larger volumes, the act of notification of the European Commission of various authentication schemes would create a solid basis for accepting these schemes in the European international context.

COVID-19 was established as one of the reasons to significantly increase the use of trust services and alternatives thereof in many of the NOBID countries.

The main conclusion of the study is that the NOBID countries are remarkably different in their approach to managing trust and that significant barriers exist for cross-border provision of services. However, no significant unresolved trust-related problems were found. Instead, a variety of innovative, mostly bilateral, solutions have been put in place to cater for the needs and trust-related use cases faced by population and in business interactions.

3. Research questions and method

This section outlines the research questions of the study (section 3.1) together with the research method (section 3.2).

3.1. Research questions

The study was designed to answer the following research questions:

- What trust services (eIDAS-defined as well as alternatives) are offered in NOBID countries? (section 5.1)
- In what areas and for which public- and private services are trust services (as well as alternatives) currently used in NOBID countries? (section 5.2)
- How can these trust services (as well as alternatives) be used between NOBID countries (especially in SDG Regulation context)? (section 5.3)
- What are the key barriers in using trust services (and alternatives thereof) in and between NOBID countries? (section 6.1)
- What are the key enablers for cross-border use of trust services (and alternatives thereof) between NOBID countries? (section 6.2)

3.2. Research method

The objectives of this study have been pursued through qualitative systematic analysis of the relevant laws, policy documents, previous reports and studies on the topic, and EU-level reports and materials on eIDAS Regulation and SDG Regulation adoption.

In order to answer the research questions, policy and product people from all NOBID countries were interviewed (see Appendix A: Interviewees). To answer the research questions regarding the uptake and usage of eID and trust services, the research team interviewed service providers, eID and trust services policymakers, and service owners. As the cross-border usage is closely connected to the services, SDG coordinators of NOBID countries were also interviewed. The full list of interviewees can be found in Appendix A: Interviewees.

In addition to interviews, the desk research focused on mapping the current trust services landscape and alternative trust services in the NOBID countries in both public (incl. building blocks) and private sectors.

The evidence collected through the interviews and desk research is used to describe the trust services landscape in and between NOBID countries as well as the barriers and enablers in using trust services across borders between NOBID countries.

The research method is visualised below in Figure 1.

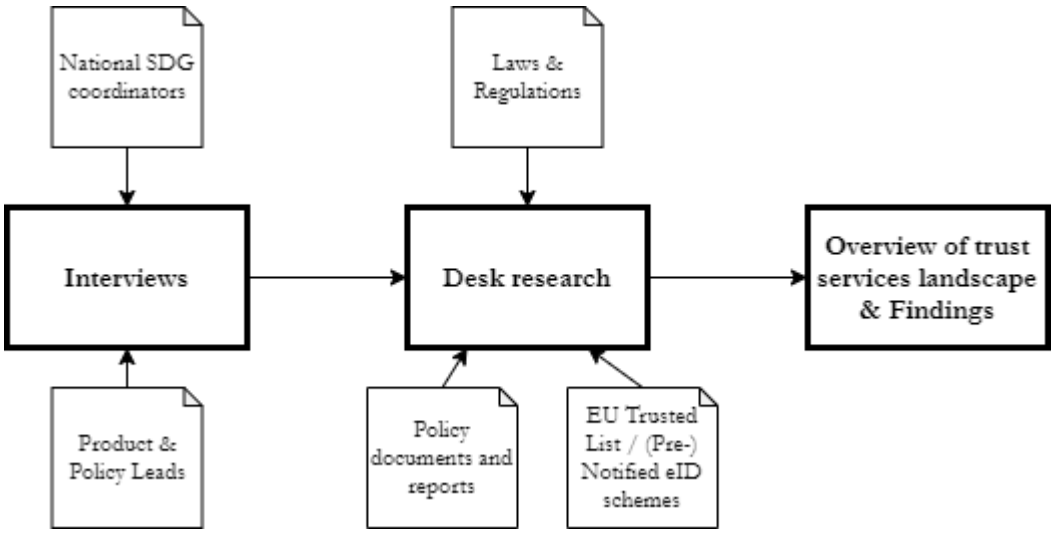

Figure 1. Research method of the study

4. Policy and Regulatory Context

This section analyses the key policy and regulatory documents both at the cross-border (section 4.1) and country (section 4.2) level.

4.1. Cross-border policy and regulation

This section outlines some of the elementary horizontal policy and regulatory documents which set the groundworks for the study – the Digital North Ministerial Declaration of 2017[4], eIDAS Regulation[5] and SDG Regulation.[6]

4.1.1. Digital North Ministerial Declaration

The Declaration was signed in Oslo in 2017. The Declaration states that the Nordic-Baltic region is a digital frontrunner and proposes means how to capitalise on this and spur innovation. The signatories of the Declaration extend beyond the countries in the scope of this study (as they include the eight NOBID countries as well as Faroe Islands, Greenland and Åland). The ministers in charge of digital development agreed on the following:

1. Strengthening the ability for digital transformation of our governments and societies, especially by creating a common area for cross-border digital services in the public sector.
2. Strengthening the competitiveness of our enterprises through digitalisation.

[4] Ministerial Declaration. Digital North: Nordic-Baltic Ministerial Conference of Digitsation, https://www.regjeringen.no/contentassets/5ed83530b83c4e4ba85338c29eb50c63/ministerial-declaration.pdf (accessed 2 July 2020).

[5] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN (accessed 2 July 2020).

[6] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012, OJ L 295, 21.11.2018, p. 1–38, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1724&from=EN (accessed 2 July 2020).

3. Enhancing the digital single market in the Nordic-Baltic region.

The Declaration describes some of the activities which will be undertaken in the future to achieve these goals by removing technical and legal barriers. The extended use of cross-border services by the signatories is captured under the first goal. In order to make advances on the first goal, the ministers have agreed, among other things, "to enable the use of unique identity numbers across borders and facilitating cooperation between national infrastructures for the use of electronic authentication in accordance with the eIDAS Regulation". Also, the Declaration states that the signatories are to "promote the re-use and free movement of data in order to support more advanced public service design that will reduce administrative burden for citizens and businesses, and identifying key fields and building common infrastructures for data exchange within these fields".

It is evident that the Declaration wishes to make advances in the area of eID (and unique identification numbers) as well as cross-border electronic services. Trust services as such are not mentioned in the Declaration nor in the context of cross-border electronic services.

Besides the cross-border services aspect, the Declaration aims to promote the Nordic-Baltic region as a trailblazer in innovative services and data economy (see goal 2), all while exchanging best practices and experiences between the signatories (see goal 3).

4.1.2. eIDAS Regulation

With the adoption of the eIDAS Regulation on 23 July 2014, the EU has created the legal framework for secure cross-border electronic transactions. The primary objective of the eIDAS Regulation has been to build trust in the online environment. This lack of trust, in particular lack of legal certainty, has made consumers, businesses and public authorities hesitant to carry out transactions electronically.[7] As the electronic identification and trust services are believed to be the central building blocks of the Digital Single Market, the adoption of the regulation was a milestone to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens, and public authorities. As an EU regulation, the eIDAS Regulation applies in all EU member states, overriding national law in case of conflict. Since the eIDAS Regulation is "of EEA relevance", it also applies to Norway and Iceland.

Interestingly, the common legal basis for cross- border recognition of electronic signatures already existed and was constituted by the Directive 1999/93/EC of the European Parliament and the Council. However, the directive lacked a comprehensive cross-border and cross-sector framework for mutual recognition of eIDs and trust services and was implemented differently by the Member States.

The eIDAS Regulation is divided into three parts[8]:

1. The first part of the regulation ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU countries.

The mutual recognition of notified eIDs is a new requirement in EU law. The member states still have their sovereign right to establish a domestic legal framework for eID, the notification of identity schemes on EU level is voluntary, and member states are allowed to

[7] A. Zaccaria, M. Schmidt- Kessel, R. Schulze, A. M. Gambino. *EU eIDAS Regulation. Article- by- Article Commentary*. C. H. Beck. 2020, p. 2.
[8] *Ibid*, p. 3.

decide if they want to include private sector means in the provision of authentication services.[9] There is a requirement to recognise 'notified' eIDs of other Member States for cross-border access to its online services when the national laws mandate e-identification. The e-authentication facility for 'notified' eID(s) must be free of charge. The eIDs are divided into three levels – high, substantial and low.

2. The second part of the regulation creates a European internal market for trust services.

The following trust services are regulated:

- the creation, verification, and validation of electronic signatures, electronic seals, time stamp, electronic registered delivery service and certificates related to those services, or;
- the creation verification, and validation of certificates for website authentication, or;
- the preservation of electronic signatures, seals or certificates related to those services.

The aim is to ensure that these processes will work across borders and have the same legal status as traditional, paper-based processes. The trust services part is an internal market regulation and member states can only regulate the parts that are left explicitly for member states to regulate or are not in conflict with the regulation. When the public sector accepts a document being signed electronically, they must accept documents signed electronically in the same format from the other member states or with the service offered by the other service providers. The qualified e-signature is equal to and has same legal effect as handwritten signature (Article 25).[10]

Member states maintain and publish trusted lists which form the Trusted List[11] where all the necessary information about the qualified service providers acting inside the EU is presented. Trust services provided by trust service providers established in a third country shall be recognised legally once there is an agreement between the EU and the third country.

3. The third part of the regulation is dedicated to electronic documents.

There is a principle stating that an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that is in electronic form. The eIDAS Regulation is not intended to cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards from laid-down national or EU law, or to affect national form requirements pertaining to public registries, in particular commercial and land registries.[12]

---

[9] Identity management is the sovereign right of a Member State. Respecting the principles of the regard to the Treaty on the Functioning of the European Union (OJ C 326, 26.10.2012, p. 47–390), eIDAS Regulation does not interfere with the issuance of electronic identities (as official documents) and status of citizens of Member States.
[10] Qualified electronic signature means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures, but the lower levels of e-signatures could also have a legal effect in different Member States. For example, advanced electronic signature with qualified certificate could be deemed sufficient although it does not include qualified electronic signature creation device or even the certificate could be non-qualified. The legal meaning of those signatures stems from national legislation.
[11] Trusted List Browser, https://webgate.ec.europa.eu/tl-browser/ (accessed 1 October 2020).
[12] eIDAS Regulation, recital 21.

4.1.3. SDG Regulation

With the adoption of the Single Digital Gateway Regulation on 2 October 2018, the EU has created the legal basis for EU-users to obtain information and complete procedures online in a cross-border setting more thoroughly and updated means for assistance and problem-solving services.[13]

As the internal market and the free movement of people, goods, services and capital are the founding principles of the EU, the SDG acts as an important enabler for not only access to information and help, but also to services. The SDG Regulation, in Article 6(1) stipulates that there are some electronic services (stated in Annex II of the Regulation) that users must be able to access and complete fully online, provided that the Member State is offering such services. Article 6(2) of the SDG Regulation states that the service shall be considered to be fully online where:

(a) the identification of users, the provision of information and supporting evidence, signature and final submission can all be carried out electronically at a distance, through a service channel which enables users to fulfil the requirements related to the procedure in a user-friendly and structured way;

(b) users are provided with an automatic acknowledgement of receipt, unless the output of the procedure is delivered immediately;

(c) the output of the procedure is delivered electronically, or where necessary to comply with applicable Union or national law, delivered by physical means; and

(d) users are provided with an electronic notification of completion of the procedure.

This means that the eIDAS Regulation must be used within the context of electronic identification and trust services to identify oneself and/or complete the procedure with a submission of evidence or by way of trust service (electronic signature, for example).

The services which, provided that such procedures have been established in a Member State, are related to specific life events are the following:

- Birth
- Residence
- Studying
- Working
- Moving
- Retiring; and
- Starting, running and closing a business.

The procedures and output of these services which are within the scope of Article 6, however, have been narrowed down by Annex II specifying which procedures are in its scope. So, for birth, for example, the procedure "requesting proof of registration of birth" must be fully online with the output of "proof of registration of birth or birth certificate". The same goes for all other aforementioned life events.

In the context of this study, we have been asked to look at the following life events and cross-border electronic services:

- studying abroad (applying for study admission or grant or study financing)

[13] Your Europe gateway, https://europa.eu/youreurope/index.htm (accessed 1 October 2020).

- working abroad (request for work permit or residence permit; also, for notifying of changes in family situation relevant for social services)
- moving abroad (registering change of address, requesting proof of residence)
- doing business abroad (establishing a company, registration of employees, reporting on changes in business status or business activity, permission for cargo transit)

Compared to Annex II of the SDG Regulation, the scope of the study does not cover birth and retirement. Although residence is brought out as a separate life event, it is represented under "moving" in the study. This scope of services for the study has been provided by the NOBID project team. The list of priority services in the NOBID project or in the Nordic Council of Minister's programme Cross-Border Digital Services (CBDS programme) was still open at the time of the interview stage of the study. It must be noted that the scope of services under the life events do not match in all cases. For example, permission for cargo transit under "Doing business abroad" is listed as one of the services in Annex II. Also, there are procedures in Annex II which are not listed in the study. As the NOBID project aimed to develop its own priority list for the study to be received as an input from the CBDS programme to be looked at in the study, the study has taken only the look at the input from the NOBID project team and not Annex II of the SDG Regulation.

4.2. Country-specific policy and regulation

This section describes the relevant policies and regulations in all NOBID countries.

4.2.1. Denmark

In order to provide guidelines for citizens and authorities in regard to the eIDAS Regulation, the Act on Issuance of NemID with Public Digital Signature for Physical Persons and Employees in Legal Entities, as well as the Danish Executive Order on Issuance and Suspension of NemID with Public Digital Signature were enforced in 2018.[14]

Danish digital governance is decentralised, with all public agencies and municipalities bearing the responsibility on the provision of public services. However, the Digitisation Pact with the Local Government Denmark and Danish Regions was concluded in 2019 with the goal to strengthen cohesion in the public digital service sphere.[15] The policy goal has consistently been to turn the interaction with citizens and business sector fully digital where possible.

The government has provided free NemID use for citizens and residents of Denmark. Initial certificates for employees (three per company) are free as well. This means that the basic infrastructure and services are provided, but there are opportunities in the market for private companies providing services connected to NemID, making this infrastructure more useable. As the new infrastructure (MitID and NemLogin[16]) will replace the current platform, the market needs to change along with this shift.[17] The new infrastructure was tendered in a

[14] Digital Government Factsheet. Denmark, European Commission, 2019, p. 13, https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Denmark_2019.pdf (accessed 1 October 2020)
[15] Digital Government Factsheet. Denmark, p. 6.
[16] In the upcoming third generation of NemLogin a new law will make it mandatory for public sector services to use NemLogin as a broker for the new national eID solution, MitID to be launched mid-2021. This law has yet to be passed in the Danish parliament.
[17] The new MitID supports as a starting point only authentication. Signing is a service that must be added, e.g. by brokers.

partnership between the government and Finance Denmark, the Danish Bankers Association.

Certificates and signatures based on the national standard for public certificates (OCES standard) are extensively used in Denmark and have been so for the last decade.[18] A national Danish standard for identity assurance levels has recently been established, corresponding to eIDAS assurance levels (high, substantial, low). The new national eID solution, MitID, will be based on this standard and apply these assurance levels, as is the case for the new solution for digital business identities for employees.

Authentication is deemed to provide sufficient proof of a person's intent online in most cases, but electronic signatures based on OCES certificates (not qualified certificates in the sense of the eIDAS Regulation) are widely used as well. These are considered binding under Danish national law, which does not require the use of qualified signatures.

The Danish act no. 617 of 8 June 2016[19] defined the Agency for Digitisation under the Ministry of Finance as the Danish Supervisory Body and set out the rules for trust service providers with reference to existing national legislation.[20] There is no official supervision for eID solutions except for the national solutions.

The Danish Agency for Digitisation is responsible for keeping the Danish trusted list[21] as well as maintaining the eIDAS node.

The responsibility for SDG-related information and framework lies in the Agency for Digitisation and the Danish Business Authority. The English-language side of the state portal borger.dk, lifeindenmark.dk is the Danish gateway for providing information and guidance to citizens as required by the regulation. The English-language side of the state portal virk.dk, businessindenmark.dk is the Danish gateway for providing information and guidance to businesses as required by the regulation.

4.2.2. Estonia

Estonia implemented the eIDAS Regulation to national legislation with the Electronic Identification and Trust Services for Electronic Transactions Act[22] which came into force in 26 October 2016. The act replaced the Digital Signature Act[23] which had already been in force since 2000.

Estonian electronic identity schemes which are also notified under eIDAS are regulated under Identity Documents Act[24] and there is no special law to regulate electronic identification. The issuance of electronic identity documents is led by the Police and Border Guard Board. Nevertheless, there have been discussions to regulate private sector e-

[18] The OCES standard is a national standard for public certificates for electronic services consisting of four certificate policies issued by the Danish Agency for Digitisation. OCES certificate policies, https://www.nemid.nu/dk-da/om-nemid/historien_om_nemid/oces-standarden/oces-certifikatpolitikker/ (accessed 1 October 2020).
[19] LOV nr 617 af 08/06/2016, https://www.retsinformation.dk/eli/lta/2016/617 (accessed 1 Octber 2020).
[20] Digital Government Factsheet. Denmark, p. 14.
[21] Danish Trusted List, https://en.digst.dk/media/22276/draft_dk_11722-prettyprint.pdf (accessed 1 October 2020).
[22] Electronic Identification and Trust Services for Electronic Transactions Act, https://www.riigiteataja.ee/en/eli/ee/527102016001/consolide/current (accessed 8 July 2020).
[23] Digital Signature Act, https://www.riigiteataja.ee/akt/693656 (accessed 8 July 2020).
[24] Identity Documents Act, https://www.riigiteataja.ee/en/eli/504022020003/consolide (accessed 22 July 2020).

identification schemes and national notification procedures in the Electronic Identification and Trust Services for Electronic Transactions Act.

The policy coordinator of electronic identity and trust services is the Ministry of Economic Affairs and Communications.[25] The policy coordinator of personal identification documents and identity management is the Ministry of Interior.[26] The Information System Authority is responsible for producing eID and trust services policy guidelines for the public sector. They are also responsible for the management of the national eIDAS node, the state authentication service (TARA), and the technical layer of the national eID schemes.

There is a legal requirement in the public sector to submit applications using a handwritten signature or an electronic signature equal to handwritten signature.[27] As the eIDAS Regulation Article 25 states that a qualified e-signature using a qualified electronic signature creation device is deemed to be on par with a handwritten signature[28], the most common way of signing in public and private sector is the qualified e-signature.

Nevertheless, the new information systems seem to be more flexible and secure high-level authentication is also deemed sufficient for instances which are explicitly stated in the law.[29]

Signing on behalf of a company is done by natural persons, no special requirement for e-seals exist, although they are used in some sectors (e.g. banking and education).

The supervision over the compliance with the requirements established for trust service providers is fulfilled by the Information System Authority[30], which also keeps the Estonian trusted list. The supervision concerns only qualified service providers. The authority is also the supervisory authority for cyber security.

The responsibility for the implementation of the SDG Regulation lies with the Ministry of Economic Affairs and Communications. The services will be mainly accessible via the state portal eesti.ee.[31]

4.2.3. Finland

The Act on Strong Electronic Identification and Electronic Trust Services[32] entered into force on 1 September 2009. It was amended to include rules on the trust network of identification services and align national legislation with the requirements of eIDAS. The amendments of trust network became applicable in May 2017 and eIDAS-related amendments became binding in July 2017. The most recent amendments concerning trust network entered into

[25] Information society. Digital Agenda 2020 for Estonia, https://mkm.ee/en/objectives-activities/information-society (accessed 22 July 2020).
[26] Supervision. State Information System Authority, https://www.ria.ee/en/cyber-security/supervision.html (accessed 8 July 2020).
[27] There is no general requirement and it is the discretion of a service owner. Each information system or registry has their legal base in form of a legal act. For example, Business Registry Act. All the applications submitted to the Business Registry must be either signed with qualified e-signature or approved by the notary (Article 33), https://www.riigiteataja.ee/akt/110072020034?leiaKehtiv (accessed 22 July 2020).
[28] Qualified electronic signature is an advanced electronic signature that is created by a qualified electronic signature creation device which is based on a qualified certificate for electronic signatures and issued by a qualified TSP.
[29] Please see article 15(1)(11) of the Funded Pensions Act: the signature of the person unless the application is submitted in a manner which enables written reproduction and identification of the person, https://www.riigiteataja.ee/en/eli/529042020002/consolide (accessed 8 July 2020).
[30] Electronic Identity eID, https://www.ria.ee/en/state-information-system/electronic-identity-eid.html (accessed 24 July 2020).
[31] Eesti.ee https://www.eesti.ee/en/ (accessed 1 October 2020).
[32] Act on Strong Electronic Identification and Electronic Trust Services (617/2009; amendments up to 412/2019 included), https://www.finlex.fi/en/laki/kaannokset/2009/20090617 (accessed 1 October 2020).

force in April 2019. The Act was founded on the principle that users must be able to trust information security and protection of privacy when using electronic identification services.[33] Since 2019 the law was amended, and driver's licenses are no longer a valid method of identification when issuing an eID. A passport or identity card needs to be shown when applying for a new strong electronic identification method from a bank or telecommunications operator.[34] As the ID-card is not a compulsory document, this legal change resulted in doubling the numbers of ID-card owners.[35]

The Ministry of Transport and Communication is the policy coordinator and responsible for the legislation on eID and trust services. The Finnish Transport and Communications Agency (Traficom) is a supervisory body for eID and trust services. The Ministry of Finance is responsible for steering the Digital and Population Services Agency (DVV) and producing eID policy guidelines for the public sector. The DVV is responsible for the management of the national eIDAS node, the public sector eID portal (Suomi.fi e-Identification) and the national ID card.

eID providers and identity brokers established in EEA-area can notify their services nationally according the Act on Strong Electronic Identification and Electronic Trust Services (section 10 and 11). They are assessed according to the methodology stated in Chapter 4 of the Act on Strong Electronic Identification and Electronic Trust Services (hereinafter the Act). If the eID provider is assessed and accepted by Traficom in the register of strong electronic identification services (section 12 of the Act), it can be used as a means of authentication in government-provided e-services. Traficom is a supervisory body and also has the right to issue more detailed regulations on the assessment criteria to be used in conformity assessments.[36] Traficom also supervises compliance with the national legislation and eIDAS Regulation and keeps the Finnish trusted list.[37]

Authentication is generally deemed to provide sufficient proof of a person's intent online in the public sector. The legislative framework for government services is flexible and there are a few cases for which the applicant is obliged to sign the application before submitting it.

Strong electronic identification also covers the identification of a legal entity or a natural person representing a legal person provided that the means fulfil the requirements of assurance level "substantial" referred to in Article 8(2)(b) of the eIDAS Regulation or assurance level high stated in Article 8(2)(c) of the eIDAS Regulation.[38] So far there are no strong electronic eID means for legal persons available.

DVV has however some certificate services suitable for legal entities. Such kinds of certificates are used by organisations (e.g. hospitals), but the certificates are issued to

[33] Digital Government Factsheet. Finland, European Commission, 2019, p. 12, https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Finland_2019.pdf (accessed 9 July 2020).
[34] Section 7b and 17 of the Act on Strong Electronic Identification and Electronic Trust Services.
See also *As of January 2019, driving license will not be valid as identity proof, read how to get an ID*, https://www.foreigner.fi/articulo/news/of-january-2019-driving-licenses-will-not-be-valid-identity-documents-and-now-what/20181228202911001013.html (accessed 15 July 2020).
[35] Partly due to misunderstanding that drivers licence wouldn't be accepted in any every day face-to-face service, which is not the case.
[36] Section 42 and 42a of the Act on Strong Electronid Identification and Electronic Trust Services. Traficom has issued a regulation (Regulation 72 A/2018) and a Guideline for Conformity assessment (Guideline 211/2019).
[37] Section 42a(4) of the Act on Strong Electronid Identification and Electronic Trust Services.
[38] Section 2 of the Act on Strong Electronid Identification and Electronic Trust Services.

natural persons. The certificates are used to verify a person's identity, meaning that information about their organisation would be added as an additional attribute in the personal certificate. These certificates also make it possible to provide an undisputed electronic signature as defined by law and to provide the authentication of network users and their access rights. They can also include an organisation's valid email address.[39] Signing on behalf of a company is done by natural persons, and there is no special requirement for e-seals.

In general, Finnish legislation does not require the use of electronic signatures. When the legislation refers to the use of electronic signature, there is typically a reference to advanced electronic signatures and often even in these cases some other trustworthy procedures can be used instead of the advanced electronic signature. However, there are some specific situations where an electronic signature of a certain level must be used, e.g. related to electronic prescriptions where an advanced electronic signature with a qualified certificate for the electronic signature must be used.

Other examples where advanced electronic signatures are required by law are:

- in the medical sector:
    - § 7 of the Electronic Prescription Act[40] requires the electronic prescriptions to be signed by advanced electronic signatures with qualified certificate; and
    - blood donator information can be signed by hand or by using advanced electronic signatures as stated in the Blood Services Act (543/2016).
- in the social and healthcare sector, the Act on Electronic Processing of Social and Health Care Customer Data (§ 9) prescribes the use of advanced electronic signatures
- in the energy sector, all energy performance certificates must be signed with advanced electronic signatures as stated in the Act on Information System for Energy Certificates of Buildings.[41]

The task of the DVV is to maintain the national eIDAS node[42] and their root certificate is always contained in a smart card in addition to other certificates.[43] The DVV has some legislated tasks concerning certification services.[44] Also, the private sector can rely on these services according to certificate policies but there is no general obligation nor right for the private sector to do so; certificates for mobile IDs are provided by the telecoms operators themselves as certification authority.

Traficom supervises qualified trust service providers and electronic identification services.[45]

[39] Digital Government Factsheet. Finland, p. 23.
[40] Electronic Prescription Act, https://www.finlex.fi/fi/laki/ajantasa/2007/20070061(accessed 1 October 2020).
[41] *Laki rakennusten energiatodistustietojärjestelmästä* 546/2016.
[42] Section 42c of the Act on Strong Electronic Identification and Electronic Trust Services.
[43] CA Certificates, https://dvv.fi/en/ca-certificates (accessed 15 July 2020). See section 61 of the Act on the Population Information System and the certificates services of the Digital and Population Data Services Agency, https://www.finlex.fi/fi/laki/ajantasa/2009/20090661 (accessed 1 October 2020).
[44] The Digital and Population Data Services Agency is Finland's first and, currently, only provider of signature certificates that are of an acceptable standard. Qualified certificate, https://dvv.fi/en/qualified-certificate (accessed 22 July 2020).
[45] Section 42a of the Act on Strong Electronic Identification and Electronic Trust Services.

4.2.4. Iceland

Iceland implemented the eIDAS Regulation into national legislation with the Act on Electronic Identification and Trust Services for e-Commerce[46] which entered into force on 1 January 2020. Electronic identity schemes are regulated under the same Act. However, the regulation of the Ministry of Industry and Innovation implementing the Act on Electronic Identification and Trust Services for e-Commerce[47] further clarifies the aspects of electronic identification.

Ministry of Finance and Economic Affairs is the policy coordinator of electronic identity and trust services in Iceland.

Section 38 of the Administrative Law[48] in Iceland states that when other laws, directives or practices require a handwritten signature, a qualified signature should be sufficient. Generally, there is no requirement of a qualified electronic signature in Icelandic laws, except for the Registration Act[49] which specifically requires the use of a qualified electronic signature.

Signing on behalf of a company is usually done by natural persons representing a company using an employee certificate.

Supervision over the compliance with the requirements established for trust service providers and authentication service providers is done by the Consumer Agency in Iceland[50]. The supervision covers both qualified and non-qualified service providers. The Consumer Agency in Iceland is responsible for keeping the Icelandic trusted list.[51]

4.2.5. Latvia

The Law of Electronic Documents[52] was adopted in 31 October 2002 and was amended aligning national legislation with the requirements of eIDAS. The amendments became applicable in May 2017.

The Law on Electronic Identification of Natural Persons[53] was adopted on 5 November 2015. The purpose is to prescribe requirements for electronic identification in order to ensure the possibility for a natural person to demand or receive the electronic service provided by a public person while performing the assigned functions or tasks, to regulate the procedures for the registration and supervision of the electronic identification service provider, as well as qualified and qualified increased security electronic identification services. The law regulates type of electronic identification that is equivalent to on-site verification of the identity of a natural person by presenting a personal identification document. The current version of the law defines services as qualified or qualified increased security electronic identification services which are similar to eIDAS "high" and "substantial" with a few

[46] Act on Electronic Identification and Trust Services for e-Commerce, https://www.althingi.is/altext/149/s/1743.html (accessed 6 October 2020).
[47] Regulation on electronic identification and trust services for e-commerce. Ministry of Industry and Innovation, https://www.reglugerd.is/reglugerdir/eftir-raduneytum/atvinnuvega--og-nyskopunarraduneyti/nr/0100-2020 (accessed 6 October 2020).
[48] Administrative Law, https://www.althingi.is/lagas/nuna/1993037.html (accessed 6 October 2020).
[49] Registration Act, https://www.althingi.is/lagas/150b/1978039.html (accessed 6 October 2020).
[50] Section 4 of the Act on Electronic Identification and Trust Services for e-Commerce.
[51] Iceland Trusted List, http://www.neytendastofa.is/library/Files/TSl/tsl.pdf (accessed 6 October 2020).
[52] The Law of Electronic Documents, https://likumi.lv/ta/en/en/id/68521-electronic-documents-law (accessed 20 July 2020).
[53] Law on Electronic Identification of Natural Persons, https://likumi.lv/ta/en/en/id/278001-law-on-electronic-identification-of-natural-persons (accessed 20 July 2020).

modifications and extra requirements. Currently only LVRTC eID services are qualified according to Latvian legislation and the eID mean is notified according to eIDAS as level "high".

The Ministry of Environmental Protection and Regional Development (VARAM[54]) is responsible for e-government, incl. e-identification whereas the State Regional Development Agency[55] runs the eIDAS node.

The Decision on 'Possible financing solutions for the provision of certification services in identity cards (eID) and as a unified and priority means for ensuring a person's electronic identity'[56] was approved by Cabinet of Ministers on 28 August 2018 and submitted to Parliament for enactment on 1 January 2021. On 9 May 2019, the Latvian Parliament approved the law[57] making the identity card (eID card) with activated electronic signature and authentication certificates a mandatory identity document for all citizens from 1 January 2023. The use of the eID will be unlimited and free of charge. The law takes effect from 1 January 2021 which initiates the transitional period.[58] The policy direction is to promote the wider use of qualified services and to use mobile-based solutions as an alternative to the identity card.

A secure electronic signature is electronic data, a unique proof of personal identification attached to a document prepared on the computer (given name, surname, personal code, etc.) or individual signature of a person in an electronic environment having legal effect.[59] It is possible to sign documents using an eID card, an eParaksta card issued to legal persons, or the eParakstsLV mobile app and a mobile phone. Regardless of how you are signing documents, the result will be the same – an electronically signed document with legal effect.[60]

According to the law of electronic documents, state and local authorities shall be required to accept electronically, documents signed with a secure electronic signature (eParaksts) from natural and legal persons, so that any written information or request may be submitted remotely to the national and local authorities using an e-document. Business operators may use eParaksts on a voluntary basis, by mutual agreement, for example for signature of contracts, invoices, submissions and any other type of document separately or by means of recording and accounting systems which incorporate eParaksts' functionality.

The task of the Ministry of Defence[61], which runs the Supervisory Committee of Digital Security[62], is to monitor compliance with the national legislation and eIDAS Regulation.

---

[54] Ministry of Environmental Protection and Regional Development, https://www.varam.gov.lv/en (accessed 20 July 2020).
[55] State Regional Development Agency, http://www.vraa.gov.lv/en/ (accessed 20 July 2020).
[56] § 62 of the Protocol No 60, Minutes of the sitting of the Cabinet of Ministers of the Republic of Latvia, 8. November 2016, http://tap.mk.gov.lv/mk/mksedes/saraksts/protokols/?protokols=2016-11-08 (accessed 20 July 2020).
[57] Digital Government Factsheet. Latvia, European Commission, 2019, p. 6, https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Latvia_2019.pdf (accessed 20 July 2020).
[58] Digital Government Factsheet. Latvia, p 6.
[59] "Secure electronic signature" means a qualified electronic signature. Article 1 of Amendments to the Electronic Documents Law, https://likumi.lv/ta/id/290826 (accessed 24 July 2020).
[60] Signing documents with a secure electronic signature, https://www.latvija.lv/en/DzivesSituacijas/tiesibu-aizsardziba/elektroniskais-paraksts (accessed 24 July 2020).
[61] Latvian Ministry of Defense, https://www.mod.gov.lv/en (accessed 20 July 2020).
[62] Supervisory Committee of Digital Security, https://www.mod.gov.lv/en/nozares-politika/cybersecurity/supervisory-committee-digital-security (accessed 6 October 2020).

The Supervisory Committee supervises not just qualified trust services but also eID service providers. Its mandate comes from the National Law of Natural Person Electronic Identification Law (for electronic identity) and from the Electronic Documents Law (for trust services).

Latvia's trusted list is kept by the Supervisory Committee of Digital Security.[63]

4.2.6. Lithuania

The Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions[64] was adopted on 28 April 2018. This law prescribes the key stakeholders in Lithuania. The Ministry of the Interior is responsible for the eID policymaking, including its implementation and coordination.[65] The Ministry of Transport and Communications is responsible for the policymaking, including its implementation and coordination in the area of trust services.[66] The policy of trust services is implemented by the trust service providers supervisory body assigned by the Government of the Republic of Lithuania, which is Communication Regulatory Authority of the Republic of Lithuania.[67]

Chapter III of the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions defines the legal effect of the electronic signature, electronic seal, and time stamp. Article 5(1) stipulates that "an electronic signature which does not meet the requirements for the qualified electronic signature provided for in the eIDAS Regulation shall have the equivalent legal effect of a handwritten signature, where the users of that electronic signature agree, in writing, in advance and where it is possible to store that agreement on a durable medium". The same applies for electronic seals. This means mostly qualified services are used and if other services are used between the parties, a special agreement should be made.

A qualified electronic signature of a representative of a legal person shall have the equivalent legal effect of a handwritten signature of a legal person authenticated by the stamp of a legal person. It is important to note that the requirement to have a stamp should be established either in a special law or during the establishment of the legal entity[68] (e.g. in the articles of association).

In addition to the legal effect of qualified electronic signatures defined in the eIDAS Regulation, Lithuanian law defines the legal effect of electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services, qualified validation, and preservation services.[69] This seems to be unique among NOBID countries.

Law no. X-239 Amending Article 19 of the Public Administration Act, passed on 9 June 2005, provided the basis for the exchange of electronic documents between the state and municipal institutions, and the public. It stipulated that requests submitted by citizens via

---

[63] Section 1.2 of the By-laws of the Supervisory Committee of Digital Security, https://likumi.lv/ta/en/en/id/286009-by-laws-of-the-supervisory-committee-of-digital-security (accessed 6 October 2020).

[64] The Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions, https://e-seimas.lrs.lt/portal/legalAct/en/TAD/c5174772ecd011e89d4ad92e8434e309 (accessed 21 July 2020).

[65] *Ibid*, article 3 (1).

[66] *Ibid,* article 3 (2).

[67] *Ibid,* article 3 (3).

[68] Article 5(4) of the Law of the Republic of Lithuania on Electronic Identification and Trust Services for Electronic Transactions.

[69] *Ibid,* chapter III.

electronic means shall be signed using an electronic signature. Furthermore, all answers of state institutions towards citizens shall be signed by the head of the public administration institution concerned, or a person authorised, by means of an advanced electronic signature.[70]

According to the interviews, there are no clear requirements to operate as an identity or authentication provider in Lithuania. The role for policymaking lies with the Ministry of Interior, but the specific requirements have not been applied.[71] The Ministry of Interior is also responsible for the operation of the eIDAS node.

Lithuania has notified its eID scheme (Lithuanian National Identity card (eID/ATK) to the European Commission on 21 August 2020.[72]

The Communications Regulatory Authority of the Republic of Lithuania[73] (RRT) is the independent regulator of the electronic communications, postal, rail markets and trust services, also keeping the Lithuanian trusted list[74]. The Order of the director of the RRT "on the approval of the specification of the procedure for granting the status of qualified trust service providers and qualified trust services and incorporation thereof in the national trusted list and provision of activity reports of qualified trust service providers"[75] defines the rules for becoming a qualified trust service provider in Lithuania.

4.2.7. Norway

The Act on Electronic Trust Services is in force since 15 June 2018.[76] This is the act that incorporates eIDAS into Norwegian law.

The Public Administration Act stipulates that whenever there is a requirement for something to be in written form, this includes the electronic format.[77] The Public Administration Act enables the King to prescribe regulations relating to the electronic communication between

---

[70] Digital Government Factsheet. Lithuania, European Commission, 2019, p. 11, https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Lithuania_2019_0.pdf (accessed 21 July 2020).

[71] Although the requirements how to classify providers of e-identification (low, substantial, high) are provided by the Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (OJ L 235, 9.9.2015, p. 7–20), Lithuania is planning to have a national level legislation. Currently it is still being discussed. Lithuania has finished a policy level document to define the methodology how to classify e- services in accordance with requested level of identifications means (low/substantial/high).

[72] Electronic identification schemes notified pursuant to Article 9(1) 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, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020XC0821(01)&from=EN (accessed 6 October 2020).

[73] Lithuanian qualified trust services and their supervision, https://elektroninisparasas.lt//indexen (21 July 2020).

[74] Trusted List of the Republic of Lithuania, https://elektroninisparasas.lt/trusted-service-list (accessed 6 October 2020).

[75] Order of Director of the Communications Regulatory Authority of the Republic Of Lithuania on the approval of the specification of the procedure for granting status of qualified trust service providers and qualified trust services and incorporation thereof in the national trusted list and provision of activity reports of qualified trust service providers, 21 June 2018 No 1V-588, Vilnius, https://e-seimas.lrs.lt/rs/legalact/TAD/845ca520ed5411e89d4ad92e8434e309/ (accessed 7 October 2020).

[76] The Act on Electronic Trust Services, LOV-2018-06-15-44, https://lovdata.no/dokument/NL/lov/2018-06-15-44?q=elektronisk%20signatur (accessed 7 October 2020).

[77] Section 2 of the Public Administration Act , LOV-1967-02-10, https://lovdata.no/dokument/NLE/lov/1967-02-10?q=electronic (accessed 7 October 2020).

the public administration and the general public when it concerns signing and authentication.[78]

Norwegian law has few references to the use of signatures. In many cases, established practice is that the use of eID for authentication is equal to signing if it is used in conjunction with audit logs from the service provider. In addition, several service providers in the market support advanced electronic signatures based on authentication. In many cases, authentication using an eID at level "high" is sufficient to meet the requirements of a signature.

One of the cases that require signing is the processing of medical data by health professionals. The Prescription Mediator Regulations[79], for example, stipulate that all messages sent to the Prescription Intermediary (i.e. national database for electronic prescriptions) must be electronically signed in the manner determined by the Norwegian Health Network and in accordance with the Electronic Signature Act (§ 2-4). This means in practice that advanced electronic signatures with a qualified certificate must be used by relevant medical staff. In addition, the messaging system used for the health care sector requires all messages to have an electronic seal for the legal organisation of the health care professional that has signed.

The commonly used electronic signature or seal level in Norway is "advanced electronic signature or seal with qualified certificate", reflecting that none of the issuers of qualified certificates have a solution that supports qualified signature creation devices.

The Norwegian Communications Authority is responsible for keeping the Norwegian trusted list.[80]

Norwegian Digitalisation Agency (Digdir)[81] is responsible for the common national IT-components[82] and the operation of the eIDAS node. These components must be used by all public organisations and deviations must be documented.

4.2.8. Sweden

Sweden implemented the eIDAS Regulation to national legislation in 2016 when the Law with Supplementary Provisions to the EU Regulation on Electronic Identification[83] as well as the Regulation with Supplementary Provisions to the EU Regulation on Electronic Identification came into force.[84]

---

[78] Section 15.a of the Public Administration Act.
[79] Regulations on the processing of health information in the national database for electronic prescriptions (Prescription Mediator Regulations), FOR-2007-12-21-1610, https://lovdata.no/dokument/SF/forskrift/2007-12-21-1610 (accessed 7 October 2020) See also the Act on Electronic Trust Services.
[80] Norewegian Trusted List, https://tl-norway.no/TSL/NO_TSL.PDF (accessed 21 July 2020).
[81] Norwegian Digitalisation Agency, https://www.digdir.no/ (accessed 7 October 2020).
[82] Such as national ID-gateway providing agencies in Norway with a log-in solution, eSignature, eDelivery, national digital mailbox.
[83] The Law with Supplementary Provisions to the EU Regulation on Electronic Identification, 2016:561, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2016561-med-kompletterande-bestammelser_sfs-2016-561#:~:text=1%20%C2%A7%20Denna%20lag%20kompletterar,EU%3As%20f%C3%B6rordning%20om%20elektronisk (accessed 7 October 2020).
[84] Regulation with supplementary provisions to the EU regulation on electronic identification, 2016: 576, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2016576-med-kompletterande_sfs-2016-576 (accessed 7 October 2020).

Electronic identity schemes are currently unregulated in Sweden. Instead, there is a quality framework called "*Svensk e-legitimation*" provided by the Agency for Digital Government (DIGG).[85]

The responsibility of eID and trust services is distributed between the Swedish Post and Telecom Authority (PTS) and DIGG. PTS is responsible for the policy coordination of (qualified) trust services and maintaining the Swedish trusted list[86], whereas DIGG has the co-ordinating role for e-government initiatives, including eID which is one of the horizontal services.

Although Sweden has not notified its eID schemes to the European Commission, the use of BankID is widespread. DIGG coordinates the Swedish open eID system by publishing eID specifications upon which all service providers meeting the specifications can become a signatory to a contract in order to provide public sector with their service. DIGG supports the public sector with effective contracts (*Valfrihetssystem*) alongside the federated infrastructure Sweden Connect. Sweden Connect consists of:

- a technical framework that describes how connecting services and e-identification publishers must behave in order to work;
- an actor registry where services and e-identification issuers register contact information and SAML metadata;
- the Swedish eIDAS node.[87]

Besides the aforementioned points, DIGG is responsible for participation in the eIDAS Cooperation Network and issuing the Swedish eID quality mark when reviewing eIDs conforming to the Swedish national eID trust framework.

In terms of supervision of eID, DIGG does not have a formal role as supervisor of eID, however, it advises public agencies on conducting the contracts with vendors. Supervision over the compliance with the requirements established for trust service providers is done by PTS as per the Regulation with Supplementary Provisions to the EU Regulation on Electronic Identification. The supervision concerns all service providers.

5. Overview of the trust services landscape in NOBID countries

This section presents the overview of the trust services landscape (section 5.1) together with country-specific information and details on the use of trust services and alternatives thereof (section 5.2). This section also investigates the cross-border electronic services and how trust services are used in the offering thereof (section 5.3). This section 5 has been created on the basis of the interviews conducted (see Appendix A: Interviewees) in conjunction with desk research carried out by the project team.

5.1. Overview of the trust services and alternative trust services in NOBID countries

This section gives an overview of the trust services landscape in the NOBID countries.

[85] *Kvalitetsmärket Svensk e-legitimation*, https://www.digg.se/digital-identitet/e-legitimering#kvalitetsmarket_svensk_e-legitimation (accessed 7 October 2020).
[86] Swedish Trusted List, https://trustedlist.pts.se/ (accessed 7 October 2020).
[87] Sweden Connect, https://swedenconnect.se/om-sweden-connect.html (accessed 7 October 2020).

5.1.1. Overview

Trust services in general, as they are offered in NOBID countries, fall into the following categories:

- Qualified trust services present in the Trusted List;
- Non-qualified trust services present in the Trusted List;
- Services, that might be similar in nature to the services appearing in the trust list whose status has not been confirmed by certification.

From the market overview perspective, a trust service provider is a company offering either trust services as defined in the eIDAS Regulation[88] or a provider of alternative trust services. To further focus the study with regards to the research questions at hand, the following additional limitations are set:

- Only organisations competing on the open market are included in the study as the goal is to understand the market forces present. While a government-owned company might provide trust services in a country, their focus is dictated by their owner's natural focus on the local market.
- Appearance on the Trusted List provides organisations with considerable capabilities to provide their services beyond national borders without explicit effort. Thus, such organisations are considered part of the market study regardless of their market focus.
- Service providers focused on servicing a local market only and not appearing on the Trusted List are excluded for two reasons. Firstly, the focus of the current study of trust services is regional in nature, thus a local provider does not contribute significantly to this perspective. Secondly, local service providers with a potentially relatively limited lifespan are exceedingly complex to spot for an outsider as they might be focused, for example, only on providing services to a national tax authority or a specific municipality.
- Service providers headquartered or notified outside of the NOBID region are excluded from the study. Although the use of such services was noted by several interviewees, it was also commonly noted, that the use of such services is difficult to quantify. For example, global corporations commonly standardise the internal use of trust services. Which services are used by all local branches of all multinational companies and to what extent is effectively impossible to gauge.

Given these limitations, a list of market participants was compiled (see Table 4 in Appendix B: The market of trust services and alternatives thereof in NOBID countries). As banks and telecom operators take an active role in the development of the market in most of the NOBID countries, the list contains several companies whose main business focus is decidedly elsewhere.

The most significant conclusion from the list is the decidedly international nature of trust services and alternatives thereof as most service providers offer their services in several NOBID countries. That said, services provided vary from country to country. For example, SEB and Swedbank provide authentication services in the Baltics and participate in the QTSP

[88] Organisations operating a signature creation device or creating AdES signatures based solely on the Remote QSCD family of standards (ETSI TS 119 431) are considered QSCD providers rather than trust service providers by the current eIDAS regulation. Although these service providers are, based on standards, effectively operating a trust service, a function provided to the end consumer is that of a QSCD device.

market via SK ID Solutions AS co-owned with Telia, however neither participates in the Finnish trust network despite business presence. Nets and Visma are other examples of companies operating widely in the region offering country-specific services. SK ID Solutions, however, is a counterexample operating in all three Baltic states with a virtually identical product offering. Signicat offers federated authentication and signing services in Norway, Sweden, Denmark, and Finland, but also covers the Baltic countries for both authentication and signing while further offering cross-border use of eIDs and integrated signing solutions. Also, companies often have business presence in a country without offering trust services or alternatives thereof despite doing so in other countries. This seems to indicate companies operating in the region do have the potential to support interoperability having both market presence and technology but experience barriers to that effect.

5.1.2. The landscape of trust services and alternatives thereof in NOBID countries

From the perspective of trust services as defined by the eIDAS Regulation, the market situation is more nuanced, clearly indicating a wide variety of national and business strategies in implementing the eIDAS Regulation.

Norway stands out with the greatest number of qualified service providers, as all members of the BankID scheme must obtain qualified status as a trust service provider. Lithuania, in turn, is the country with the largest variety of trust services offered. Denmark has only one trust service provider that has not obtained a "qualified" status. This is likely due to the government driven NemID dominating the market and the regulations not requiring the use of qualified signatures. The reasons for the lack of trust service providers is different in Iceland. While the market will certainly develop, the progress is unlikely to yield a proliferation of Icelandic trust services due to the small size of the market.

In terms of services, the qualified certificate for electronic signatures is the most popular service in terms of offerings observed. This aligns with the notion, that identification of an individual is treated as closely related to a given national context while less personalised services, like QWAC, can be obtained from the open market with ease. This leads to QWAC and validation services being the least popular offerings having been declared to operate in two countries only. There are no preservation or electronic registered delivery services from NOBID countries in the Trusted List. However, the existence of various non-qualified e-delivery services was mentioned repeatedly, e.g. Swedish Kivra and Mina Meddelanden services. Also, Signicat, Scrive and other electronic signing service providers as well as document workflow providers offer non-qualified preservation services currently not appearing on the Trusted List.

Table 1 provides an overview of the Trusted List service providers by their type.

Name	Country	Type of services
Nets DanID A/S	Denmark	Cert for ESig
Digital and Population Data Services Agency	Finland	QCert for ESig, QWAC
Auðkenni	Iceland	QCert for ESig
Bankenes ID-tjeneste AS	Norway	QCert for ESig
Commfides Norge AS	Norway	QCert for ESig, QCert for ESeal
Danske Bank	Norway	QCert for ESig
Nordea Bank Abp filial i Norge	Norway	QCert for ESig
SpareBank 1 Utvikling DA	Norway	QCert for ESig
Buypass AS	Norway	QCert for ESig, QCert for ESeal, QWAC
DNB Bank ASA	Norway	QCert for ESig
Eika Gruppen AS	Norway	QCert for ESig
Signicat AS	Norway	QTimestamp
TrustWeaver AB	Sweden	QVal for ESig, QVal for ESeal
ZealID AB	Sweden	QCert for ESig
GuardTime OÜ	Estonia	QTimestamp
SK ID Solutions AS	Estonia	QCert for ESig, QCert for ESeal, QTimestamp
Latvian State Radio and Television center	Latvia	QCert for ESig, QCert for ESeal, QTimestamp
Identity Documents Personalisation Centre under the Ministry of the Interior	Lithuania	QCert for ESig
State Enterprise Centre of Registers	Lithuania	QCert for ESig, QCert for ESeal, QTimestamp
UAB Dokobit	Lithuania	QVal for ESig, QVal for ESeal
UAB BalTstamp	Lithuania	QTimestamp

Table 1. Trusted List members and their services in NOBID countries

As for the notified authentication schemes (see Table 2), four countries have notified the European Commission of their schemes. Norway, Sweden and Finland mostly rely on a multitude of commercial eID providers accepted by the government. This complicates notification as a large number of private services must be notified about in a non-discriminatory manner.

	Level	Scheme
Denmark	Substantial	NemID
Estonia	High	ID-Card, RP card, Digi-ID, e-residency Digi-ID, Mobile-ID, diplomatic identity card
Finland		
Iceland		
Latvia	High, Substantial	eID karte, eParaksts
Lithuania	High	National Identity Card
Norway		
Sweden		

Table 2. Notified electronic identification schemes[89]

The relatively small size of many of the NOBID countries, openness of the European market of trust services and the reluctance of countries to relinquish control of personal identity has led to some interesting phenomena in the region. Issuance of strong electronic identities should have minimal external dependencies while trust services can easily be procured from the international market. In several cases (Estonia, Iceland, Latvia), this in conjunction with a small market size has led to one dominant trust service provider other market participants need to rely upon. Dependence on a singular source of trust, however, has proven to be dangerous in Estonia[90] and the need for the population to have at least two independent authentication and signature creation devices was expressed in interviews with the Latvian State Radio and Television Center.

The overview of the trust services as defined in the eIDAS Regulation offered in NOBID countries is described in Table 3.

	Denmark	Estonia	Finland	Iceland	Latvia	Lithuania	Norway	Sweden
Cert for Esig	X							
QCert for Esig		X	X	X	X	X	X	
QWAC			X				X	
QCert for Eseal		X			X	X	X	
QTimestamp		X			X	X	X	
QVal for Esig						X		X
QVal for Eseal						X		X

Table 3. Trust services offered locally in NOBID countries

In addition to the trust services as defined by the eIDAS Regulation, other trust-related services are clearly offered in the NOBID region market.

What stands out is the presence of various bank-ID-s in NOBID countries. Banks have commonly pooled their authentication devices and customer bases to provide electronic identity services to each other as well as third parties. It is remarkable, however, that these systems have all taken a very different approach to providing these functions. Baltic banks have an identity federation standard (called BankLink[91]), that is much more loosely defined, lacks government support and can also provide payment services. Finland, meanwhile, has a very strongly regulated trust network encompassing not only banks but other identity providers like telecom providers. Norway and Sweden have taken an approach between these. The main trust service provider in Iceland, Auðkenni, was founded by Icelandic banks who remain the largest shareholders with registration services available in all bank branches.

[89] Electronic identification schemes notified pursuant to Article 9(1) 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, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020XC0821(01)&from=EN (accessed 7 October 2020).

[90] ROCA Vulnerability and eID: Lessons Learned, Estonian Information System Authority, https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf (accessed 7 October 2020).

[91] Specification of BankLink, https://pangaliit.ee/arveldused/pangalingi-spetsifikatsioon (accessed 7 October 2020.

Another apparent feature of the services is the extent to which the Baltics emerge as one unit of management: SK ID Solutions (owned by SEB, Swedbank and Telia) operates across all Baltic States with minor deviations. The BankLink standard, although governed by the Estonian Banking Federation, is commonly used by banks and public sector entities in all Baltic States, and equally Dokobit has a clear focus on the Baltics. This grouping likely stems from the fact that all major telecom and financial institutions treat the Baltic states as one singular business unit with minimal local specialisation.

The Baltic states stand apart from other NOBID countries also in terms of the approach to identity carriers. In Estonia, Latvia, and Lithuania the government supplies the citizens with QSCD devices. In addition, SK ID Solutions is active in the market and provides a mobile-based QSCD. In conjunction, this means that a significant portion of electronic identity users can issue qualified signatures. Even if QSCD devices are issued in other NOBID countries, they are not widespread with non-cryptographic identity means reliant on alternatives to those trust services dominating the markets.

The Nordic Institute for Interoperability Solutions (NIIS) stands out from among the other service providers. It develops the functional core of X-Road, a non-qualified e-delivery-like service used by Estonia, Finland, Iceland, and the Faroe Islands with each country operating their own extended instance of the core solution. On one hand, NIIS is not a typical private sector market actor.[92] On the other, it is international in nature working actively to expand its partnership network within the NOBID countries and outside of it.

5.2. Country-specific view on trust services and alternatives thereof

This section provides a country-by-country overview of the trust services as well as alternatives used in each NOBID country as well as their use.

5.2.1. Denmark

The market of trust services and their alternatives is dominated by the NemID scheme supplied by Nets DanID A/S. The scheme is supervised by the Ministry of Finance, via the Agency of Digitisation.

There are no qualified service providers in Denmark, but Nets DanID A/S is part of the Trusted List as a provider of non-qualified certificates of electronic signatures. Also, NemID as an authentication scheme has been notified to the European Commission on the assurance level "substantial".

That said, several non-qualified providers such as Penneo, DocuSign, Cryptomathic, Signicat operate in the market with Penneo and Cryptomathic headquartered in Denmark and offering their services in other NOBID countries. Varying levels of electronic signatures, signature validation, e-seals and time stamping services are offered by these providers.

Commissioned by the government and the Banking Association, the identity infrastructure is in the transition phase as NemID will be phased out and replaced with a different architectural set-up called MitID. MitID will only provide eID and authentication.

[92] The non-profit organisation Nordic Institute for Interoperability Solutions (NIIS) is an organization acting in public interest and was estabished by the Republic of Estonia and the Republic of Finland. Memorandum of Association, https://static1.squarespace.com/static/59ba41ee64b05fd6531f498d/t/59d1e536914e6b6e0ec0d048/1506928747397/Memorandum+of+Association+of+NIIS+signed_EN.pdf (accessed 28 July 2020).
History of NIIS, https://www.niis.org/history (accessed 28 July 2020).

Infrastructure for employee (corporate) identity and overall eID cycle administration will also be provided as well as an electronic signature solution providing qualified signatures for private people and businesses.

In Denmark, non-qualified certificates created in the context of the NemID scheme are commonly used in communication between private enterprises and public authorities. The NemID infrastructure includes identification for citizens, public authorities, private businesses and their employees. NemID is thus both used to document the user's identity as well as to sign documents digitally. For private use, authentication (mostly using NemID) is usually legally sufficient to prove one´s intent online.

Approximately 5.1 million Danish citizens use NemID[93], more than 55 million transactions are conducted monthly. It is used by citizens and in professional use by businesses who need NemID to log in to public portals, private digital services including online banking, and to access digital mailbox provided by the public authority. The NemID follows the national OCES standard.[94] All companies must have digital identity and account to report taxes.[95] In organisational setting, around 489 000 companies and more than 1,2 million employee certificates have been issued.[96] OCES certificates are currently only issued by Nets DanID A/S.

The use of NemID as an authentication means is mandatory. NemLogin as the authentication portal will be mandatory for public digital services with the coming legislation. NemLogin provides authentication and single-sign-on as well as a power of attorney solution.[97]

For a private individual, NemID can only be obtained based on a Danish CPR number and is free of charge. The CPR number is issued in the citizen service centres and requires physical presence.

The Danish eIDAS-infrastructure, the eID-gateway, consists of the eIDAS Connector and eIDAS Service. Work is ongoing to integrate notified eIDs into the existing infrastructure. The eID-gateway is connected to several digital services by the means of an existing national SAML-based protocol. By the end of 2019, citizens from seven different EU Member States were able to access Danish digital services through the Gateway.[98]

The Danish Business Authority hosts the Danish government's point of single contact, Business in Denmark, for foreign service providers from other EU/EEA countries with business activities in Denmark. Here, service providers can obtain information about procedures and formalities relating to access to a service, and complete registrations.[99]

5.2.2. Estonia

The Estonian market of trust services is dominated by SK ID Solutions AS, qualified provider of certificates for e-signatures and e-seals and timestamps. SK ID Solutions also operates the SIM-based mID identity carrier and the app-based SmartID, both of which are certified as qualified signature creation devices. SK ID Solutions has also been contracted to work on various other elements of government-operated trust services like software for desktop-

[93] Statistics of NemID, 09.07.2020, https://digst.dk/media/22379/nemid_statistik_ekstern_rapport_juni_2020.pdf (accessed 7 October 2020).
[94] Trusted Service List (TSL) Denmark, Specific information, https://en.digst.dk/digitisation/eid/trusted-list/ (accessed 7 October 2020).
[95] Next generation NemID, https://en.digst.dk/digitisation/eid/next-generation-nemid/ (accessed 7 October 2020).
[96] About Danish Digital Signature (OCES), https://developer.signicat.com/id-methods/danish-digitial-signature-oces/ (accessed 7 October 2020).
[97] Nordic digital identification, 2016, p. 17.
[98] Digital Government Factsheet. Denmark, p. 27.
[99] *Ibid,* p. 25.

based signature operations. SK ID Solutions (owned by SEB, Swedbank and Telia Estonia, all active in all three Baltic states) positions itself as a Baltic company rather than a strictly Estonian one and is active in all three Baltic states.

Guardtime[100] has been providing timestamping services using its proprietary technology and was part of the Estonian trust list since before eIDAS Regulation was adopted. Recently it has also acquired the qualified status as a timestamping provider. Estonia-based identity provider Agrello.id[101] provides an electronic signature platform rooted in blockchain technology. Both companies clearly target international customers but their foothold in the NOBID region is unclear.

The Estonian government funds development and operation of two identity carriers capable of both qualified electronic signature and authentication: the ID-card and SIM-based mID with SK ID Solutions acting as the CA in both cases and as the operator for mID. Both eID means are notified to the European Commission on the level "high". In addition to funding qualified trust services, the Estonian government also offers non-qualified signature validation services and provides DigiDoc software allowing signature operations on PC and Mac desktop platforms. Major elements of the eID infrastructure are available as open source software.[102] Finally, the Estonian government operates an e-delivery-like service called X-Road reliant on an in-house qualified certificate authority.[103] The service is in massive use by public sector organisations using it to altogether exchange more than one billion messages annually with public and private sector organisations.[104] A central government-provided authentication service called TARA is provided to be used by public sector.

The trust services market cannot be said to be fully matured. Firstly, services like QWAC are not offered locally, despite clearly required by local companies (especially in the context of PSD2). Also, Estonia does not have its own trusted time source, a foreign vendor is used for this. Secondly, the market is dominated by one player, SK ID Solutions. However, with an open EU market and few limitations on the use of alternatives to trust services in a corporate setting (DocuSign and AdobeSign have been mentioned), the relative lack of market maturity matters little as trust services are commonly procured from the open market outside of Estonia. All major stakeholders of the market are international in terms of service focus, owned by foreign companies, or both. Thus, the local market opportunity is limited and can possibly only accommodate niche providers like Guardtime.

In Estonia, various forms of electronic identity are in common use. For all citizens from the age of 15, the certificate-containing ID-card is mandatory.[105] The capability to use trust services does not, however, lead directly to any actual use of them. About 10% of ID-cards with valid certificates have never been used in any online scenario, while another 10% have used them only once. About 65% of the user base can be considered heavy users as of December 2019.[106]

---

[100] Guardtime, https://guardtime.com/ (accessed 7 October 2020).
[101] Agrello, https://www.agrello.id/ (accessed 7 October 2020).
[102] Estonian Electronic Identity Software, https://github.com/open-eid (accessed 7 October 2020).
[103] Section 9 of the *X-Road Regulation*, RT I, 06.08.2019, 17, https://www.riigiteataja.ee/akt/106082019017.
[104] Interoperability services, e-Estonia, https://e-estonia.com/solutions/interoperability-services/x-road/ (accessed 7 October 2020).
[105] Section 5(2) of the Identity Documents Act, RT I, 31.01.2020, 14, https://www.riigiteataja.ee/en/eli/504022020003/consolide (accessed 7 October 2020).
[106] Statistics from Estonian Information System Authority, issued on request.

There are about 14 million authentications per month and 24 million qualified electronic signatures issued every month in Estonia. The use of mobile devices in an eID context is on the rise. Around 230 000 people have active mIDs and around 500 000 people possess an active Smart-ID. Both these figures have been rising constantly since the roll-out of the services.[107]

In addition to service provisioning, identity is seen as a prerequisite of privacy as without a strong identity it is hard to identify the person who should be in control of data. This means many services, especially in the public sector, use electronic identity not necessarily as a means for service delivery but as a method to hand control (and thus responsibility) for data and services over to the citizen.

Mostly, eID means of level "high" are used for authentication. The use of lower level means is mostly driven by customers from 3rd countries. For example, the Tax and Customs Board supports lower levels of authentication for cross-border service provisioning. In the education sector, username and password-based authentication schemes (linked to the same identity code as is used for higher-level schemes) are used because of difficulties with underage children acquiring and using qualified-level authentication devices.

In addition to using the centrally deployed eIDAS node, several services (Tax and Customs Board, Business Registry etc.) are supporting certain identity schemes by neighbouring countries directly. In the future, the goal is to migrate these point-to-point integrations to the eIDAS node.

In addition to trust services, alternative authentication services are widely offered. All present major banks offer their own non-cryptographic authentication mechanisms, typically PIN calculators. These mechanisms are commonly federated via a mechanism called BankLink governed by the Estonian Banking Association. As most banks in Estonia operate in all Baltic states, the use of this standard has spread to Latvia and Lithuania as well. In the Estonian public sector, the use of Banklink is trending down as organisations migrate to the centrally provided state authentication service and banks move their customers off proprietary authentication methods like PIN calculators.

Cross-border use of Estonian electronic services and identity means remains negligible: Estonian services are used by EU citizens a few hundred times a month and there are a few thousand cases of attempting to use foreign electronic services with Estonian identity means.[108]

5.2.3. Finland

The Digital and Population Data Services Agency (DVV), a government entity, is the only qualified trust service provider in Finland. It provides qualified certificates for electronic signatures as well as QWAC. In addition to supplying the certificates, the agency also supplies the software infrastructure for those certificates to be used in conjunction with the Finnish identity card containing them.

Only the government-issued ID-card is certified as a QSCD, therefore mostly non-qualified electronic signatures are issued. The non-qualified advanced electronic signature is the most common trust service with electronic prescription being the most common use case.

[107] Statistics from Estonian Information System Authority, issued on request.
[108] Statistics from Estonian Information System Authority, issued on request.

There are no authentication schemes notified or pre-notified to the European Commission. There are registered and supervised eID providers and identity brokers according to the Act on Strong Electronic Identification and Trust Services. These registered services constitute a regulated Finnish Trust Network (FTN). The eID means providers are 10 separate Bank ID providers or provider consortiums, 3 Mobile ID providers and DVV. Many Bank ID or Mobile ID providers also offer brokers services and there are 2 broker services without their own eID means services. The point of the FTN regulation in the Act is the legal compulsion for eID providers to enter into a contract with broker services so that the brokers can provide aggregated identification services for online services. Without FTN regulation the online services were forced to enter into a contract with all the eID means providers whose customers they wished to authenticate.

Service providers are not allowed to connect directly to the eID providers, instead they must connect via a broker, which provides a federated identity service. Several service providers offer broker services in the market subject to passing third-party audit and under supervision by Traficom.

The eID means providers and identity brokers of FTN as well as other providers provide electronic signatures based on strong electronic authentication and audit trails. The FTN is a regulated network of identity providers and brokers assessed according to eIDAS assurance levels.[109] Only four of these providers are not banks, making the FTN similar in concept to the Bank IDs of Norway and Sweden. However, the approach taken in Finland is different as the networks in Norway and Sweden are controlled by privately owned legal entities rather than dedicated regulation and they mediate only identities managed by the financial sector.

In terms of non-qualified services, a variety of services (timestamping, web certificates, e-delivery etc.) are offered. Telia, Signicat, Visma, Signom, Avaintec and others provide trust services or alternatives thereof. Visma, for example, provides a signing platform (also used by some public sector organisations) where the signing process relies on audit logs in addition to authentication based on username and password. Signature validity is confirmed using meta-data without the user being able to validate signatures directly. In case of some of the signature providers, the certificate of the service provider is used in signing making them similar to a sealing service.

For the public sector, the volume of authentications using bank ID, mID or identity card is approximately 140 million transactions annually. There are 13 private eID providers – all being widely used in public and private services, but there is so far little commercial interest in notifying the scheme(s) to the European Commission. The authentication solutions used and brokering services are being assessed according to the Act on Strong Electronic Identification and Trust Services and secondary regulation that those are compatible with eIDAS levels and the list is made publicly available in the registry stipulated in the same Act (Register of identification service providers).[110] All private eID means providers are being contracted by the government and can be used in accessing government services, so can the only public provider in the FTN operated by the DVV. One of the key methods of doing

[109] Electronic identification, https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification (accessed 7 October 2020).

[110] Register of identification service providers (*Tunnistuspalvelurekisteri*), https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tunnistuspalvelurekisteri_01062020.XLSX (accessed 7 October 2020).

so is using the central government-operated authentication and information service suomi.fi.

Bank ID, consisting of interoperable eID solutions of 10 individual banks, is the most common eID. Mobile based solutions are provided by the mobile operators. Many people have an identity card that has an authentication and qualified electronic signature certificate in it, but is not as widely used as Bank ID.

The use of qualified electronic services in private use is reportedly very low (about 2 million signatures per year according to interviewees). However, there are professional scenarios where the use of advanced electronic signatures is widespread. One example of this is the medical sector (see 4.2.3 above). The use of advanced electronic signatures amounts to 30 million per year and dispenses by the pharmacy (for this, advanced electronic signatures with qualified certificates is required) amount to 67 million per year.

There are more than 140 million transactions per year in the suomi.fi authentication service offered by DVV. The authentication service incorporates both identity solutions offered by banks or mobile operators via the FTN as well as the DVV certificate card options. This statistic is limited to authentication and does not cover signing. The use of the eIDAS node receives about 1000 authentication cases per month, most of which are initiated from neighbouring Estonia.

5.2.4. Iceland

Auðkenni is the only locally operating trust service provider in Iceland. Its focus is on CA services providing qualified certificates, but it also offers physical tokens in the form of a chip card, SIM-based tokens as well as software to use these tokens for authentication purposes. An app based QSCD offering, based on the SmartID technology supplied by SK ID Solutions AS, is being implemented with the planned launch before end of 2020. Auðkenni is a qualified service provider in terms of certificates for electronic signatures and is in process of acquiring the status for electronic seals. Due to the small size of the market and easy access to the global trust services market and the eIDAS trust context, investment in competition between trust service providers is unlikely to pay off. That said, Lithuania-based Dokobit operates in the market offering qualified validation services for electronic signatures.

Iceland has neither notified nor pre-notified authentication schemes to the European Commission, although plans to do so were expressed.

Two competing authentication solutions exist on the market: a government-issued service called IceKey and the PKI-based solutions provided by Auðkenni.

IceKey was introduced in 2013 and can be used at over 200 companies, organisations, municipalities and other public and private bodies. As of November 2019, 290 978 private persons and 18 126 legal entities have been issued IceKeys.[111] However, Skatturinn, the Icelandic tax and customs office, banks and many other service providers do not accept IceKey. The solution is based on passwords but can be augmented with a SMS-based OTP.

[111] Login service statistics, https://vefur.island.is/en/indentification-services/login-service-statistics/ (accessed October 2020).

Around 250 thousand people have mobileID and/or eID card linked to certificates issued by Auðkenni. These eID´s can be used in the majority of online services in Iceland, including banks and Skatturinn.

Iceland is a partner at NIIS and uses the non-qualified e-delivery-like service X-Road between public sector organisations.[112]

While electronic signing is used, services rely mostly on authentication. That said, general eID adoption in Iceland is high and the usage has apparently grown during the COVID-19 pandemic.

Electronic ID usage has been driven mainly by online banking services and the central authentication portal iceland.is. The latter supports both Icekey and PKI-based eID schemes and is seeing a rapid growth in use. For example, there were 739 474 authentication events via the portal in October of 2018 and 1 635 238 in October of 2019, representing a 121% growth.[113]

The most commonly offered trust service is the qualified e-seal while the most common alternative trust service is electronic authentication.

5.2.5. Latvia

In the Latvian market, there are three main trust providers. Firstly, the state joint-stock company Latvian State Radio and Television Center (LVRTC) provides qualified certificates for electronic signatures and seals as well as qualified timestamping services. In addition to issuing certificates, LVRTC also provides the main government-issued electronic identity carrier in the form of an ID-card. Secondly, Estonian-based SK ID Solutions operates a branch located in Riga, Latvia. The product offered by the company is the same app-based QSCD-certified solution SmartID that is offered in Estonia and Lithuania. Dokobit, active in the market both directly and via integrators, is the third QTSP in the market offering qualified validation services.

Latvia has notified the European Commission of one identity scheme with four means. Three of these are on the level "high" and one (a mobile solution storing the private key of the user in the secure enclave of the device) on the level "substantial".[114] A central authentication gateway integrated with the eIDAS node is operated by the State Regional Development Agency. BankLink is commonly used by both private and public sector entities for identity federation.

The overall trust services market can be characterised as emerging. Organisations have commonly used internal tooling and trust solutions to preserve integrity of records and to authenticate users. A significant shift of such solutions to use external trust service providers is relatively recent caused, in case of banks, by the PSD2 Directive.

The COVID-19 pandemic has caused a significant increase in the use of electronic identity and signatures. User knowledge, competence and practical needs are all stated as barriers to the use of trust services. After being forced to switch to electronic processes by the

[112] Iceland becomes a partner of the Nordic Institute for Interoperability Solutions, https://www.niis.org/newsroom#/pressreleases/iceland-becomes-a-partner-of-the-nordic-institute-for-interoperability-solutions-2680217 (accessed 7 October 2020).

[113] Login services Ísland.is and Íslyklar in October 2019, https://skra.is/um-okkur/frettir/frett/2019/11/01/Innskraningarthjonusta-Island.is-og-Islyklar/ (accessed 7 October 2020).

[114] Opinion No.7 of the Cooperation Network on the Latvian eID scheme, https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=148898039 (accessed 7 October 2020).

pandemic, users are seeing the benefits and are reluctant to switch back to paper-based processes.

The PSD2 Directive has provided a strong incentive for banks to move from bespoke authentication methods to standardised and shared ones.

As the government-issued ID-card is not yet mandatory, the enterprises have faced challenges in implementing strong authentication and signatures. Those users that do not have an authentication device cannot be mandated to acquire one from the government and need to be issued one by the organisation. However, the recent developments show that there is strong support from the government to make the acceptance of national eID means mandatory by both sectors. That said, currently the government agencies already support ID-card based electronic signatures which can be used for filing taxes, for example.

The dominant government-issued ID-card uses separate lifecycles for the physical identity document and the certificates it contains. Currently, the ID-card is not a mandatory document. This will change from 1 January 2023 (see 4.2.5). This leads to only about half the population having the ID-card of whom about half have a card with active certificates. This means about 500 000 cards with active certificates can currently be used.

5.2.6. Lithuania

Lithuania has the largest variety of qualified trust services offered locally among the NOBID countries. Lithuania is also the only country that has provided all of the eIDAS trust services a legal meaning within their national legislation (see 4.2.6.). Four qualified trust service providers (two from the public and two from the private sector) offer qualified certificates for electronic signatures and seals, qualified validation services of both and, finally, qualified time stamping. The two public sector providers are the Identity Documents Personalisation Centre under the Ministry of the Interior (providing qualified certificates for electronic signatures) and the State Enterprise Centre of Registers (offering qualified certificates for electronic signatures and seals and qualified timestamping). UAB Dokobit (operating in all the Baltic states and in Iceland) offers qualified validation services for electronic signatures and seals, UAB BalTstamp offers qualified timestamping service. The only significant trust service missing from the market is QWAC.

Such variety of service offering in conjunction with a relatively small market has already led to one CA, UAB Skaitmeninio sertifikavimo centras, shutting down due to strong competition. Even so, the use of foreign (especially Polish) trust services, in particular qualified timestamping, was mentioned in the interviews. Also, the Estonian company SK ID Solutions is active in the market offering their app-based QSCD in the form of the Smart-ID product.

In addition to qualified trust services, a signature provider called SignOnTab operates in the market offering non-cryptographic signatures. It is used by both public and private sector entities. Also, an e-delivery solution for government exists.[115] The platform was previously only offered to public sector organisations but now plans exist to expand the service offering to private sector.

[115] Part of the SIRIP platform developed by Ministry of Transport and Communications, https://joinup.ec.europa.eu/collection/eprocurement/discussion/sirip-state-information-resource-interoperability-platform (accessed 7 October 2020).

Lithuania has notified its national identity card to the European Commission on level "high".[116] Similar to the solution in Latvia, the electronic and physical aspects of the identity card are separated by differing lifecycles: the certificates are valid for 3 years while the card itself is valid for 10. This leads to only about a third of the documents having valid certificates.[117] In total, about 1.5 million certificates exist with Smart-ID occupying roughly the same market share as the ID-cards.

As is the case in Latvia and Estonia, the identity federation solution called BankLink is in active use by private and public sector. An e-government gateway exists consolidating authentication of government services.[118]

As can be observed in other countries, the banking sector drives much of the eID use and is thus the dominant use case. This is exemplified by the wide use of Smart-ID. As of 2019, about 40% of active certificates are based on Smart-ID, as much as are based on the state-issued identity card.[119] Such wide use and rapid adoption (the number of certificates on devices increased from about 74 000 to 618 000 between 2018 and 2019[120]) of a device that only in 2018 acquired the QSCD certification[121] is difficult to explain without taking into consideration the ownership of the technology by the dominant banks in the region.

In the public sector, social insurance and taxation are the biggest use cases for electronic identity. Both, however, still mostly rely on their internal authentication mechanisms.

It is estimated that about half of the electronic services require electronic signing with public sector services leaning more towards use of qualified instead of non-qualified signatures than the private sector. The law generally allows but does not require the use of qualified signatures. While requirements towards services in terms of the levels of assurance needed are being compiled, service providers can commonly adjust the levels of assurance accepted based on their own risk analysis. This situation is perceived to be changing, especially in the banking sector, as more stringent regulations like the PSD2 Directive drive banks towards external trust services like QWAC.

The use of electronic identity has been steadily increasing over the past 6 years with the percentage of people having used qualified certificates increasing from 6% in 2014 to an estimated 29% in 2020.[122] That growth is apparently further accelerated by the COVID-19 pandemic with additional growth figures of 6 to 30 percent quoted for different usage scenarios.

5.2.7. Norway

The trust services market in Norway stands out amongst other NOBID countries as having the largest number of qualified trust service providers, amounting to nine. This is caused by

[116] Electronic identification schemes notified pursuant to Article 9(1) 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, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020XC0821(01)&from=EN (accessed 7 October 2020).
[117] There are around 2 300 000 citizens, for whom the card is compulsory. As of 2019, there were 621 018 active qualified certificates on these cards. *Patikimumo Užtikrinimo Paslaugų Rinkos 2019 Metų Apžvalga***,** 2020-04-23 Nr. (65.4E) ND-6, Vilnius 2020, p. 12, https://elektroninisparasas.lt/images/ataskaitos/2019.pdf (accessed 7 October 2020).
[118] E-Government Gateway, https://www.epaslaugos.lt/portal/ (accessed 7 October 2020).
[119] *Patikimumo Užtikrinimo Paslaugų Rinkos 2019 Metų Apžvalga,* p. 13.
[120] *Ibid.*
[121] Smart-ID's recognition as Qualified Signature Creation Device (QSCD), https://www.smart-id.com/e-service-providers/smart-id-as-a-qscd/ (accessed 7 October 2020).
[122] *Patikimumo Užtikrinimo Paslaugų Rinkos 2019 Metų Apžvalga,* p. 20.

the BankID scheme requiring the use of qualified certificates for signatures, meaning that all BankID issuers must be qualified trust service providers for certificates. In addition to the BankID banks, the main stakeholders are Buypass and Commfides. Buypass is significantly larger than Commfides in terms of market share while the consumer-oriented authentication market is dominated by BankID.

Despite numerous providers of qualified-level personal certificates, there are no QSCD devices nor remote QSCD services on the market. This leads to majority of the electronic signatures being advanced electronic signatures issued using qualified certificates. Signicat, Signant, and Verified provide advanced electronic signing solutions based on authentication.

BankID is a common eID scheme used by all Norwegian banks. The owner and the commercial actor of the scheme is Vipps AS, but formally certificates (for authentication and signing) are issued by six qualified certificate authorities where DNB, Danske Bank, and Nordea have their own CA while the other three serve the rest of the banks. BankID is based on a common infrastructure, where all user private keys for authentication and signing are held in a centralised service, which effectively means that BankID provides a remote signing service.

BankID also has a mobile variant with the private key stored on SIM cards, like *Mobiilivarmenne* in Finland and mID in Estonia and Lithuania. All Norwegian mobile operators co-operate with BankID on this setup. BankID Mobile has qualified certificate for signing but can only be used to sign short text statements.

The Norwegian government has created an alternative solution to BankID that is called MinID. It allows citizens to access public services that require a medium level of security. It is used by 2.6 million Norwegians as of 2019.[123] The centrally provided authentication portal ID-porten for public sector organisations exists providing access to approximately 2000 web services as of 2020.[124] ID-porten is widely used by public sector organisations. The Norwegian eIDAS node is operated in conjunction with ID-porten. In addition to private sector services, the government has created a central electronic signature and workflow portal[125] usable by logging in via ID-porten.

Norway is one of two NOBID countries where QWAC services are offered to both local and international markets. Qualified electronic seals are offered, but there are no validation services. Buypass increasingly operates in an international market, e.g. selling PSD2-compliant QWAC and qualified electronic seal certificates. Public sector organisations utilise a non-qualified e-delivery service.

A strong enterprise market for qualified trust services exists and is mainly served by Buypass and Commfides. Commonly, an employee is issued a dedicated certificate for use in the context of their employment, often in conjunction with an electronic seal of the company.

There are no notified or pre-notified authentication schemes, although the desire to notify a scheme was expressed.

---

[123] Digital Government Factsheet. Norway, European Commission, 2019, p. 21, https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Norway_2019.pdf (accessed 7 October 2020).
[124] ID-porten, https://www.difi.no/fagomrader-og-tjenester/difis-felleslosninger/id-porten (accessed 7 October 2020).
[125] Signering, https://signering.posten.no (accessed 7 October 2020).

In terms of use of trust services by citizens, BankID is clearly dominating the Norwegian market with estimates of penetration varying between 90 to 98 per cent of the population. BankID Mobile has about 50 % market penetration. The government-run MinID scheme is a distant second in terms of usage as the government portal ID-porten sees more than 10 times more BankID (including BankID Mobile) than MinID logins each month.[126] For enterprise and professional use, Buypass is the major driver providing its certificates to customers in all NOBID countries (authentication and signature services are not being delivered cross-border).

As issuing signatures to prove intent is very seldom required by law, the society leans heavily towards authentication in conjunction with audit logs to prove one's intent online. Where signatures are required, the level of "advanced electronic signature with qualified certificate" is most common, as none of the three actors BankID, Buypass, and Commfides currently offer qualified signature creation devices, hence no qualified signature solution exists in the Norwegian market.

While in some countries service provider decisions on levels of assurance used are based on risk analysis, Norwegian service providers are said to often prioritise usability over risks.

Norway has developed its Point of Single Contact portal Altinn. It is tasked with the provision of all information needed by any European service provider interested in starting a business in Norway.[127] The Altinn portal for reporting to the public sector has a consent solution consisting of authentication, click to consent, and a "legal log" recording the chain of events with timestamps.

An interesting approach to signature interoperability is being considered: a remote-QSCD single-certificate solution based on authentication allowing anyone in possession of an accepted authentication token to issue electronic signatures acceptable by Norwegian authorities. This turns the signature interoperability problem into an authentication interoperability problem.

As of July 2020, 395 businesses use eSignering (personal electronic signature), 165 058 signatures were issued in July 2020 using the government-provided signing service.[128] ID-porten sees around 20 million logins a month with about 20% growth year on year as of May 2020.[129]

Use of the Digdir-provided signing service demonstrates, that the COVID-19 pandemic has had a major impact on the use of Norwegian electronic services.[130] 170 965 electronic signatures were issued in March 2020 versus 19 164 in March 2019, an almost nine-fold increase. April showed 4.5 times growth with February and May demonstrating about two-fold growth. This seems to indicate the pandemic has not only increased eID use during the peak of the crisis, but the momentum is continuing as customers shift their behaviour.

[126] ID-porten, August 2020, https://samarbeid.difi.no/statistikk/id-porten (accessed 7 October 2020).
[127] Digital Government Factsheet. Norway, p. 20.
[128] eSignering, statistics as of July 2020, https://samarbeid.difi.no/statistikk/esignering (accessed 7 October 2020).
[129] ID-porten, August 2020, https://samarbeid.difi.no/statistikk/id-porten (accessed 7 October 2020).
[130] eSignering, statistics as of July 2020, https://samarbeid.difi.no/statistikk/esignering (accessed 7 October 2020).

5.2.8. Sweden

In Sweden, there are two qualified trust service providers, TrustWeaver AB and ZealiD, are present locally. They offer qualified validation services for electronic signatures and seals focusing on invoicing solutions for large multinational companies. That said, several non-qualified trust service providers are present offering a wide range of services. The likely reason for the service providers not pursuing the "qualified" status is the lack of national regulatory pressure to explicitly require use of that level of trust services.

The consumer authentication market is dominated by Finansiell ID-Teknik BID AB operating the Swedish BankID scheme. The scheme offers advanced electronic signatures as well as authentication services. Although different identity means can be issued for various purposes by the stakeholders of the scheme, the app-based mobile ID is the most common.

Freja eID+ is a mobile eID from private company Verisec. This eID does not require a Swedish bank account but the Swedish personal identification code is required.[131] Verisec additionally has two other eID offerings using the same app, Freja eID Basic, which is based on self-registration and Freja eID Extended, which is based on registration by optical scanning of an ID document in conjunction with a selfie picture and comparison of the pictures. Verisec offers the Freja eID Basic and Extended products also in the UK, Denmark, Finland, and Norway but has recently announced it would focus predominantly on Sweden and the UK.

Kivra is the biggest service provider for non-qualified e-delivery covering approximately 85% of the market. An e-delivery service (Mina meddelanden) exists that is used by both private and public sector organisation. It provides means for secure message delivery from organisations to citizens.

There is no electronic identity scheme notified or pre-notified to the European Commission.

The electronic identity market is strongly influenced by the regulation specifying different requirements on levels of assurance, for authorisation attributes etc. for finance, health, education and other domains. This leads to separate eIDs being procured, implemented and used for public servants and employees in their respective domains. This fragmentation is reflected in the private sector where, like in Norway, it is common for enterprises to procure a dedicated electronic identity solution for their employees. One example is the SITHS smart card based eID from Inera that is used extensively by health care professionals and to some extent by employees in municipalities.

The usage of electronic identity in Sweden is dominated by BankID. It is used by public and private sector alike for both authentication and electronic signatures. BankID creates a common infrastructure but individual authentication or signature means are issued separately and can incur a cost. The most common means of authentication is mobile ID. It is currently used by 7.5 million people (out of 10.3 million registered citizens) which is a large majority of the adult population. There are also older smartcard-based and file-based BankID solutions which have low usage rates.[132]

Based on a study conducted in 2019, around 60% of public organisations (government agencies, municipalities and regions) that provide digital services for citizens have some

[131] Freja eID, https://frejaeid.com/en/home/ (accessed 7 October 2020).
[132] BankID, https://www.bankid.com/en/ (accessed 7 October 2020).

services which require an electronic signature from the citizen.[133] The most common approach is to sign directly via BankID. The recommended solution for e-signatures is however a "Central signing service" (also called "remote signing"). The central signing service issues a unique signing certificate for each signature based on the previous authentication using a certified eID such as BankID or Freja eID+. Each public organisation is responsible for procuring their own implementation.

The verksamt.se portal provides a single-point of entry for entrepreneurs and enterprises to access digital eServices and information from three public authorities: the Swedish Companies Registration Office (*Bolagsverket*); the Swedish Tax Agency (*Skatteverket*); and the Swedish Agency for Economic and Regional Growth (*Tillväxtverket*). The portal is integrated with the eIDAS node allowing login using electronic identity means from seven European countries as of July 2020.[134]

5.3. Cross-border use of electronic services

During the interviews with the representatives of all NOBID countries including the SDG Regulation national coordinators, the input received was that the volume of cross-border use of electronic services is currently very low.

All NOBID countries have designated service portals where SDG Regulation services could be reached, but all of them mainly serve their respective populations.

In countries such as Sweden, Finland, Norway and Denmark, a central state portal is in place where foreign citizens can authenticate. The challenge in getting access to actual services is however that the specific personal identification code of the country in question is usually needed as a "username", and that the code cannot directly be obtained from an authentication using a foreign eID.

Sweden reports that over 100 public agencies and municipalities have integrated cross-border authentication means to allow access to their electronic services.[135] Also, in Norway, municipalities do not have a common gateway for access or authentication.

In Norway, the Altinn portal[136] is a single point of contact for conducting business in Norway. For citizens there are domain-specific portals, based on large service areas, e.g. the Tax Administration and the Labour and Welfare Administration.

In many NOBID countries, there are bilateral use cases where authentication services or trust services of another country are used, or the authentication means of a neighbouring country could be used to use local e-services. For example, the Estonian Business Register enables logging in with Finnish ID-card which is not a notified scheme.

Most of the cross-border e-service users in Finland come from Estonia, but there are also German and Italian eIDs used for requesting access to services (approximately 10 000 queries per month). Finland has the e-prescription service based on the X-Road shared interoperability platform in place between Estonia and Finland. This is the most commonly

---

[133] *E-legitimering inom den offentliga förvaltningen*, 2019, p. 5, https://www.digg.se/globalassets/dokument/publicerat/publikationer/elegitimering-inom-den-offentliga-forvaltningen.pdf (accessed 7 October 2020)

[134] Digital Government factsheet 2019. Sweden, European Commission, 2019, p. 6, https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Government_Factsheets_Sweden_2019.pdf (accessed 7 October 2020).

[135] Digital Government Factsheet. Sweden, p. 21.

[136] Altinn, www.altinn.no (accessed 7 October 2020).

used cross-border service despite not relying on electronic identification of citizens to function.

The list of cross-border electronic services provided to the project team (see 4.1.3) are a combination of diverse services and are operated by different public agencies. As a result, the national SDG coordinators could not provide a complete overview regarding the use of authentication means and trust services in case of specific services as the decisions regarding what levels of assurance or trust services are to be used is mostly made by the service provider (e.g. the business registry).

When asked about the cross-border services which the representatives of the NOBID countries deem most relevant, they mostly agreed with the list provided to the project team (e.g. studying, working, moving abroad or the domain of social security such as pensions and social benefits) by saying that these would be the first use cases they would look at, but at the moment, there are no cross-border services of this kind. There is general agreement that when the volume and variety of use cases arises for digital services, the demand for trust services will go up alongside.

Estonia sees that the following three main types of use cases for cross-border services may show more demand in the future:

- Learning and teaching-related services (enrolment in schools and classes, issuance and validation of academic certificates)
- Services related to legal entities (business registry services, changes in ownership and representative rights)
- Tax and Customs related services (permission requests and management e.g. in transit of goods, declaring and refunding taxes)

Finland expects that working abroad and doing business abroad could be the use cases with most potential demand.

Norway expressed that there are not many cross-border services people can use at the moment. There are cases that are conducted offline, but not to an extent which would motivate investment into developing digital services. Norway has not notified any eID schemes to the European Commission prompting cross-border interaction. However, companies like Signicat have developed a platform which integrates different e-signature means and eID schemes and this is seen as an important element for cross-border e-service delivery.

Norway would like to have a connection at the database level, and not use trust services to guarantee trust. Rather, it should work seamlessly in the backend for the individual. This would likely mean bilateral agreements between countries like there is in place between Estonia and Finland. For example, there is a treaty between the Nordic countries on co-operation and interoperability between their respective population registers.

The project team tried to explore attempts to authenticate by using the eIDAS node in different state portals. The volume of the attempts confirms what the interviewees indicated – there simply are not enough cross-border electronic services available and currently not enough demand to use them online.

Iceland, for example, has not yet implemented the eIDAS node. Meanwhile, Sweden has a well-established statistics tool which shows that most of the eIDAS node access attempts come from Estonia. The Finnish eIDAS node apparently also gets most access attempts from

Estonia. The eIDAS node, however, does not show which online services were requested or consumed by the person requesting them.

The Finnish central gateway suomi.fi offers authenticator service for nationals of other countries to register a foreign identifier (UID) and verify his or her identity using the Finnish Authenticator application. After registration and implementation of the application, the foreign citizen can log in to the transaction service with the foreign ID or e-mail, password and the application's PIN code. This type of authentication is not a strong electronic authentication service, but by using the application, the user can prove his or her identity with documents when logging in to the transaction service. Suomi.fi Authenticator service is run centrally by the Digital and Population Services Agency (DVV).[137]

The Lithuanian state portal VIISP (epaslaugos.lt), provides authentication by foreign means of identification. However, most of the service providers do not accept non-Lithuanian personal identification codes. One of the assigned services „Declaration of the place of residence when leaving Lithuania" was used 15583 times in 2019 by Lithuanian citizens going abroad to live. 44 logins with non-Lithuanian personal identification codes took place in 2019 at the eIDAS node.

A Latvian state portal exists[138], but the cross-border volume is low (approximately 400 access cases in 2019). The Latvian state portal supports various eID providers beside the notified ones (e.g. mainly bank solutions), but the decision of what to support is made by each service provider.

In general, there was a strong drive from the Nordic countries to use national authentication means cross-border (i.e. BankID-s) while relying on trust services in cross-border electronic services was mostly not established due to the fact that Nordic countries mostly do not require an electronic seal or signature in private use (professional use differs). Baltic countries rely more on electronic signatures together with a high level of authentication to prove one's intent online. As a result, a division could be seen where Baltic countries would be more accepting towards the use of cross-border electronic services where trust services are requested to complete the service and Nordic countries would like to use the authentication means as the common denominator.

[137] Finnish Authenticator, https://www.suomi.fi/ohjeet-ja-tuki/tietoa-tunnistuksesta/finnish-authenticator-tunnistuspalvelu (accessed 7 October 2020).
[138] State service portal latvija.lv, https://www.latvija.lv/en (accessed 7 October 2020).

e-Residency – where there is a will, there is a way![139]

The difficulties with the cross-border use of eID has given roots to a government-led initiative that enables the use of the Estonian eID infrastructure by foreigners. The e-Residency card[140] enables a foreigner[141] to use e-services of Estonia without physically being in Estonia.[142] As most business operations can be done online in Estonia (e.g. tax reporting, submission of annual reports), the e-Residency is a way to do business in Estonia (and in Europe) while actually operating from another physical location. The most e-Residents come from Finland (more than 5500) and wish to do location-independent international business.[143] Looking at statistics from other NOBID countries, there are 1850 e-Residents coming from Latvia, 1268 from Sweden, 913 from Lithuania, 449 from Denmark and 385 from Norway. It is notable that Finland, which has the highest number of e-Residents, has not notified any eID schemes to the European Commission. This would enable the use of Finnish eID in Estonian electronic services. Although the eIDAS Regulation sets the framework for mutual recognition of national eIDs, the fact that many e-residents come from EU countries where they could use their own national eIDs for cross-border use instead of e-Residency card shows that there is no interoperable solution or they cannot use the national eIDs as they are not notified according to the eIDAS Regulation.

In total, there are 68 774 e-Residents who have created more than 7000 companies giving employment to more than 1500 employees. Since the roll-out of the programme, Estonia has generated more than 25 million euros in additional tax revenue.[144]

The reasons why there are numerous e-Residents from NOBID countries vary and some only do it because of novelty aspects, but there is the inescapable fact that if the landscape of eIDAS Regulation and SDG Regulation would function properly, there would not be a need for the e-Residency programme. Given the current situation, however, it is unsurprising that the number of applications has been constantly rising since 2014.

e-Residency should not be confused with citizenship or a physical residence permit. Being an e-Resident does not grant any permission to live or work in Estonia or the rest of Europe, but the use of a notified eID gives access to EU electronic services.

6. Findings

This section highlights the main findings induced from sections 4 and 5 by presenting the key barriers (6.1 and enablers (6.2) of trust services both in and between NOBID countries. The section also describes other important observations (6.3).

[139] In July 2020 Lithuania also passed amendments to Law on Legal Status of the Aliens, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/57df8b40839211e5bca4ce385a9b7048?jfwid=gzvyqtmdd (accessed 7 October 2020). According to the law foreigners are allowed to obtain the status of an e-resident starting from January 2021. Being similar to Estonian programme, e-residents will be able to set up companies, open bank accounts, and declare taxes online. E-residence applications will have to be submitted to the Migration Department.

[140] The requirements for the issuance or the refusal of the e-resident's digital identity card are stipulated in chapter 5^2 of the Estonian Identity Documents Act, https://www.riigiteataja.ee/en/eli/504022020003/consolide (accessed 7 October 2020).

[141] Recipient of the eResidency card must not be eligibe for any other electronic identity (e.g. resident's eID).

[142] To receive the card, however, one needs to physically apply and obtain the eResidency card either from Estonia or at the Estonian embassy, making the eResidency card 'High' in light of the eIDAS Regulation. eResidency card is also notified to the European Commission.

[143] eResidency Dashboard, https://e-resident.gov.ee/dashboard/ (accessed 7 October 2020).

[144] *E-residentsuse programm on toonud Eestile juba 25 miljonit eurot otsest tulu*, Ärileht.ee, 1 August 2020, https://arileht.delfi.ee/news/uudised/e-residentsuse-programm-on-toonud-eestile-juba-25-miljonit-eurot-otsest-tulu?id=87016125 (accessed 7 October 2020).

6.1. Barriers to the use of trust services and alternatives thereof between NOBID countries

This section focuses on the barriers to the use of trust services and alternatives thereof both in NOBID countries and between them.

6.1.1. Barriers to the use of trust services and alternatives thereof in NOBID countries

- QWAC is only used in the PSD2 context in **Estonia** because it is deemed not to fit well with the wider security concept of the world wide web and lacks support by the community, most notably browsers.
- In **Finland**, there is a strong legacy of using authentication and there are no drivers to develop new kinds of services that also include e-signatures. Service providers also often lack the capabilities in understanding the level of e-signature. There are products and services on the market, but it is difficult to assess if the particular service fulfils the eIDAS requirements and what is the level of a particular trust service (for example advanced or qualified electronic signature).
- The size of the market influences the availability of trust services. As the cost of certifying a service to "qualified" trust service provider level is fixed, market size can become a barrier as a service provider stemming from the country cannot afford certification but cannot expand internationally without it. This is the case reportedly in **Iceland**.
- In general, users in **Latvia** were deemed to lack experience and understanding of digital identity but it was also found that once the users feel the benefits of electronic interaction, for example during the COVID-19 pandemic, both the experience and understanding improve.
- Service providers in **Latvia** are seeing the form factor of the identity carriers as a barrier to electronic identity use as users are increasingly moving away from desktop devices and might not have a card reader at hand even if a compatible device for its use is available.
- Several countries (**Latvia** in particular) appear to be experiencing a stalemate where the non-obligatory identity carriers see low penetration as users see little point in obtaining them in absence of compatible services. The service providers on the other hand see little point in supporting the identity carriers in absence of the users. **Finland** and **Latvia** have taken regulatory steps to increase user adoption and break the deadlock.
- Lack of information about the benefits, security and legal meaning of trust services was deemed to be a barrier in **Lithuania**. Still, Lithuania surveyed the document management providers (e.g. Dokobit) and saw that the pandemic increased demand for electronic signatures by up to 30% in some systems and as much as 120% in others.[145]
- In **Norway**, only personal eIDs exist in the market. In some cases, this creates friction as individuals may be reluctant to use personal certificates for professional use, and even in some cases are forced to buy such certificates at a price to use them professionally. Sometimes, e.g. in health care, this seems to be overcome by people obtaining the

[145] As the demand for Electronic Signatures Increases, RRT provides advice to users (in Lithuanian), 9 April 2020, https://www.rrt.lt/isaugus-elektroninio-paraso-paklausai-rrt-teikia-patarimus-vartotojams/ (accessed 7 October 2020).

certificates on a token, e.g. a smart card, that is issued specifically to health care professionals, even though the certificates are still only personal.

- Lack of qualified trust services creates a challenge for private businesses in **Sweden** who need to handle documents from abroad, e.g. when participating in procurement processes where tenders need to be signed with qualified electronic signatures. There are not enough validation services that would satisfy the demand fully. There are products on the market, but these are seen to be too complicated to use as it is difficult to determine if the service fulfils both eIDAS and Swedish national requirements. Therefore, it is difficult for a buyer to distinguish services suitable for different formal requirements.
- In **Sweden**, there is a lack of a common layer of authentication even on national level, e.g. Sweden Connect Federation is developing common standards for eID framework, based on the requirements set by DIGG, the agency for digital government. However, BankID is not part of the common standards framework that Sweden Connect proposes. BankID is the most used solution with very high penetration in the domestic market.
- The relationship between personal and commercial identities appears to be a challenge resolved in different ways and with varying levels of success in different NOBID countries. The challenge lies in the need to differentiate between a person's role as a citizen and their role in an official capacity. An organisation must be able to grant or revoke the privileges of a person to represent a company but should not be able to restrict their ability to fulfil their role as a private individual. Differences in the approaches taken in different countries act as barriers between countries while a cumbersome national authorisation strategy can act as a barrier for commercial use of trust services.

6.1.2. Barriers to the use of trust services and alternatives thereof between NOBID countries

- Although authenticating a citizen (i.e. allowing a person to prove they are in control of a particular national identifier) is technically possible, the semantic interoperability between the identities is said to be lacking. For example, in Finland, the very fact that a person has a Finnish identity code allows the service to make a range of assumptions about the status of the person and the applicable business rules. In other countries, the connotations are different as the rights and obligations of a citizen are determined on the national and not EU level. It is currently mostly up to the individual service providers to map the national meaning of a person's identity and the one of their homeland. Typically, this complex task is accomplished by simply deciding the service is not intended to be used by foreign nationals.
- On the EU level, there appears to be a stalemate where the services are not accepting foreign electronic identities because there is no demand and the lack of demand is in turn caused by the lack of services.
- There is no concept of shared physical identity between the NOBID countries and therefore the sharing of electronic identity is hindered. A person can obtain several identities from several NOBID countries and there is no way for the service providers to link these various identities to a single person as required by risk profiles, regulations, and the nature of the services that were used. Also, differences in identity policies mean a person might legally have two different devices for authentication and electronic signature referencing two separate identifiers. This would mean they are able to

authenticate as one identifier to a foreign service but provide an electronic signature referencing a different one. The service would have no means of linking the two identities causing the transaction to fail.

- The lack of technical and legal standards around the identity codes appears to be a barrier. For example, the Estonian and Lithuanian ID-codes share the same format and it can be hard for a service provider to distinguish between them without an explicit statement of origin. Similarly, it is hard for a Finnish service provider to accept an Estonian user whose identity code is formatted completely differently to the Finnish one. Sweden is solving this problem by issuing surrogate identity codes to citizens approaching their services via the eIDAS node and Estonia is planning the same. Issuing identity codes is very strictly regulated in some other NOBID countries (e.g. Finland), however, and a similar approach is unlikely to be taken.
- Authentication services are significantly linked to interoperability services. A person logging in to a service could mean anything from the simple confirmation of their name from a registry to accessing a range of services to pre-filled forms and automate services. Access to this information is not available to foreign nationals, the semantics of the information is likely to differ, and therefore the service usability can be significantly lower if the service is usable at all. This is augmented by various legal regimes where access to certain registries might not be available at all (Finland, Latvia, Estonia, Lithuania)
- Lack of cooperation in software and service development was seen to be a cross-border barrier. For example, the Estonian DigiDoc service offers a robust platform for validating standard electronic signatures but there is no functional mechanism for third parties like other countries to request features in that software despite the software being open source.
- The vast majority of citizens currently do not need cross-border services. Thus, use of cross-border services in NOBID countries is a subset of a subset of all eID users in a country. People needing a particular service in a neighbouring country further limits this group. Combined with relatively small countries, this leads to difficulties in creating a sufficiently critical mass of users to solve problems of cross-border service provisioning. The complex business process and technical changes necessary (see the semantics and interoperability barriers mentioned above) might simply not pay off for an individual service due to a very small user base.
- Difficulties in determining the level of trust in trust services and alternatives thereof is a barrier to their use between NOBID countries.
- The extent of the cross-border demand, challenges or potential use is difficult to estimate since there is a lack of statistics. An outlier is Sweden which collects statistics of the SDG gateway cross-border usage in a central dashboard. The dashboard is designed to be made available in an open data format, displaying the number of entries for authentication via the eIDAS node by individual countries.[146]
- Despite international standards being present, technical compatibility in terms of the ASiC-E signature container compatibility between NOBID countries (the Baltic states were mentioned in particular) remains a challenge as countries differ in the precise way

[146] The portal where the dashboard would be made available is www.swedenconnect.se.

standards are utilised (e.g. Lithuania uses the .adoc format while Estonia uses the .asice format)

- Electronic services are dependent on a personal identification codes both in terms of technological solution as well as service design. This means dependence on a local identification code is hard-coded into services creating a major barrier for cross-border use.
- All countries, quite naturally, prioritise their national services and compliance over cross-border compliance and services.

6.2. Potential use of trust services and alternatives thereof between NOBID countries

- There is strong preference among Nordic countries (clearly expressed by **Finland**, **Sweden**, **Norway** and **Denmark**) to focus on authentication in the cross-border dimension and only then on trust services. All people should be able to have strong authentication mean to access e-services.
- Close cooperation should be established for use cases for working and studying in countries nearby. The SDG itself is seen as a driver in **Finland**.
- Similarly, the creation of electronic services for those who need them, making them aware of these and enabling the use of local trust services in the provision of these services is seen as crucial. The focus should be on the cases where cross-border interaction happens today in the offline world – studying and working abroad. For example, there are many Lithuanian migrant workers in Iceland, as well as notable streams of workers commuting between Sweden and Denmark who acquire an administrative personal identification code for taxation reasons or even for getting their wages and interacting with public agencies via a digital post-box. A Danish person would get a Swedish BankID which is used for the same purposes.
- Cross-border trust between eID schemes would be the most important element as more than 90% of the population have the means available. **Danish** interviewees believe that the first step would be for each country to have their national eID notified - this would raise confidence in the ability to issue national eIDs in the reliable way. Buypass (**Norway**) is thinking about a one-time-certificate for signing based on eID LoA High to enable cross-border signing.
- A deliberate effort must be made to start trusting identification by other countries. Gradual progress may come when a service-providing leader e.g. the Tax Board starts to implement cross-border trust services and electronic identity, then others will follow the example. The X-road is used in three NOBID countries (Estonia, Finland, Iceland) and is considered as a non-qualified e-delivery service. As NIIS, the maintainer of X-Road, is considering making X-Road a fully compliant e-delivery service, further cooperation between NOBID countries in terms of trust services can be created.

6.3. Other observations

- The COVID-19 pandemic was seen as a major driver of eID adoption and trust services in general. Latvia has done electronic parliamentary voting while Estonia has not. Generally, people are not willing to take the effort of learning unless they are sure of

benefits or have no other options, but are not falling back to paper after they have put the effort in.

- Qualified certificates are more common than qualified devices because there is no need, no attention, or no desire to certify the devices.
- Personal identity tends to be under tight control of national governments while other trust services are commonly procured within an international context (e-delivery, timestamping, web certificates etc.).
- Cooperation and cross-border use are to a very large extent driven by corporate strategy of a much wider group of organisations than just trust service providers
    - Large multinationals tend to utilise centrally developed solutions using a corporate trust network rather than adopting the local one (Latvia, Estonia)
    - Integrators, document management service providers and other parties operate internationally and bring their international cooperation networks into local context (Latvia)
    - Large Relying Parties often operate internationally and seek to unify solutions at least on a regional basis (Telia, Swedbank, SEB in the Baltics but also in other NOBID countries)
    - Trust service providers operate internationally and, seeking to minimise cost, will unify solutions creating interoperability in the process (SK ID Solutions in the Baltics, Nets, Signicat and others in the Nordics, Dokobit)
- The use of authentication instead of signatures in services is commonly at the discretion of the service provider and based on a risk analysis. Commonly, some high-risk operation at certain services require an electronic signature while the rest can be conducted based on authentication only. Two distinct strategies can be observed here: one that uses the minimal level of security to maximise user convenience and ramps it up as necessary and the other, that defaults to the highest level of security at the expense of some usability. The latter is mostly used in Estonia and, to a lesser extent, in other Baltic countries.
- Different requirements for assurance level of eIDs create interoperability problems. As countries find their own optimal solutions to the complex equilibrium of usability and risk, citizens from countries with relatively low assurance levels requirements are simply lacking the devices required to access services in a country, where a higher level of authentication or signatures is expected. For example, a Norwegian citizen would find it challenging to create the qualified electronic signatures expected by most Estonian public sector organisations.
- Banking is a significant driver of eID use (Bank-initiated schemes in Sweden, Norway, Finland; respective mentions in Latvia and Estonia, Bank-owned or operated TSPs in the Baltics, Iceland and elsewhere).
- The use of cross-border services in general is very low. Specific solutions focused either on specific services or interoperability between countries do exist where use cases are present but general service access sees very low use.

7. Conclusion

The study answered all the research questions that were initially stated.

Firstly, trust services (both eIDAS-defined as well as alternatives) offered in NOBID countries were mapped and the landscape was analysed both generally (see section 5.1) and in the context of all the NOBID countries (see section 5.2). The services observed are summarised in Appendix B: The market of trust services and alternatives thereof in NOBID countries.

Secondly, the areas where public and private sector currently utilise trust services and their alternatives were described (see section 5.2).

Thirdly, the use of these trust services as well as alternatives between NOBID countries was described section 5.3) along with barriers preventing their use (see section 6.1) and key enablers (see section 6.2).

In addition to the research questions answered, the study yielded the following main conclusions:

- Despite a very similar shared regulatory context in terms of the eIDAS Regulation, the countries are remarkably different in terms of the specific ways the eIDAS Regulation has been implemented and in how services use trust services and their alternatives.
- Significant barriers exist in the use of trust services and alternatives thereof between NOBID countries. Some of the most significant barriers stem from the differences in approach to physical identity and other areas not governed by the eIDAS Regulation.
- Despite the observed differences between the countries as well as significant barriers, no large-scale unresolved problems were encountered during the research.

Appendix A: Interviewees

Country	Person	Title	Institution
Denmark	Thoke Graee Magnusson	eIDAS technical expert	Agency for Digitisation
Denmark	Klavs Helberg Jensen	SDG national coordinator	Agency for Digitisation
Denmark	Christian-Schmidt-Madsen	IT-, Security- and Chief Architect for NemLog-in	Agency for Digitisation
Denmark	Charlotte Marlene Jacoby	Head of department responsible for the development of our future generations of the national eID and our trust services.	Agency for Digitisation
Estonia	Kalev Pihl	CEO	SK ID Solutions AS
Estonia	Helen Raamat	eID product owner	Information System Authority
Estonia	Mark Erlich	Head of eID	Information System Authority
Estonia	Kärt Karus	SDG national coordinator	Ministry of Economic Affairs and Communications
Estonia	Ott Vatter	Head of eResidency Programme	Enterprise Estonia
Finland	Anne Lohtander	Chief specialist	Finnish Transport and Communications Agency
Finland	Laura Kolinen	Senior officer	Ministry of Transport and Communications
Finland	Teemu Tukiainen	Development Manager	Digital and Population Data Services Agency
Finland	Jarmo Kovero	SDG national coordinator	Enterprise Finland (Suomi.fi)
Finland	Kirsi Mikkonen	Senior Specialist	Development and Administrative Services Centre (KEHA-Centre)
Iceland	Haraldur Bjarnason	CEO	Auðkenni
Iceland	Vigfus Gislason	Head of Division/Specialist	Ministry of Finance and Economic Affairs
Latvia	Lauris Linabergs	Head of ICT architecture unit	Ministry of Environmental Protection and Regional Development
Latvia	Edvards Kreišmanis	Identity product portfolio manager	Latvian Radio and Communications Centre
Latvia	Karlis Melnieks	Compliance manager	Latvian Radio and Communications Centre
Lithuania	Vytautas Krasauskas	Chief specialist at the	Ministry of the Interior

		Information Processing & Statistics Division, Information Technology and Communications Department	
Lithuania	Vaidotas Ramonas	Director of Digital Services Department	Communications Regulatory Authority
Lithuania	Asta Žilienė	SDG National Coordinator	Ministry of the Economy and Innovation
Norway	Tor Alvik	Director of trust services and digital public services	Norwegian Digitalisation Agency
Norway	Stig Slaatto-Hornes	Product owner	Norwegian Digitalisation Agency
Norway	Pål Müller	Sales Director	Buypass AS
Norway	Jon Ølnes	Product Manager	Signicat AS
Sweden	Björn Schärin	Senior advisor	Post and Telecom Authority
Sweden	Roger Fagerud	Strategist	Agency for Digital Government
Sweden	Viktoria Hagelstedt	Director, SDG national coordinator	Agency for Digital Government
Sweden	Sven-Erik Ceedigh	IT-architect	Agency for Digital Government
Sweden	Henrik Bengtsson	Local SDG coordinator	Agency for Digital Government

Appendix B: The market of trust services and alternatives thereof in NOBID countries

The following table depicts the landscape of trust services and the alternatives thereof in NOBID countries as defined in section 5.1.1. The table uses the following acronyms:

- QTSP – The company is a Qualified Trust Service Provider as defined in the eIDAS regulation
- TSP - The company provides a trust service or an alternative thereof
- A - The company offers authentication services to third parties in the market
- B – The company is present in the market
- HQ – The company is headquartered in the market

	Denmark	Estonia	Finland	Iceland	Latvia	Lithuania	Norway	Sweden
Agrello.id[4]		HQ						
Auðkenni				QTSP, HQ				
BalStamp						QTSP, HQ		
Bankenes ID-tjeneste							QTSP, HQ	
Buypass[8]							QTSP, HQ	
Citadele[6]		B			A, HQ	A		
Commfides							QTSP, HQ	
Cryptomathic[4]	HQ							
Danske Bank	HQ		A				QTSP	B
DNB Bank	B		B				QTSP, HQ	B
Dokobit		TSP		TSP	TSP	QTSP, HQ		
Eika Gruppen							QTSP, HQ	
Elisa		B	A, HQ					
Finansiell ID-Teknik BID AB[3]								A, HQ
GuardTime[4]		QTSP, HQ						
Handelsbanken	B		A, HQ				B	B
Kivra[7]			TSP					HQ
Luminor[6]		HQ			A	A		
Nets	TSP, HQ		A				TSP	TSP
Nexus				TSP^1				HQ
NIIS/X-Road[7]		TSP, HQ	TSP	TSP				
Nordea	B		A, HQ				QTSP	B
Penneo	HQ						TSP	TSP
Scrive[4]								HQ
SEB[2,6]	B	A	B		A	A	B	HQ
Signicat	TSP, A		TSP, A				QTSP, A, HQ	TSP, A
Signom[4]			HQ					

SignOnTab[4]						HQ, TSP		
SK ID Solutions		QTSP, HQ			QTSP	QTSP		
Sparebank							QTSP, HQ	
Swedbank[2,6]	B	A	B		A	A	B	HQ
Telia[2]	B	B	A		B	B	B	HQ
TrustWeaver AB								QTSP, HQ
Verisec	TSP		TSP				HQ	
Visma[5]	TSP		HQ		B	B	B	B
ZealID[4]								QTSP, HQ

Table 4. Trust service providers in NOBID countries

[1] Nexus is a solution vendor to Audkenni

[2] Owners of SK ID Solutions

[3] Owned by Danske Bank, Handelsbanken, Ikano Bank, Länsförsäkringar Bank, SEB, Skandiabanken and Swedbank

[4] Unclear market penetration in NOBID region, clear international focus

[5] Non-cryptographic signature services providers

[6] Provide identity federation via the BankLink protocol

[7] e-delivery provider (non-qualified)

[8] Claimed customer base across NOBID