Nordic Council of Ministers

ANALYSIS ON POWER OF ATTORNEY IN THE NORDIC-BALTIC REGION

Contents

This publication is also available online in a web-accessible version at:
https://pub.norden.org/temanord2025-537

ABSTRACT

Purpose and Context

The Nordic Council of Ministers commissioned this report to analyze the current state and future potential of cross-border digital Powers of Attorney (PoAs) in the Nordic-Baltic region. The aim is to ensure interoperability, enhance digital infrastructure, and promote inclusivity while aligning with key EU initiatives such as the **European Digital Identity Wallet (EUDIW)**and the **Single Digital Gateway (SDG).**

Key Findings – As-Is Analysis

1. Digital PoA Maturity Varies

- Different platforms, electronic ID (eID) solutions, and national PoA registries create fragmentation in digital PoAs across the region.
- Some countries use sector-specific solutions (healthcare, taxation, business), while others consolidate PoAs in a single system.
- The digitalization level of PoAs differs—some countries use fully digital solutions, while others still rely on PDFs and e-signatures.

2. Legal and Governance Barriers to Interoperability

- Legal differences include variations in governance models, age requirements, and residency prerequisites.
- While most Nordic-Baltic countries allow login via **eIDAS nodes** (enabling foreigners to use EU-recognized eIDs), identity matching across borders remains a challenge.

3. EU Initiatives Present Opportunities for Interoperability

- The **European Digital Identity Wallet (EUDIW)** could enable **secure authentication and verification** for PoAs.
- The **Once Only Technical System (OOTS)** may help streamline cross-border data exchange.

4. Social Inclusion Challenges

- Vulnerable groups (elderly, non-digital users, immigrants) risk being excluded from digital PoA solutions.
- Some countries offer alternative access options like **physical PoAs, English-language interfaces, digital literacy workshops,** and allowing **trusted representatives** to assist non-digital users.

Key Recommendations – To-Be Analysis

1. Leverage EUDIW for Verification and Authentication

- EUDIW could support secure login, confirmation, and acceptance processes for PoAs.

2. Align National PoA Systems with EU Regulations

- Standardizing data attributes for PoA creation under **eIDAS 2.0** is essential for interoperability.

3. Increase Digital PoA Adoption

- Countries still using manual or PDF-based PoAs could transition to fully digital, validated, and stored PoAs.

4. Enable Cross-Border Assignments of PoAs

- The current systems do not allow assigning PoA rights to foreign organizations.
- OOTS could facilitate data retrieval from foreign registries.

5. Improve Notification and Acceptance Systems

- PoA assignees could be notified and required to **accept assignments** in a structured manner.

6. Enhance Identity Matching for Foreign Users

- Existing PoA platforms struggle to **match international identities and PoA mandates.**
- **EUDIW, OOTS, and national digital ID systems** could work together to resolve this.

Concluding Remarks

The **Nordic Council of Ministers (NCM)** is well-positioned to **drive digital PoA harmonization** across the region. Possible steps to improve cross-border interoperability include:

- Aligning formats and attributes with **EUDIW**
- Developing **pilot projects** in countries with advanced PoA systems
- **Gradual implementation** of digital PoAs within the EUDIW framework
- Addressing interoperability challenges through **OOTS and other EU mechanisms**

This analysis provides a **strategic roadmap** for integrating digital PoAs across the **Nordic-Baltic region,** ensuring greater accessibility, efficiency, and cross-border functionality.

EXECUTIVE SUMMARY

The Nordic-Baltic region is navigating significant challenges and opportunities in digitalizing cross-border Powers of Attorney (PoAs), a critical tool for collaboration and integration. Despite substantial progress in some areas, disparities in digital infrastructure, legal frameworks, and social inclusivity continue to hinder the seamless implementation of PoAs across borders. The Nordic Council of Ministers commissioned an analysis to address these issues, aligning regional efforts with key EU initiatives, such as the European Digital Identity Wallet (EUDIW) and the Single Digital Gateway (SDG).

This report identifies critical insights into the state of digital Powers of Attorney (PoAs) in the Nordic-Baltic region, focusing on challenges and opportunities for enhancing cross-border functionality. It focuses on achieving interoperability, enhancing digital infrastructure, and promoting inclusivity to ensure equal access to PoAs. The analysis is structured around two key areas:

1. An as-is assessment of the current PoA landscape, focusing on digital, legal, and social aspects.
2. A to-be analysis exploring future scenarios, including use cases, Proof of Concept and alignment with EU-wide frameworks like the EUDIW and the Once Only Technical System (OOTS).

This report underscores the importance of harmonizing regional PoA systems with EU initiatives to strengthen digital cooperation and economic integration across the Nordic-Baltic region. The findings aim to guide policymakers in addressing existing gaps and fostering innovative solutions to create a unified and sustainable framework for digital PoAs. Further analyses and detailed impact assessments will be required to adapt these recommendations effectively within national contexts.

Key takeaways

As-Is

To explore future cross-border interoperability of Power of Attorney solutions, the following key insights emerge from the as-is analysis:

1. Variations in platforms solutions to access and handle PoAs, the adoption of electronic IDs (eID), approaches to national PoA registries, and digitalization level of PoA creation, result in differing levels of digital PoA maturity across the Nordic-Baltic region. Most countries have sector-specific platforms to handle PoAs for healthcare, taxation, and business matters separately, while some have a single solution, consolidating PoAs. Further, most countries have adopted eIDs, but the level of advancement vary with some countries supporting multiple EU notified eIDs, and others offering alternative forms of authentication and verification. The PoA registry landscape is also complex, with few countries operating with a national cross-sector PoA registry, meaning that PoAs are generally stored and registered in many different registries nationally. Finally, the digitalization level of PoAs varies, with some countries offering fully digital PoAs across all sectors via national solutions, and others relying on PDF forms signed with e-signatures. This results in a complex landscape for digital PoAs, especially with regards to cross-border interoperability.
2. Wide-ranging differences in PoA governance, legal standards, and digital readiness across the Nordic-Baltic countries create barriers to interoperability, which refers to the ability of different systems to work together seamlessly across borders. The current PoA landscape in the Nordic-Baltic region is highly complex, as countries prepare for cross-border interoperability. Many countries have enabled login via an eIDAS node, allowing foreigners to login with their local EU notified eIDs. However,

identification of actors is currently dependent on personal identifiers located in national registries. Thus, matching and verifying international identities of legal and natural persons remains a general challenge, as well as matching PoA mandates across borders, with only a few cases of existing cross-border PoAs. Consequently, developing cross border initiatives for PoAs may be difficult. The EU initiatives regarding cross-border interoperability may help with this.

3. EU-wide initiatives, including the European Digital Identity Wallet (EUDIW), offer critical opportunities for enhancing interoperability. Alignment with these initiatives and leveraging their frameworks for proof of concepts can provide valuable insights and models for advancing cross-border PoA solutions. Testing use cases and integrating verified credentials and attestation mechanisms are essential steps toward overcoming current technical and legal obstacles.
4. The legal frameworks governing PoAs in the Nordic-Baltic countries are, to a high degree, built on the same principles, including the fundamental freedom to enter into agreements. However, the application of these legal principles differs to some degree, especially regarding legal barriers, e.g. age requirements, mental capacity stipulations, and residency prerequisites. A more uniform legal approach in the Nordic-Baltics should make for cross-border easier and more available to Nordic-Baltic people and companies.
5. While there are ongoing challenges in achieving full digital inclusion, such as the risk of excluding vulnerable groups, especially the elderly, individuals with cognitive impairments, and those with limited digital skills or health conditions, significant progress has been made in the Nordic-Baltic region. Efforts have been made to improve access to digital Powers of Attorney (PoAs), including providing physical PoA options for those unable to use digital platforms. Additionally, accessibility measures, such as English language resources and provisions for individuals with impairments, have been introduced. Alternative pathways for obtaining digital identification and options for trusted representatives to assist individuals unable to manage their digital tasks have also been established. Educational and support services, including digital literacy workshops, have played a crucial role in helping those with limited digital skills navigate PoA processes. However, the rapid pace of digitalization still presents challenges, particularly in preventing the exclusion of certain groups as in-person interactions decrease. While substantial progress has been made, continued efforts are necessary to ensure equitable access to PoAs for all citizens across the region.

To-Be

From the identified use cases and developed Proof of Concept (PoC), the following key observations highlight the challenges and opportunities for cross-border PoA implementation. These observations focus on critical areas such as cross-border identity matching, digital PoA creation, and data retrieval. They provide insights into how the European Digital Identity Wallet (EUDIW) can address current limitations and enable seamless cross-border PoA solutions in the future.

1. The verification and authentication mechanisms could be enabled via EUDIW, which will be key multiple times during login, confirmation, and accepting processes for digital PoAs. EUDIW could integrate national eID solutions to authenticate users, often through national registries. Security is key for identity verification and authentication, with strong ID infrastructure standards being necessary to ensure this.
2. Different countries require varied attributes for PoA creation, with basic data needed for platform login and more detailed information for PoA assignment. EUDIW could formalise most of these required attributes, but additional local attributes may need to be sourced, for instance via OOTS.

Consequently, aligning national attributes required with eIDAS 2.0 regulations may be key.

3. Some countries still rely on manual processes for PoA creation, using PDFs. To facilitate EUDIW integration, it could be essential to explore how PoAs can be created, validated, and stored digitally. Increased digital maturity could streamline processes and enhance interoperability across borders.
4. Assignors may need to grant PoA rights to foreign organizations, but current systems do not support cross-border assignments on national platforms. Including foreign entities in the PoA scope could be achieved through OOTS, which allows data retrieval from foreign registries.
5. For cross-border PoAs, it is essential to accurately identify and assign international assignees. Current systems struggle with this but allowing log-in via eIDAS nodes may improve functionality. Additionally, OOTS could help retrieve international assignee data.
6. OOTS could retrieve PoA data directly from national registries to be used in cross-border PoA systems. EUDIW can store documents and credentials, but integrating OOTS mechanisms could ensure accurate, up-to-date data. Although manual validation may be necessary initially, over time, OOTS could optimize the process, streamlining cross-border PoA workflows.
7. Notifications could be needed to ensure assignees are aware of their assigned PoAs. Some countries lack effective notification systems, leaving the assignor responsible for informing assignees. Integrating PoA notifications into EUDIW could provide secure and timely updates, supporting successful cross-border PoA adoption and improving user experience.
8. In some countries, assignees must accept their PoA assignment. This could be important for verifying PoA accuracy and strengthening trust in the system. Whether, when and where PoA acceptance should occur, possibly combined with a notification, could be clarified.
9. National PoA platforms, despite eIDAS node implementation, struggle to reliably match identities, when foreigners login to local platforms. EUDIW, along with interlinking systems such as OOTS and ongoing initiatives with NCM, could resolve these issues.
10. For cross-border PoAs, national platforms must be able to match foreign PoAs mandates with local requirements. EUDIW may be used to provide the initial PoA data, while OOTS could be used to retrieve additional data if needed. Streamlining legal requirements across borders may facilitate cross-border PoA implementation.

Concluding remarks

The Nordic Council of Ministers (NCM) is well-positioned to take a leading role in addressing the challenges identified in the to-be analysis. To advance the Nordic-Baltic digital PoA landscape and align with EU initiatives, the following may be considered:

- Achieving a streamlined cross-border PoA framework within the EU may necessitate concerted efforts to ensure format and attribute compatibility with the EUDIW, foster public-private partnerships, and harmonize legal and technical standards.
- Additionally, developing clear policies could provide important guidance, while a phased, incremental implementation approach may allow for careful integration of digital PoAs into EUDIW.
- Furthermore, initiating pilots in countries with advanced digital PoA systems could help provide insights for broader application.
- Finally, targeted testing of PoA components in the EUDIW architecture may inform system development, while a dedicated focus on resolving interoperability challenges, possibly with the aid of the Once Only Technical System (OOTS), could be key for facilitating a cross border PoA landscape.

INTRODUCTION

The purpose of this analysis is to examine the current state and future potential of cross-border digital Powers of Attorney (PoAs) in the Nordic and Baltic countries. The analysis is structured around two main areas: i) an as-is assessment of the digital, legal, and social landscape, and ii) a to-be analysis exploring future scenarios, including use cases, Proof of Concept, and alignment with EU frameworks such as the EUDIW and OOTS.

With this project, the Nordic Council of Ministers wish to both increase the integration of the Nordic-Baltic region as well as align with key EU-initiatives such as the European Digital Identity Wallet (EUDIW) and Single Digital Gateway (SDG).

Context

Established in 2017 by the Nordic Council of Ministers for Digitalisation, MR-DIGITAL plays a central role in promoting digital cohesion and addressing cross-border challenges for citizens and businesses in the Nordic-Baltic region. Acting as a strategic coordinator, MR-DIGITAL is committed to achieving the shared vision of making the Nordic region the most sustainable and integrated in the world by 2030. This ambition is supported by the Digital North 2.0 declaration, which leverages digitalization to improve mobility, integration, and entrepreneurship, as well as to foster green economic growth and drive global digital transformation.

A current priority for MR-DIGITAL is the digitalization of Power of Attorney (PoA) systems in the Nordic-Baltic countries, aiming to ensure greater interoperability and harmonization across the region. PoA solutions are increasingly tied to digital advancements across Europe, where technological developments in the public sector have led to new EU regulations and initiatives, such as the European Health Data Space (EHDS), the revised eIDAS regulation, the European Digital Identity Wallet (EUDIW), and the Single Digital Gateway (SDG). These initiatives are designed to facilitate secure, efficient digital interactions for businesses, citizens, and public authorities across the EU, thus enabling seamless cross-border services and enhancing user experience.

In this context, this project addresses significant differences in PoA accessibility, governance, and legal frameworks across the Nordic-Baltic region. As PoA solutions vary widely due to differences in national governance models, legal traditions, and levels of technological readiness, the project's objective is to conduct a comprehensive analysis that identifies best practices and proposes strategies for

harmonization. By aligning Nordic-Baltic PoA systems with EU digital initiatives and strategies, this work will not only contribute to a more cohesive digital environment and strengthen cross-border digital interactions and access to services for all users in the region but also position the Nordic-Baltic area to both align with and actively influence the development of EU frameworks in this political realm, fostering greater regional integration and mobility.

Scope of the study

The scope of this study encompasses both a geographical and conceptual framework, defining the PoA concept in a digitalized Nordic-Baltic context. It covers the Nordic countries—Denmark (including Greenland and the Faroe Islands), Finland (including Åland), Iceland, Norway, and Sweden—and the Baltic countries, Estonia, Latvia, and Lithuania. These countries form the analytical scope due to the region's ambition to become the most digitally integrated in the world.

This study provides an in-depth examination of PoA within the Nordic-Baltic region, specifically focusing on digital PoA. Digital PoA refers to legally binding authorizations granted by an individual or an organization to another person or entity to act on their behalf, executed through digital platforms.

The scope also includes a detailed breakdown of PoAs digital, legal, and social dimensions:

- Digital Dimension: Analysis of digital tools and platforms that support PoA transactions across borders, enabling secure, efficient authorizations.
- Legal Dimension: Examination of the legal frameworks governing PoA in each country and the variances in governance models.
- Social Dimension: Consideration of the social factors influencing PoA adoption, especially for vulnerable and non-digital users.

Findings from Greenland, the Faroe Islands, and Åland will be included under Denmark and Finland, as their digital, legal, and social infrastructures overlap.

The report provides a two-part analysis of the PoA landscape in the Nordic-Baltic region, divided into an as-is and a to-be description.

The as-is description will contain an identification of the most frequently used digital PoAs within the sectors of health, tax and business - both for natural persons, e.g. individuals, and legal persons, e.g. companies. Subsequently, there will be a mapping of the current PoA landscape, divided into digital, legal, and social sections. The report will contain an overall cross-border description of the PoA landscape, with Annex 1 providing a detailed review of each country.

The to-be analysis is carried out on the basis of the as-is description with the modification that the to-be analysis primarily focuses on legal persons, e.g. companies. The to-be analysis will, i.a., include the following:

- Key take aways for securing future cross-border interoperability of digital PoAs.
- Insights on how new (EU?)regulation of PoAs will influence the Nordic-Baltic region
- Preparation of use-cases for EU Digital Wallet (EUDIW), including evaluation of verified credentials and attestation of attributes.
- Identification and description of a possible Proof of Concept that could be tested in the EUDIW's architecture.
- If possible, examination of other relevant interlinking systems or frameworks for providing cross-border PoAs.

Report structure

The report consists of three main sections, leading to a set of recommendations aimed at enhancing cross-border digital PoA interoperability in the Nordic-Baltic region.

Chapter 2, Methodology, outlines the study's approach, including data collection methods, scope, definitions, and frameworks for analysing the current (as-is) and future (to-be) PoA landscapes across legal, digital, and social dimensions.

Chapter 3, As-Is Analysis, investigates the current PoA practices within health, tax, and business sectors, detailing governance models, digital maturity, and accessibility variations between countries. This section identifies common challenges, such as support for vulnerable groups and cross-border compatibility.

Chapter 4, To-Be Analysis, proposes potential future developments for digital PoA solutions, including key takeaways for enhancing interoperability, use-case scenarios for the EU Digital Identity Wallet (EUDIW), and a potential Proof of Concept. This section concludes with strategic recommendations for aligning regional PoA solutions with EU initiatives.

At the end of the report, there are 4 appendices. Appendix 1 contains a thorough review of the use of digital proxies in all countries. Appendix 2 presents a list of the most used digital proxies, also distributed across all countries. Appendix 3 is a review of Frequently Used Abbreviations. Appendix 4 is descriptions on relevant regulations.

METHODOLOGY

This section provides a definition of a PoA and describes the methodology for the analysis, including data-collection, and strategy for mapping the current PoA landscape in the Nordic and Baltic Region.

Definition of a PoA

In the following section we will summarise the characteristics of a PoA. The examples used below are illustrative and the same principles apply to business using PoAs for other actions, e.g. establishing subsidiaries, managing taxes, etc.

A PoA describes a process where an *assignor*, the legal or natural person, assigning rights to the *assignee* with the purpose of obtaining a service from a third party, e.g. a sick person in need of medicine from a pharmacy. The *assignee* is a legal or natural person acting on behalf of the assignor, e.g. a family member picking up medicine. *Third parties* are other entities interacting with the assignee, e.g. the pharmacy providing medicine.

The data collection has not shown signs of formal requirements for legally binding PoA's. A PoA constitute an agreement, and verbal agreements are as a starting point equally as binding as written agreements. However, written agreements are obviously easier to document than verbal agreements. Similarly, in practice, PoA's should be in written form, as they would be difficult to utilise towards a third party in verbal form.

Digital PoAs vary in their structure and functionality and can be characterised by different degrees of digital maturity. One country could for example have digital formulars to create a PoA, where it is still necessary to interact physically with an institution to obtain it. Other countries may have digital PoAs that requires digital ID, authentication, and a digital signature to create. In both cases, the PoA would be considered being digital, however at different levels of advancement.

The definition of a PoA is for the purpose of this report interpreted in a broad scope, including – in addition to the definition described above – the rights by parents to act on behalf of their children until a certain age as well as any rights for employees to act on behalf of their employer companies.

Data collection strategy

The as-is analysis is based on data from interviews and desk research collected in the Nordic and Baltic Countries.

The data collection has been guided by a data collection tool package consisting of an analytical framework including an interview guide and a format for documenting and delivering the collected data to the core delivery team. The data collection tool package has been developed centrally to ensure that the data being collected is streamlined and comparable across countries. The data has then been collected by national experts from the respective countries of scope allowing for context-specific data collection in local language and a higher degree of cultural and national understanding of the given country, timing of interviews etc.

While the country experts were free to decide how to best answer the questions in the framework, the core delivery team recommended prioritizing interviews and desk research to obtain more detailed data.

4-6 stakeholders have been interviewed per country, and the following types of stakeholders have been interviewed:

- The NOBID contacts in each country.
- Ministries or agencies in sectors like digitization, health, taxation, or business, with digitization agencies.
- Representatives from municipalities or regions.
- Professional bodies, such as organizations representing citizens' interests in PoA-related areas.
- Relevant private actors, such as financial institutions (e.g., banks).

Additionally, a workshop with participants from the member countries was held with the objective of discussing future needs and potential gaps to close. The workshop was utilized to secure key insights to ensure further alignment and cross-border interoperability. The outcomes of the workshop will be used in the to-be analysis.

Strategy for mapping the current PoA landscape in the Nordic-Baltic Region

To highlight country-specific solutions, as well as similarities and differences across countries, Ramboll has developed a framework to aid mapping the current PoA landscape of each country's strengths and weaknesses across digital, legal and equality aspects. The framework aims to present the current as-is status per topic (i.e. digital, legal, and equality) by country, and afterwards synthesize the findings to compare the as-is situation across all countries examined.

The following section elaborates on the models for each topic area.

Digital aspects and PoA processes

To fully grasp the current state of the PoA landscape and effectively compare national PoA structures, it is necessary to describe the general PoA processes. Thus, each country report outlines the national PoA processes as-is on a general level with a focus on the following steps:

1. Access PoA (incl. verification and authentication)
2. Create PoA (incl. acceptance, storage, and costs if relevant)
3. Use PoA (incl. third party interactions)
4. Terminate PoA (incl. implications of changes to PoA if relevant).

The digital aspects of the PoA landscape per country is showcased in **table 1**. The model depicts horizontal maturity levels ranging from Basic to Fully integrated, focusing on four key technical categories to distinguish between different variations of digital PoAs. Moreover, it focuses on cross-border readiness of the digital infrastructure. The model will be used to categorise the maturity level for each technical category for the digital PoAs in each country and across.

Table 1. Maturity of Categories for Digital PoAs

Low ——— Maturity level ——— High

Category/Level	Basic	Intermediate	Advanced	Fully integrated
Access to PoA	PoA sent via e-mail or other simple service.	Accessed via shared digital public inbox or similar.	Access via a single platform solution to one or multiple sector-specific PoAs (e.g. Health PoAs).	Access is gained via a platform solution providing access to all relevant PoAs for assignor, assignee and third-party actors.
Verification	Digital document, e.g., PDF signed electronically using basic electronic signature (scanned signatures, a typed name, or a clicked checkbox.).	Secure website or App service where documents can be signed digitally using advanced electronic signature (basic e-sign, e.g., Docusign, Adobe Acrobat sign).	Signature secured using qualified electronic signature with proof of identity, e.g., national eID or provided manually, e.g., passport.	Signature secured digitally using qualified electronic signature with proof of identity, e.g., national eID. Digital identity proven automatically.
Authentication	Password or email used for authenticating identity or accessing the service.	Two-factor authentication, *(e.g. requires password and a code sent to a mobile device to access to the service and confirm identity.)*	Multi-factor or single sign on, *includes biometrics or security tokens via authenticator app or similar (e.g. Microsoft or google authenticator).*	-
Integration	Used for individual day-to-day services and agreements. Data is not interconnected with systems outside the platform.	Used for public sector or for few selected services. Data is not interconnected with systems outside the sector.	Fully used for public sector or for a single private sector *(e.g. health, business, taxation etc.)*. Data is integrated with some systems outside the sector.	Fully integrated into all digital PoA services. Data fully integrated across sectors, interconnected data exchange to all relevant stakeholder/agency systems automatically
Cross-border interoperability	Infrastructure for foreign access to PoAs in development.	Infrastructure ready for foreign access to PoAs, but not yet fully implemented.	Foreign natural or legal persons from selected EU countries have access to specific PoAs, e.g., via national eID.	All EU natural and legal persons have access to selected PoAs via EUDIW or EU approved eID.
General description of maturity level	Analogue process to sign document digitally and hand over digital power of attorney. Not particularly secure or integrated with other systems.	A digital service for signing documents and handing over digital power of attorney, that provides a more integrated and secure system. Often used for more than one service or the whole public sector.	More integrated digital PoA service with the most secure solution available for electronic signatures. Generally used across a sector such as health or the whole public sector.	Fully integrated digital PoA service used for all confirmations and electronic signatures across all digital services in both public and private sector. As well as verified using a digital ID.

This enables as-is descriptions to differentiate between the components of the national infrastructure and setup, and thus allows for better comparison with other countries. This is important, as the PoA landscape in one country may have a strong level of verification, while PoA solutions are scattered across sectors or are not integrated across (or vice versa).

Each level is defined in the model to guide the assessment and ensure a common language for the readers of this report.

Moreover, general descriptions can be related to each level:

Basic: Analogue/manual processes, e.g., to sign document digitally and hand over digital PoA. Not particularly secure or integrated with other systems.

Intermediate: A digital service for signing documents and handing over digital PoA, that provides a more integrated and secure system. Often used for more than one service or the whole public sector.

Advanced: More integrated digital PoA service with the most secure solution available for electronic signatures. Generally used across a sector such as health or the whole public sector.

Fully integrated: Fully integrated digital PoA service used for all confirmations and electronic signatures across all digital services in both public and private sector. As well as verified using a digital ID.

Legal Aspects

The legal aspects outlined below are important to the cross-border use of PoAs, as they outline the basics of if and when PoAs are legally binding or not as well the consequences thereof. Without such overview, countries would risk legal uncertainty for their citizens acting on behalf of others in other Nordic-Baltic countries.

The as is description regarding legal aspects – for each country – consists of a description of:

1. Selected legal topics
2. The status for implementation of relevant EU initiatives.

Detailed below the countries will only receive scores with regard to the status for implementation of relevant EU initiatives.

Selected legal topics

The description of legal topics include:

1. Semantics
2. Types of PoAs
3. Legal basis
4. Liability
5. Legal barriers.

The Nordic-Baltic countries have different approaches to regulation of these topics, but the countries will not receive scores in this regard. The reason being that regarding PoA different regulations cannot be viewed as "better" than others, e.g. an age barrier of 18 for using PoAs is not necessarily "better" than an age barrier of 15.

The exhaustive method for preparation of a legal description is by the use of the legal methodology entailing identification and description of the legal sources relevant to the use of PoAs. Legal sources are not necessarily easily available and may require extensive interpretation. For the purpose of this project the described legal methodology has been modified, as the respondents from each country have been used as the source for the description of the above-mentioned legal topics, and it has in many instances been challenging for country experts to find legal specialists available for interviews. Consequently, the focal points, quantity and quality of the data on legal topic may vary from country to country.

Status for implementation of relevant EU initiatives

The description includes the scale below consisting of four different levels for scores.

Table 2. Maturity of Categories for EU initiatives

Legal	Have not started	Planning implementation	Pilot phase or partly implemented	Fully implemented
EU initiatives	This is given if the Member State have not started the implementation yet	This is given if the Member State is planning how to implement the regulation	This is given if the Member State is participating in pilot projects or have finished implementing the regulation within a given sector	This is given if the Member State has implemented the regulation completely

The EU initiatives being scored for each country include:

1. Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)
2. Once Only Technical System (OOTS)
3. EU Single Digital Gateway Regulation (SDGR)
4. EU Digital Identity Wallet (EUDIW)
5. The European Health Data Space (EHDS)
6. Upgrading Digital Company Law (UDCL)

The scoring of the Nordic-Baltic countries on the parameters above is based on the collected data and supplementary desk research. Naturally, the further in the process with implementing the different EU initiatives the country is, the higher their score will be.

The initiatives EHDS and UDCL are not yet adopted at an EU level, and data regarding the implementation of the initiatives have not been available in most of the Nordic-Baltic countries. However, some countries have already started implementing the EHDS initiative and will receive scores accordingly. However, due to the initiatives not being adopted yet, any score given for the initiatives have not been included in the total score for each country.

Please note, that other regulations – not mentioned above – maybe have relevance to the use of PoA's depending on the circumstances, including the Interoperable Europe Act which entered into force on 11 April 2024. However, in order to focus the scope of the analysis, such other regulations are not given further considerations in this report.

Social inclusion

Different kinds of vulnerable users have been identified across the countries of scope. Yet, across countries it is in general elderly people, people with cognitive challenges, immigrants and non-native speakers that are highlighted as particularly vulnerable when it comes to digitalization and digital PoAs.

To promote digital inclusivity for all citizens, the Nordic and Baltic countries have implemented a range of measures to strengthen digital PoAs. Additionally, countries that have advanced inclusion measures are better positioned for cross-border collaboration, as many of these measures align with EU regulatory guidelines and allows for flexibility when using digital platforms.

The social inclusiveness scale consists of six different parameters to assess the country's degree of social inclusivity:

1. **Options for physical PoAs:** In cases where the user is prevented from making a digital PoA e.g. due to the lack of digital skills, ID/credentials, etc. there is a possibility to generate a physical PoA that often will be followed by an online registration. The parameter for inclusion is to some extent ambiguous as the solution for being digitally inclusive is going back to a physical and analogue format. However, the solution is rather handhold, thus time consuming, allowing it to include more people.
2. **English language options available:** PoAs and websites to obtain the PoAs are available in several languages incl. English. This provides increased accessibility for non-native speakers.
3. **Information Systems are adapted to people with impairments:** This includes accessibility features such as screen readers, high contrast modes, or keyboard navigation. These measures are included in the European best practice standards EN 301 549 and WCAG 2.1.
4. **Alternative access to digital ID:** The measure includes alternative digital ID provisions and/or alternative authentication methods for people otherwise unable to obtain a digital ID. This could be due to the lack of digital skills and/or lack of opportunities to obtain a digital ID, e.g. due to another citizenship, missing documentation or similar.
5. **Spokesperson/ representation of other people to obtain a PoA:** In cases where a person is hindered in creating a PoA, e.g. due to neurodiversity or lacking capabilities to understand the consequences of creating PoAs, a spokesperson or representant can create the PoA on behalf of the assignor.
6. **Education, support-service and facilitators to obtain a digital PoA**: The provision of education and trainings to support citizens in generating digital PoAs. This is especially relevant for citizens with lacking digital skills.

Table 3. Maturity of Categories for social inclusion

Social inclusion	Have not started	Planning implementation	Partly implemented	Fully implemented
Indicators	No measures or systems are currently in place to address the respective need or issue.	Strategies are being developed and plans are being considered to introduce a solution or system to meet the respective requirement.	The solution or system has been introduced and is operational in some capacity, but it is not yet complete or widely available.	The solution or system has been fully deployed, is operational across all intended scopes, and effectively addresses the respective need or challenge.

AS-IS DESCRIPTION

The as-is description identifies the most frequently used PoAs in the Nordic and Baltic regions and maps the current PoA landscape, focusing on governance differences and identifying practices, particularly for vulnerable populations and non-digital users. This analysis draws on data from the interviews and desk research conducted by national experts in each country of scope.

The analysis will cover the following themes across the country descriptions:

- **Digital aspects**, addressing differences in digital governance like infrastructure access and PoA technical standards.
- **Legal aspects**, highlighting variations in legal governance, such as liability, authorization barriers, and the legal basis for PoAs, while considering relevant EU initiatives.
- **Equality aspects**, exploring the social implications of proposed solutions, especially how different countries address representation for vulnerable and non-digital populations.

Most Frequently Used PoAs

As the first part of the analysis, the most frequently used PoAs in the Nordic-Baltic countries have been identified. The identification process consists of four steps, which are summarized in figure 1 below.

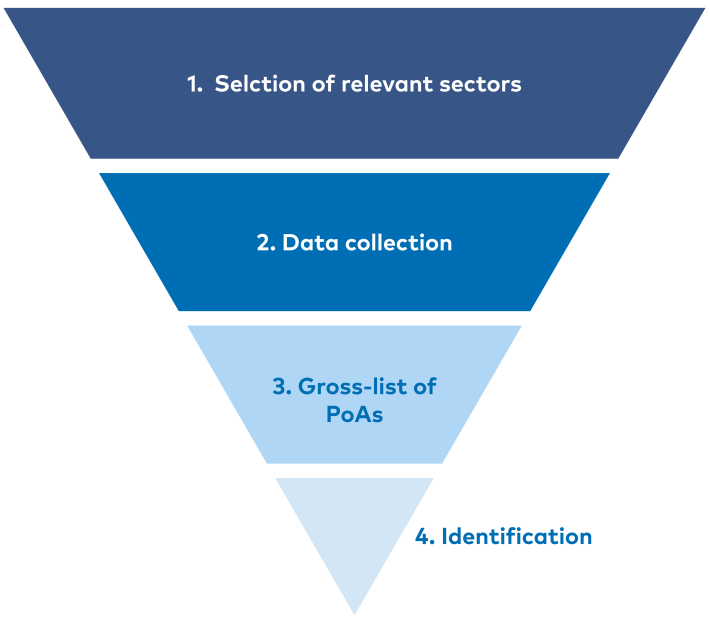

Figure 1. Identification process steps

In the first step, the analysis is narrowed down to focus on health, tax and business. The sectors have been chosen in close collaboration with Nordic Council of Ministers, including NOBID, based on workshops and interviews showing the most important sectors for PoA use.

The second step builds on an extensive data collection approach, where up to the three most frequently used PoAs in each sector are identified for all countries included in the project.

The data collection in step two results in a gross list of PoAs sorted by countries providing an elaborate overview in step three making it possible to identify similarities and trends across countries (see appendix 2 for a full overview).

The selection of the most frequently used PoAs is the result of an assessment of a number of factors.

The primary factor is the determination by country experts and their respondents regarding how frequent the PoAs are used in the respective countries. This is especially relevant for the PoA "Collecting prescription drugs" appearing as one of the most frequently used PoAs in the health sector for almost all Nordic-Baltic countries.

Other factors include insights from desk research as well as workshops and interviews with stakeholders including representatives from NOBID and national departments and authorities – These factors have i.a. contributed to the assumption that the "Parent/guardian representing a child" is one of the more frequently used PoAs in across the Nordic-Baltic countries.

Especially with regard to the tax and business sector, the data collection shows many different PoAs covering a number of quite specific tasks or actions. However, even though the PoAs concern different specific tasks, they seem very similar with regard to i.a. actors, platforms, process, regulation, equality measures etc. Thus, for the purpose of the above high-level overview, we have aggregated the PoAs to reflect the actions within "Tax affairs" and "Business management", respectively.

The described approach identifies the four most frequently used PoAs (step 4) across the relevant sectors in all Nordic-Baltic countries provided in the table below:

Table 4. The most frequently used PoAs

Sector	PoA title	Description
Health	Collecting prescription drugs	Allows picking up prescribed medicine on behalf of another person.
Health	Parent/guardian representing a child	Gives parents or guardians power of attorney over their child's medical data, allowing them to view it, make changes, book appointments etc.
Taxation	Tax affairs	Grants accountants or other trusted persons access to view and manage tax info on behalf of another person, submit annual tax returns, handle tax-related tasks, etc.
Business	Business management	Allows for CEO or other legal person to access company data, or act on behalf of the company.

Mapping of the current PoA landscape in the Nordic-Baltic Region

The level of interoperability of each country's digital PoA solutions has been assessed across the digital, legal, and social themes. The purpose of this assessment is to provide an overview of the PoA landscape in each country, including how PoAs are obtained, which systems/platforms it involves and the requirements for doing so. In total, the examination evaluates the solutions' ability to operate across Nordic countries—i.e., their interoperability. A more advanced PoA solution in legal, social, and digital aspects indicates that a country is better equipped to support cross-border functionality with its PoA system.

Table 4 provides an overview, and the three dimensions are expanded upon in their own sections below. The review will vary in depth and approach for each dimension, with the digital dimension being particularly examined . This is because the digital dimension is especially significant in working with digital PoAs, as well as in the upcoming work in the to-be analysis.

Table 5. Comparative state of integration/implementation across the Nordic-Baltic region

Focus	Denmark	Estonia	Faroe Islands	Finland	Iceland	Latvia	Lithuania	Norway	Sweden	Green-land
Digital										
Access to handle PoAs										N/A
Verification										N/A
Authentication										N/A
Integration										N/A
Cross-border interoperability										N/A
Legal										
eIDAS 2.0			N/A							N/A
OOTS			N/A							N/A
SDGR			N/A	N/A		N/A				N/A
EUDIW			N/A							N/A
Social Inclusion										
Options for physical PoAs										N/A
English language options available										N/A
Information Systems for people with impairments										N/A
Alternative access to digital ID		N/A								N/A
Spokesperson/ representation of other people to obtain a PoA										N/A
Education, support-service and facilitators to obtain a digital PoA		N/A								N/A

Scale of integration/ implementation

N/A	Basic / have not yet started	Intermediate / planning implementation	Advanced / partly implemented	Fully integrated / implemendet

The figure illustrates a comparison between all Nordic-Baltic countries examined across various relevant focus areas, based on the country reports located in appendix 1. For each focus areas across digital, legal, and social aspects, the darker the colour indicate the level of integration or implementation at the current state in each country. Further, some of these areas hints to whether the countries are geared for cross-border PoA interoperability.

Digital

In the following, there will be an overarching review of the digital landscape across countries. Each criterion that has been presented in table 5 will be described and reviewed.

Access to handle PoAs

Access to handle PoAs examines how PoA platforms are accessed, and how the PoAs can be handled domestically. This involves the technical ease of creating, assigning, and using a PoA for healthcare, business, and tax matters. The handling may vary from basic solutions where a PoA is sent directly via e-mail or similar simple services, to a fully integrated one-stop-shop for PoA management and use for all actors involved. Reaching an advanced level requires access via at least a single platform solution to one or multiple sector specific PoAs (e.g. for health), while the intermediate level depicts a less mature process, which may involve more manual steps, for instance, sending a self-developed document via public mailbox or uploading via a platform solution.

The existing processes and solutions present for gaining access to handle PoAs differ widely across the Nordic-Baltic region. All countries except Greenland have one or more platform solutions in place for citizens and companies to handle PoAs domestically, hence, no country can be considered basic in this regard. Of all countries, the currently most advanced access to handle PoAs is found to be in Finland, with Denmark, Sweden, Iceland, and Lithuania at a slightly lower level of maturity.

Most countries have multiple PoA platforms specific to the sectors of healthcare, taxation, and business, while a few have or are developing a single access point aggregating the access to handle PoAs across all public sectors. Finland has a single platform, *Suomi.fi-valtuudet*, that aggregates and presents all PoAs to be handled end-to-end. Thus, the country is considered having fully integrated access to handle PoAs. Countries with sector specific platforms include Denmark, Faroe Islands, Norway, Iceland, Estonia, Latvia, and Lithuania. Following right behind Finland, are countries like Denmark, which has a common platform (*Digital Fuldmagt*) for most public PoAs, and *MitID Erhverv* for most business matters, but a separate platform to handle taxation PoAs. Meanwhile, Sweden just launched a

similar platform (*Mina ombud*) which is not fully integrated with all the current sector specific PoA solutions yet. Iceland does not have a dedicated, central PoA platform solution, however, the central platform for public administration e-services, *Ísland.is*, serves as a single access point for handling PoAs across the three sectors, through the 'My pages' feature. Lithuania is like many others divided into sector specific platforms. The solutions allow citizens and businesses to access and handle PoAs by sector in an easy way.

Further, Estonia's central authorization management platform, *Pääsuke*, enables central authorization management, but it currently only works for healthcare matters. A solution for businesses is also being developed, to which the country shows strong progress towards the advanced level. Albeit Norway also has separate PoA platforms for each of the three sectors in question and provides access to handle PoAs, the country's PoA platforms landscape in some cases appear complicated. This leaves Norway at a slightly lower level, but ongoing developments set the direction for a more advanced access infrastructure, e.g. with the implementation of *Altinn 3.0* and the *DSOP* collaboration.

Furthermore, some platform solutions in the countries, regardless of sectors, allow both citizens and companies to access and handle PoAs end-to-end on the platform. Other countries' solutions involve PDFs, e-signatures, and e-mails, which is a decisive factor in the assessment score for digital aspects, depicted as slightly lower than countries with more developed end-to-end platform solutions.

For instance, Estonia, Latvia, and Faroe Islands also have PoA solutions segregated by sectors. Some of the solutions facilitates the PoA handling to a rather mature level, but these or the general processes face challenges or complexity compared to other countries. In Estonia, the access to handle the most frequently used PoAs described is rather well-functioning across health, taxation, and business. Nevertheless, it is common practice in the country to grant PoAs via digitally signed documents (e.g., PDFs), often sent by e-mail. In Latvia, accessing the healthcare PoA solution in *e-veseliba* allows to handle PoAs end-to-end. However, creating PoAs for taxation in *EDS* in some cases requires assignors to upload a self-created, digitally signed PoAs, which sometimes require a notary. To this, gaining access to some business matters (procuration or commercial PoAs) require a formal application with notarized approval to the authority. In the Faroe Islands, *Vangin* is accessed to handle healthcare and public matters end-to-end. Meanwhile, the taxation and business PoA solutions, *Borgaragluggin* and *Vinnugluggin* require users to fill out a PDF, electronically sign it, and sending it to the relevant authorities.

Verification

Verification is the process used to confirm that a digital identity is associated with an actual person. It is essentially a truth check that validates if an identity

corresponds to a real-life individual. Hence, this section seeks to map: **(1)** How the identity of assignees and assignors is verified to gain access to respective country's PoA platform solution(s), and **(2)** How the identity of assignees and assignors is verified when initiating a PoA transaction (i.e. creating or requesting a PoA). The digital verification of an identity can be done through different methods, each varying in the level of maturity for basic e-signatures on PDFs to fully integrated qualified electronic signatures via eIDs.

Across the Nordic-Baltic region, there is a tiered approach to the level of digital maturity for verification, which is primarily determined by the standardisation and integration of electronic identification (eID) solutions. In some countries there is a relatively mature approach with a single eID solution that works across PoA platforms (and other public and private e-services), while other countries use multiple verification methods, both digital, e-signatures and sometimes physical ID cards, to which these are considered less mature. See **table 6** for a complete overview of the different digital ID options in each country and whether they are EU notified. The eID notification process within the EU entails the incorporation of national electronic identification (eID) schemes into the eIDAS Network after a peer review to ensure compliance with the eIDAS Regulation's quality and security standards. While notification is typically mandatory for eID schemes to join the eIDAS Network, certain exceptions allow for the use of non-notified eID schemes. The responsibility for notifying an eID scheme rests with its corresponding Member State. Having a notified eID enables optimised PoA interoperability across EU countries (see further elaboration in section Cross-border interoperability).

The countries with the most advanced verification standards are Denmark, the Faroe Islands, Iceland, and Estonia. These have a single standardised eID solution that works across platforms in the public and private sectors. These countries can be considered 'fully integrated', which is the highest level defined.

Denmark is emerging as a frontrunner with a highly standardised approach, using the nationally adopted and EU notified eID, *MitID*. This is split into *MitID Privat* for individuals and *MitID Erhverv* for businesses with corresponding digital identities for both natural and legal persons. This separation ensures streamlined verification processes, using mechanisms such as physical photo IDs for initial verification of individuals, and business registration numbers alongside executive representation for businesses.

The Faroe Islands, despite not being an EU member, comply with EU standards through their eID solution, *Samleikin*, displaying a level of maturity comparable to that of Denmark.

Iceland adheres to a similarly stringent digital identification standard, relying solely on eIDs to meet the security requirements for PoA verification. The Icelandic Registry (*Þjóðskrá*) manages the critical National Identification Number

(*Kennitala*), which is a cornerstone in establishing the identity of legal and physical persons within PoA processes. The requirement to contract with certified providers and, for certain services, biometric identification further solidifies Iceland's strong verification security.

Estonia has implemented a comprehensive digital identity system that integrates mandatory EU-approved eID criteria and attributes, enhanced by a PKI solution providing high security and facilitating widespread use of public and private sector services. The range of eID carriers, including a physical ID card, mobile ID, smart-ID and digi-ID, meets the needs of both the public and private sectors. Estonian PoA verification seamlessly integrates personal identification numbers for both citizens and businesses within their eID system, indicative of an advanced stage of digital verification maturity.

The countries considered marginally less integrated are Norway, Sweden, and Latvia. While the countries all possess EU notified eIDs, which can enable cross-border solutions equally to those achieving fully integrated maturity, they also possess other verification solutions that are not EU notified. As a result of this, they can be recognised for their advanced digital verification infrastructure but have a more complex verification landscape with differing levels of maturity. Norway has an ID infrastructure with several eID options, including *BankID*, *Buypass*, *Commfides* and *MinID*, where BankID and Buypass are EU notified. These are all linked to the individual personal identification numbers of Norwegian citizens. Latvia's verification system is centred on its eID, namely the *eParaksts* card and *eParaksts Mobile*, which is EU notified, while PoA platforms also accept *SMART-ID* and internet banking methods. Similarly, Sweden's verification system emphasises a high trust level eIDs (a Swedish e-identification standard) such as the EU notified *BankID* and *Freja eID*, as well as Foreign eID.

Lastly, Finland and Lithuania's digital verification method show room for advancement, as they are evaluated to have an intermediate maturity level. In Finland, national eIDs are not in use yet. Instead, citizens log into *Soumi.fi* using their bank credentials, *mobiilivarmenne* (Mobile ID certificate) or an ID-card issued by the police. Lithuania has a diverse approach to verification, allowing for methods such as *iPasas*, *VIISP*, separate services such as bank credentials and the EU-notified eID-ATK. *ATK* is associated with a physical card with an embedded chip that can be used with a card reader or by linking the chip-enabled card within the mCard LTU application.

Looking across the Nordic and Baltic verification landscape, a spectrum of digital verification processes is evident, ranging from highly standardised and mature systems in Denmark, Faroe Islands, Iceland, and Estonia to more diverse and developing infrastructures. Nevertheless, all the countries examined can be considered above basic verification methods, hence, there is generally a high level of

maturity in digital verification across all countries. However, the divergence highlights the need for further development and possibly an increasing need for standardisation, especially given the security implications and ease of cross-border transactions within this geographical grouping.

Table 6. Electronic ID (eID) solution

Country	Electronic ID (eID) solution – EU notified in blue
Denmark	• MitID
Greenland	• MitID
Faroe Islands	• Samleikin
Norway	• BankID • Buypass • Commfides • MinID
Sweden	• BankID • Freja eID • Foreign eID • AB Svenska Pass
Iceland	• Rafræn skilríki (eID) • Auðkenni • SmartID
Finland	• Bank credentials • Mobiilivarmenne (Mobile ID certificate) • ID-card issued by the police
Estonia	• Physical ID card • Mobile ID • Smart-ID • Digi-ID card

Latvia	• eID card • eParaksts (and eParaksts Mobile) • SMART-ID • Internet bank method • EDS local username and password
Lithuania	• iPasas • ATK eID • VIISP

Authentication

Authentication involves confirming that a previously verified individual trying to access a platform is indeed the legitimate owner of the associated digital identity. This authentication is a recurring process, undertaken whenever an individual tries to access a platform solution or the services of a PoA, ensuring the user's identity matches their claim during access attempts. The authentication phase within a PoA across the Nordic and Baltic countries exhibits varying degrees of digital maturity, with some countries demonstrating advanced levels of authentication mechanisms, while others show intermediate to developing stages.

Iceland, Denmark, Faroe Islands, Estonia, and Norway can all be considered at an advanced level, utilizing, for example, multi-factor authentication mechanisms, biometrics, encryption of data, and high-security measures. None of the countries has reached the highest level, 'fully integrated' for authentication, while the advanced level is considered the highest possible according to technical standards.

Iceland's authentication maturity reaches a high maturity due to its integration of the national ID database with the eID system and the use of multi-factor authentication. This authentication mechanism is widely adopted across the public and private sectors, reflecting Iceland's strong position in digital identity authentication, despite its eID system not being notified by the EU under the *eIDAS* regulation. Both Denmark and the Faroe Islands exhibit an advanced digital PoA maturity level by using similar secure, centralized solutions to authenticate digital identity. In Denmark, *MitID* serves this purpose by requiring multi-factor authentication. In the Faroe Islands, the *Samleikin* system demands multiple personal details and upholds the same level of digital authentication maturity as Denmark. Estonia and Norway demonstrate a similar high degree of maturity, with Norway utilizing a robust eID infrastructure that includes qualified electronic signatures paired with multi-factor authentication mechanisms. Conversely, Estonia relies on eID solutions such as *Smart-ID* and *Mobile-ID*, incorporating

encryption and security measures to confirm identities across private and public services.

Finland and Sweden show an intermediate authentication infrastructure. Finland uses several robust identification mechanisms, such as bank codes, *mobile ID* and the *citizen certificate*, to facilitate logins to its *Suomi.fi-valtuudet* (e-Authorizations) platform. Meanwhile, Sweden offers several authentication options, including *BankID*, *FrejaID* and authenticator apps. Both countries are making significant efforts to improve their digital authentication frameworks. Finland, for example, is currently developing a national eID that is expected to improve authentication capabilities in the future.

Latvia can also be considered at an intermediate state for authentication, using several EU notified methods such as eID cards and *eParaksts mobile*, but does not require additional authentication for PoAs, relying instead solely on the national personal code. Similarly, Lithuanias authentication offers a wide range of options such as *iPasas*, *VIISP* alongside banking credentials etc. for access to the PoA. There are signs of progress for Lithuania, such as the introduction of a digitalized national eID and advances in multi-platform integration.

The observation highlights a spectrum of maturity in digital identity authentication for PoAs among these nations. Frontrunners such as Denmark, the Faroe Islands, Iceland, Norway, and Estonia have secured and sophisticated authentication infrastructures that are both standardised and advanced. In contrast, nations such as Finland, Sweden, Latvia, and Lithuania are in an active development phase, working to fill existing gaps and improve their digital authentication capabilities.

Integration

The category of integration examines **(1)** How the specific PoA platform solutions are integrated with other public and private platforms and systems, focusing on healthcare, taxation, and business, and **(2)** How the existing ID infrastructure is integrated with systems in the PoA landscape.

The scale in the assessment of the maturity of integration aspects goes from one off, day-to-day PoA agreements (e.g. stand-alone, signed document to be used one time), to a fully integrated environment, in which data exchange is interconnected with all relevant stakeholder and agency systems automatically. This highest level of maturity can, however, be seen as an ideal state of integration, which no country currently has achieved with respect to the PoA landscape. Nevertheless, all countries (except Greenland) have reported a certain level of integration, while two countries stand out with a more advanced level of integrated infrastructure for PoAs.

The most advanced integration level reported for PoA solutions are identified to be in Denmark and Finland. According to the data collected, the Danish and Finnish

national PoA platform solutions integrate with other public services for at least a single sector. Particularly, the primary solution for each country separately, *Digital Fuldmagt* (DK) and *Suomi.fi-valtuudet* (FI), aggregates a multitude of PoAs for almost the whole public sector and enables data exchange with third-party platforms. In Finland, the solution integrates with a range of national registries to (1) verify and authenticate digital identities and validating these against the defined representation rights, and (2) to verify the validity of PoAs in real-time, e.g. when interacting with third parties. While Finland's level of integration with a single platform function for all public PoAs, Denmark, additionally portrays a strongly integrated eID infrastructure, having a single ID solution working across all public e-services (see section Verification).

The other countries, Sweden, Faroe Islands, Iceland, Norway, Estonia, Latvia, and Lithuania exhibit intermediate integration levels. Sweden's three sector specific PoA platform solutions currently use different IT infrastructures but have APIs in place. The country is pursuing a fully integrated model, and finds its newly launched platform, *Mina ombud*, bringing together PoAs from various domains, and strengthening integrations to a more advanced degree going forward. The Faroe Islands has certain integrations between taxation and healthcare PoAs through the central *Vangin* platform, however, any further integration availability is either lacking or unknown. The country, however, relies significantly on its eID, *Samleikin*, for integration across different public and private platforms. For Iceland, PoA platforms are sector-specific (e.g., *Heilsura* and *Skatturinn*). PoAs created here are not compiled in a centralized database, but the platforms integrate with a range of e-services accessible via the central *Island.is* platform. However, no data exchange outside each sector has been reported. Norway's setup also forces citizens and businesses to handle PoAs for the examined sectors separately. Moreover, there is no central PoA archive, hence, the PoAs can only be used within the sector in which it is registered. The country is in a transitional phase towards better integration through services like *Altinn* and the *DSOP* initiative.

In the Baltics, Estonia currently relies on granting authorizations separately in each database, as no central register exist, except for the central PoA platform, *Pääsuke*. However, this only integrates with few registries, e.g., the health portal. The eID solution is moreover strongly integrated across public and private solutions, and all integrations from PoA platforms are done via APIs. Latvia's PoA platforms are also sector-specific, but the rather disparate systems hinder seamless inter-sector data exchange. The *e-veseliba* health platform works end-to-end, but the *EDS* (tax) and *Enterprise Register* (business) platforms involves PDFs. Although these can be uploaded and viewed by all actors, the information about the agreement to relevant institutions happens manually. Lithuania exhibits no direct integrations between its sector-specific PoA platforms, but the interoperability platform, *VIISP*, integrates with some State Enterprise registers, which administers PoAs. Moreover,

the PoA landscape integrates with various authentication methods, and for business PoAs can be identified via a public search engine.

Cross-border interoperability

The cross-border interoperability category focuses on the extent to which the countries in the Nordic-Baltic region handles PoAs and ID infrastructure for digital identities across national borders. It outlines whether it is feasible for foreign individuals or legal entities to create a PoA in one country and authenticate using a digital identity issued by their home country. This review applies to legal entities, individuals and individuals acting on behalf of a legal entity.

The digital PoA landscape within the Nordic and Baltic nations showcases diverse levels of interoperability for cross-border PoAs. These variations are influenced by each country's legal structures, technological progress, and engagement with European Union-wide initiatives for digital collaboration (e.g. technical implementation of the eIDAS Node and EUDIW).

Finland and Estonia stand out with a higher degree of interoperability for digital cross-border PoA solutions, demonstrating a forward-looking approach. This is primarily due to the existing integration between the two, and other EU countries[1], on healthcare PoAs, such as medical prescriptions and allowing health professionals access to view health data. These efforts are part of an ongoing eHealth initiative to allow ePrescriptions, eDispensations, and patient summaries to be fully accessible cross-border in the EU. These efforts provide a framework for cross-border PoAs within the healthcare sector. To this, Finland is preparing EUDIW to replace current banking credentials, while this is still a technically immature topic for Estonia. Foreign businesses or individuals can gain a PoA to act on behalf of businesses if they have Finnish authenticator app, which requires a user identifier (UID). Nevertheless, challenges remain, including verifying identities against other countries' databases and the limited ability to grant PoAs to foreign individuals lacking a Finnish personal identity code. Estonia has further made progress in facilitating cross-border tax and business rights, but this requires the foreign company to register in Estonia as a non-resident. A primary challenge, however, is establishing cross-border PoAs due to the absence of a central EU registry to record authorization data, making the verification of identities for assignors or assignees complex.

Norway, Denmark, and Lithuania are assessed to be just at an intermediate state in its effort to accommodate cross-border interoperability for PoAs. In Norway, the process for granting or requesting digital PoAs is heavily intertwined with national citizen credentials, which creates a barrier for foreign citizens and businesses. Efforts are underway to incorporate other EU eIDs, but the current lack of

1. Such as Croatia, Portugal, Spain, Czech Republic and Poland

integration across sectors presents additional obstacles to achieving cross-border functionality. Denmark, like all other countries, faces the significant task of establishing a reliable system to authorize non-residents, particularly those without a Danish CPR number. Current solutions, like *MitID*, could potentially align with EU regulations, but there remain issues, especially concerning tax matters for non-residents, which highlight the need for further enhancements of the system to support effective cross-border integration. As for Lithuania, its initiative with the *iPasas* service to provide authentication using an eIDAS-approved electronic identification reflects a commitment to European norms. However, since this feature has not been fully implemented, it highlights the present challenges.

On a basic maturity level, Iceland, Sweden, the Faroe Islands, and Latvia are found, which present a diverse picture of development stages within their respective PoA cross-border readiness. Iceland confronts limitations due to an outdated legal framework and financial constraints in implementing digital solutions, particularly in healthcare. However, Iceland's acknowledgment of eIDs from the EU represents progress toward greater integration. There is a recognized need for further advancements to facilitate cross-border PoAs, especially challenges related to verifying roles and rights for both the assigner and the assignee in transactions across borders. Sweden's PoA framework is in the early stages of adopting cross-border solutions, underpinned by active deliberations on their practical implementation. For now, the eIDAS Node is not applicable in the health sector, but the portal works with the taxation platforms. Demand for these services from other countries is currently minimal. Sweden is looking forward to regulatory and technological developments – for instance, the EUDIW to improve the process of accessibility and verification for cross-border identities. For the Faroe Islands, their EU non-member status introduces additional complexities in achieving cross-border integration. While they have an eID compliant with eIDAS, there's currently no support for integration with Danish systems, except for citizens with a Danish CPR number. In Latvia, inconsistent practices across various sectors and a lack of cohesive links between state institutions pose challenges for enabling cross-border PoAs. There is scepticism among some parties in Latvia and Lithuania about the feasibility of establishing an integrated system that effectively manages where data is stored on Latvia's end.

Lastly, the following countries have an EU notified eID which strengthens their possibilities for cross-border PoAs: Denmark, Faroe Islands, Norway, Sweden, Estonia, Latvia, and Lithuania. Iceland has an eID that complies with the EU regulation but is not EU notified yet. Finland does not have an EU notified eID. See **table 6** for a complete overview of the different digital ID options in each country.

The common denominator among these countries is the pressing need for legal and technological harmonisation to advance cross-border PoA solutions, supported by EU-wide initiatives such as eIDAS, EUDIW and EHDS. Active efforts are being

made to close the gaps in legal recognition, authorization, verification, and identity matching, all of which are critical elements in improving a PoA infrastructure that can operate across borders. Many of the countries have implemented the eIDAS Node technically, allowing foreign actors to login using their local EU-notified eIDs, however, without identity matching, this does not work in practice. Incremental progress, mutual recognition and refinement of the EU digital framework are essential for these countries to unlock the full potential of cross-border digital PoA functionalities.

Legal Aspects

In the following, there will be an overarching review of the legal landscape across countries. First, there will be a description of selected legal topics. Secondly there will be a general description of the status of the implementation of the EU initiatives.

Legal Topics

On a general level, the legal approach to PoA in the Nordic-Baltic countries is quite uniform and the countries share many regulation features as further described below, including i) semantics, ii) types of PoAs, iii) legal basis, iv) liability and v) legal barriers. However, the specific regulation varies to some extent in the countries and some data has not been exhaustible accessible to the country experts.

Semantics

The following table shows the most commonly mentioned assignor and assignee within the different sectors. Moreover, the most common third parties within the three sectors have been highlighted in the table below.

Table 7. Most commonly mentioned assignor and assignee within the different sectors

	Health sector	Taxation sector	Business sector
Assignor	Citizen over a given age (see legal barriers to see different age limits across the countries)	Taxpayer, pensioner, or anyone with tax obligations who wishes to delegate their responsibilities.	The legal entity or company. Could be the business itself, typically represented by a person, such as CEO, owner, or legal representative.
Assignee	Anybody chosen by the assignor	Anybody chosen by the assignor. Alternatively, an accounting company or individual capable of managing tax returns and such.	An employee, such as a CFO, an external accountant or lawyer. The assignee is authorized to act on behalf of the company in certain contexts.
Third parties	National authorities, e.g. health departments/authorities, and other actors, e.g. pharmacies	National authorities, e.g. tax departments/authorities	National authorities, e.g. business departments/authorities, or private actors, including banks

Type of PoAs

In the Nordic-Baltic region, various forms of digital PoAs are used to assign and exercise rights across the health, taxation and business sectors.

An often-occurring type of PoAs across all sectors in the Nordic-Baltic countries is the specific/limited PoA entailing an assignor assigning their rights to an assignee within a certain area. An example from the health sector is an assignor in need of prescription assigning their right to pick up an exact type and amount of medicine from a specific pharmacy before a certain date.

Another often occurring type of PoA is the general type of PoA, including the rights to handle all the assignor's affairs unless otherwise restricted. The data collection shows parents' acting on behalf of their children is the most widely used general PoA across the Nordic-Baltic countries.

Legal basis

All the Nordic and Baltic countries are based on civil law. The specific legal governance of PoA varies depending on the sector and country but the

Nordic-Baltic countries share a number of regulatory similarities.

Most importantly, the Nordic-Baltic countries seem to have a widespread use of PoA regulation through national acts, especially general acts concerning agreements, including e.g. agreements' commencement, termination, and validity. Especially, the Scandinavian general acts concerning agreements seem very similar.

These general acts seem in most countries to be supplemented by more specific acts on specific types of PoA – e.g. the Danish act on future powers of attorney – or certain sectors, e.g. the Latvian law on the rights of patients.

Furthermore, based on the data collection, the legal basis for PoAs is assumed to be governed at least in part by contractual customs and traditions as a PoA, in its essence, is simply a series of agreements between the relevant parties.

Liability

Liability for PoA use in the Nordic-Baltic countries seem to depend on the objective circumstances and subjective motives of the parties involved in a transaction making liability relevant.

Evidently, the objective circumstances include a loss for an involved party in order for a liability issue to be relevant. Otherwise, there would be nothing to be liable for. Also, the PoA must be misused, i.e. utilized in a way not intended by the assignor, in order for someone else than the assignor to be liable for the actions – in other words, if the PoA is carried out in accordance with the assignor's instructions, then no one else but the assignor can be liable for the actions occurred.

The subjective motives are, usually, that an actor in Nordic-Baltic countries must act with different types of due care or risk being liable for losses – also sometimes described as good faith or "how a normal person would have acted". Of course, an actor can be liable for a loss after deliberate misuse of the PoA, however the standard of due care means that an actor can also be liable for negligent actions, depending on the circumstances.

As shown above as well as in the country reports, this subject is not easily accessible and contain many nuances and different terminology across the Nordic-Baltic countries making a precise and in-depth legal coverage across all countries difficult.

Legal barriers

The overall subjects for the legal barriers across the Nordic-Baltic countries are quite similar and include at least the following: i) age, ii) mental capabilities and iii) resident details. Some countries also use requirements of notarization adding a layer of security.

Regarding i) age, all Nordic-Baltic countries seem to have age requirements in place, but the exact requirements are varying from 13 years to 18 years and PoA use for underage persons require parents' consent. Therefore, an otherwise legal PoA

made by a citizen under the required legal age will not be binding.

Furthermore, based on the data collection and desk research all Nordic-Baltic countries are assumed to have requirements for ii) mental capabilities, stating – in various forms and wordings – that legal PoA use is contingent on sufficient mental capabilities of the actors. Thus, citizens cannot assign their rights to other actors if they are not mentally sound.

Finally, all Nordic-Baltic countries seem to have implemented requirements regarding iii) resident details, including in most countries requirements of having a social security number before being able to apply for digital ID in order to create digital PoAs on the relevant platforms. However, at least one country has implemented measures enabling non-resident persons to apply for a digital ID. Some countries have implemented a requirement of having an address in the country. These types of requirements entail an obvious hindrance for increased cross-border use and will be described in further detail in the to-be section of this report.

EU Initiatives

This section provides an overview and an assessment of the countries' work with implementing the EU regulations listed in section Status for implementation of relevant EU initiatives in relation to PoAs. The implementation stage of these EU initiatives varies across the Nordic-Baltic countries, although all countries recognize the importance of implementing the regulations.

Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)
Across all the Nordic-Baltic countries, the revised eIDAS ("eIDAS 2.0") is being implemented. The countries are implementing the adjustments in the regulation towards 2026.

Once Only Technical System (OOTS)
According to the data collected and to European Commission's "June 2024 version of the OOTS Acceleratormeter" all the countries in the Nordic-Baltic region are currently working with the OOTS and some of the countries are very close to having a final and complete product.

EU Single Digital Gateway Regulation (SDGR)
Regarding the SDG Regulation, the data is insufficient but for the countries where we have collected data the national agencies and directorates are currently working on the implementation.

EU Digital Identity Wallet (EUDIW)
Most of the countries in the Nordic-Baltic region are participating in multiple pilot projects regarding the European Digital Identity Wallet. The pilot projects are expected to continue until either 2025 or 2026.

The European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL)

The initiatives EHDS and UDCL are not yet adopted at an EU level, and data regarding the implementation of the initiatives have not been available in most of the Nordic-Baltic countries.

Social inclusion

This section provides a cross-border overview of the current state of PoA options and support systems, with a particular emphasis on social inclusion.

It examines various aspects, including physical PoA options for individuals with limited digital skills or health conditions, the availability of English language resources to support non-native speakers, and the accessibility of information systems for individuals with impairments. Additionally, it discusses alternative pathways for obtaining digital identification and the representation options for those unable to manage their digital tasks. Finally, the section highlights educational and support services that assist individuals in navigating the PoA processes, underscoring the importance of creating inclusive environments that enable equitable access to legal resources for all.

Across the countries, different concerns have been raised when it comes to include all citizens in the digital development/solutions. The concerns are especially related to elderly people, people with cognitive challenges, people with disabilities (e.g. vision impairments) and people who do not have the sufficient documentation to obtain a digital ID or other credentials necessary to use digital services.

Although all the countries of our research have developed different solutions to strengthen the digital inclusion, some concerns have still been raised. The concerns relate to the rapid digital development and the declining in-person interaction that the digital development leads to.

A general concern has been raised about lacking digital skills and a citizen's mental and physical state to manage online PoAs, risking accidental authorizations without full understanding. Often reliant on relatives for assistance, these citizens face challenges when family members are unavailable, raising questions about legitimate consent. The lack of oversight in digital processes can make it easier for unauthorized individuals to exploit these users.

Also, relying on automated systems often removes necessary human interaction, limiting flexibility for tailored solutions. Automated processes may overlook the needs of diverse users, making it difficult for those who don't fit a typical profile, which is an argument for the countries to have the option for physical PoAs still.

Overall, while significant strides have been made in enhancing social and digital inclusion through PoA systems, continued efforts are necessary to address remaining barriers and ensure equitable access for all individuals across these countries.

Options for Physical PoAs

All countries are assessed to have fully implemented options for physical PoAs. This is because in most countries, physical PoA options are crucial for those unable to use digital platforms due to limited digital skills or health conditions.

Denmark, for example, allows physical PoAs to be issued through municipal service centres for individuals, particularly the elderly, who struggle with digital processes. Here, an authority figure digitizes the physical PoA on behalf of the user, making it more accessible. In Finland, citizens can give PoAs physically at Digital and Population Data Services Agency (DVV) offices, which then register them in a database for future digital use. If an individual cannot physically visit the office, they can assign an assistant who provides the signed PoA to the DVV on their behalf. Iceland also allows individuals without electronic ID (eID) to submit a physical PoA, which provides an essential alternative for digital inclusion.

English Language Options Available

Many countries have implemented English language options to ensure inclusivity for non-native speakers. Finland's main public platform, Suomi.fi, provides options in Finnish, English, and Swedish. Similar Estonia's main digital service portal, Eesti.ee, is available in Estonian, English, and Russian, facilitating access for the country's diverse linguistic groups.

Information Systems for People with Impairments

Countries across the board comply with the EN 301 549 and WCAG 2.1 standards for accessibility, ensuring public sector websites and mobile applications are accessible to individuals with disabilities.

Denmark, for instance, goes beyond the minimum standards, requiring feedback mechanisms and accessibility statements for all public digital content. The Danish Agency for Digitization enforces these laws, making accessibility compliance a priority. In Sweden, the Agency for Digital Government (DIGG) oversees compliance with the Act on Accessibility to Digital Public Services, ensuring that digital environments are accessible to all users, including those with disabilities.

Alternative Access to Digital ID

Alternative pathways for digital ID are being explored to include vulnerable individuals who cannot easily access traditional ID channels. These differs between countries, whether they have fully implemented alternative access, or only partly implemented it.

Denmark allows certain institutions, such as psychiatric wards, to issue or renew digital IDs (MitID) for patients, reducing the need for them to visit municipal offices and minimizing stress. Similarly, Norway offers options like MinID, BankID, and Commfides USB tokens as alternatives, providing secure access to public services. Iceland has ongoing discussions about enabling municipalities to provide electronic IDs, allowing familiar social workers to assist vulnerable individuals in accessing digital services.

Spokesperson/Representation of Other People to Obtain a PoA

For individuals unable to handle their digital tasks, countries offer representative options that allow a trusted person to act on their behalf. Most countries have fully implemented this, but some countries have not started implementing it, or are planning to implement it.

In Iceland, personal spokespersons, known as "persónulegir talsmenn," can assist people with disabilities by making decisions on their behalf, although they must be formally authorized by the Rights Protection Office to ensure credibility and prevent fraud. Finland, meanwhile, requires legal documentation for representatives, including certified PoA copies from the Office for Digital and Population Information, ensuring a legal basis for such authority.

Education, Support Services, and Facilitators to Obtain a Digital PoA

Educational and support services play a significant role in assisting individuals with limited digital skills to navigate PoA processes. Almost all countries have partly implemented this.

In Iceland, public libraries and institutions like Fjölmennt and TMF offer free digital literacy workshops and IT courses, creating inclusive spaces for diverse groups to gain digital competence. In Norway, the Digihjelpen initiative offers municipal-level guidance services at designated locations, such as libraries and service centers, specifically tailored to help vulnerable individuals with digital services.

Main takeaways

To explore future cross-border interoperability of PoA solutions, 5 key takeaways emerge from the As-Is analysis and findings.

1. Countries have varying levels of digital PoA maturity. Variations in platforms solutions to access and handle PoAs, the adoption of electronic IDs (eID), approaches to national PoA registries, and digitalization level of PoA creation, all result in differing levels of digital PoA maturity across the Nordic-Baltic region. Most countries have sector-specific platforms to handle PoAs for healthcare, taxation and business matters separately, while some has a single solution, consolidating PoAs. Further, most countries have adopted eIDs, but the level of advancement vary with some countries supporting multiple EU notified eIDs and others offering other forms of authentication and verification. The PoA registry landscape is also complex, with few countries operating with a national cross-sector PoA registry, meaning that PoAs are generally stored and registered in many different registries nationally. Finally, the digitalization level of PoAs varies, with some countries offering fully digital PoAs across all sectors via national solutions, and others relying on PDF forms signed with e-signatures. This results in a complex landscape for digital PoAs, especially with regards to cross-border interoperability.
2. Cross border interoperability is still lacking. Wide-ranging differences in PoA governance, legal standards, and digital readiness across the Nordic-Baltic countries create barriers to interoperability. The current PoA landscape in the Nordic-Baltic region is highly complex, as countries prepares for cross-border interoperability. Many countries have enabled login to national PoA platforms via an eIDAS node, allowing foreigners to login with their local EU notified eIDs. However, identification of actors is currently dependent on personal identifiers located in national registries. Thus, matching and verifying international identities of legal and natural persons remains a general challenge, as well as matching PoA mandates across borders, with only a few cases of existing cross-border PoAs. Consequently, developing cross border initiatives for PoAs is challenging. The EU initiatives regarding cross-border interoperability may help with this.
3. Engagement with EU-wide initiatives may be key. Ongoing EU-wide initiatives, including the European Digital Identity Wallet (EUDIW), offer critical opportunities for enhancing interoperability, as they include several European countries, are aligned with existing legislation, and have a pragmatic starting point, looking to solve concrete challenges. Alignment with these initiatives and leveraging their frameworks for proof of concepts can provide valuable insights and models for advancing cross-border PoA

solutions. Testing use cases and integrating verified credentials and attestation mechanisms are essential steps toward overcoming current technical and legal obstacles.

4. All Nordic-Baltic countries use the same overarching legal principles, even though these principles are applied differently across the countries and the different domestic circumstances. For instance, all countries apply the same freedom to enter into agreements, however the relevant domestic acts across the Nordic-Baltic varies depending on the countries. The legal frameworks governing PoAs in the Nordic-Baltic countries are, to a high degree, built on the same principles, including the fundamental freedom to enter into agreements. However, the application of these legal principles differs to some degree, especially regarding legal barriers, e.g. age requirements, mental capacity stipulations, and residency prerequisites. A more uniform legal approach in the Nordic-Baltics should make for cross-border easier and more available to Nordic-Baltic people and companies.
5. Progress and challenges in social inclusion vary across countries. While there are ongoing challenges in ensuring full digital inclusion, such as the risk of excluding vulnerable groups, particularly the elderly, individuals with cognitive impairments, and those with limited digital skills or health conditions, the Nordic-Baltic countries have made significant progress. The Nordic and Baltic countries have implemented various measures to improve access to digital PoAs, including physical PoA options for those who are unable to use digital platforms. Furthermore, English language resources and accessibility measures for individuals with impairments have been introduced. There are also alternative pathways for obtaining digital identification and options for trusted representatives to act on behalf of individuals who are unable to manage their digital tasks. Educational and support services, such as digital literacy workshops, have played a crucial role in assisting those with limited digital skills to navigate the PoA processes. However, concerns remain about the rapid pace of digitalization and the potential for excluding certain groups, particularly when in-person interactions are reduced. While substantial progress has been made, continued efforts are necessary to address these barriers and ensure equitable access to PoAs for all individuals across these countries.

TO-BE ANALYSIS

In this chapter, we explore the "to-be" scenario of PoAs, while remembering digital transformation within the European Union, with a particular focus on emerging solutions shaping the future of cross-border processes as a natural backdrop. The EU is actively supporting the development of key initiatives like the EU Digital Identity Wallet (EUDIW) and interconnected systems such as the Once Only Technical System (OOTS), both of which are currently under development and implementation.

The chapter begins by summarizing key takeaways from the current state ("as-is") analysis. It then explores the potential impacts of relevant legislation, examining where these initiatives currently stand on the path toward a fully digitized EU.

Two use cases derived from the "as-is" descriptions are presented to illustrate future scenarios for the two most common Powers of Attorney (PoAs). These use cases, drawn from respectively business and tax contexts, take a generic approach to highlight critical challenges that can be addressed through the integration of EUDIW and systems like OOTS.

To substantiate these use cases, a comprehensive Proof of Concept (PoC) is introduced. This PoC provides a detailed breakdown of the stakeholder journey, shedding light on both technical and procedural insights necessary for the successful integration of the EUDIW into a larger European solution framework. The PoC focuses on optimizing PoA management, examining how the EUDIW can streamline the process while addressing technical considerations for future implementation. It tracks the four key phases of PoA management—accessing, generating, using, and concluding—and identifies the roles and interactions of essential participants, including the PoA assignor, the assignee, the EUDIW, and the PoA service platform.

The effect of PoA relevant EU regulation

This section contains an assessment of the effect of PoA relevant EU regulation, including the following:

- The European Digital Identity Regulation 2024/1183 (eIDAS 2.0), including EU Digital Identity Wallet (EUDIW)
- Single Digital Gateway Regulation 2018/1724 (SDGR), including Once Only Technical System (OOTS)
- Regulation on the European Health Data Space (EHDS), COM(2022) 197, and the

- Directive on Upgrading Digital Company Law (UDCL), COM(2023) 177.
- Interoperable Europe Act?
- Web Accessibility directive?

Section Methodology aims to delineate the impact of each EU regulation by exploring the deviation between the digital standard demanded by each regulation against the pre-existing digital capacity within the Nordic-Baltic region prior to the regulations' introduction.

The assessment comprises a legal analysis of the necessary digital levels set by the EU, a comparative look at the digital maturity before these regulations, and an analysis of the impact based on the gap between the required and prior standards.

It is important to clarify our analysis does not contrast EU regulations against more rigorous potential national requirements or current implementation status. Rather, it provides a broader evaluation of what implementation may entail for EU member states, with emphasis on the Nordic-Baltic context. The analysis will be refined to articulate this scope more clearly, ensuring readers grasp the specific effects on the Nordic-Baltic states without confusion.

Methodology

The effect of each of the regulations above is uncovered by finding the difference between the digital standard required by the regulation and the actual digital level of the Nordic-Baltic countries before the implementation of the regulations above.

Thus, the first step is a brief legal analysis of the digital level required by each EU regulation, including most important requirements.

The second step involves outlining the digital readiness levels within the Nordic-Baltic region as it stood just before the new regulations took effect, detailing the existing digital infrastructure and capabilities at that time.

The third step is the comparison of the two steps above – a large difference between the required digital level and the digital level before each regulation means a large effect of the regulation, while a small difference means a small effect.

This methodology described above is illustrated below.

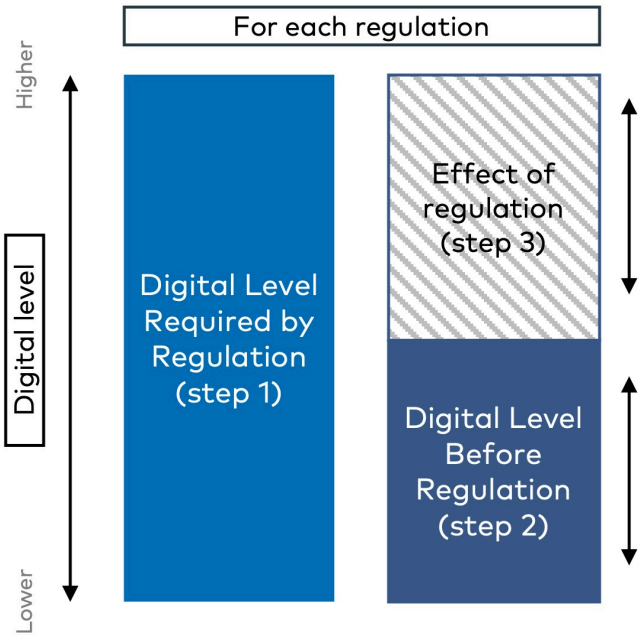

Figure 2. Methodology for assessing the effect of PoA-relevant EU regulation

eIDAS 2.0 2024/1183, Including EU Digital Identity Wallet

The eIDAS 2.0 entered into force on 20 May 2024 and is a revision of the original eIDAS regulation from 1 July 2016. The objective of the eIDAS 2.0 is to introduce digital identity solutions and new trust services, which provide access to secure and reliable electronic identification services for EU residents.

Digital Level Required by the Regulation

The regulation aims to ensure a proper functioning internal market and the provision of a proper level of security of electronic identification and trust services across the union, cf. the regulation, art. 1.

The following three subjects in the regulation are of greatest importance to cross border PoA use and is described in further detail in appendix 3 below:

i. Digital Identity Wallet
ii. Electronic attestation of attributes
iii. Unequivocal identity matching

Digital Level Before the Regulation

Prior to the adoption of the eIDAS 2.0 regulation, the original eIDAS regulation served as the regulatory framework for electronic transactions in the European

Union. The aim of the original eIDAS regulation was to establish a comprehensive EU cross-border and cross-sector framework for secure, trustworthy and user-friendly electronic transactions which embraced the electronic identification, authentication and trust services.

Despite becoming a fundamental element to facilitate a single market in several sectors, e.g. financial services and reuse of data in administrative procedures, the eIDAS had some limitations, such as limited attributes and no obligation to notify national eID schemes.

Effect of the regulation

The eIDAS 2.0, cf. above, is a major upgrade to the original eIDAS, with the introduction of the EUDIW, expansion of trust services and identity matching to facilitate cross-border interactions. The Nordic-Baltic countries are moving in tandem with the EU initiatives to enhance the digital identity and trust framework, although specific progress and readiness levels can only be accurately determined with detailed into each country's ongoing efforts and current digital infrastructure capabilities.

The journey from existing levels of digital identity infrastructure to those required by eIDAS 2.0, including the EUDIW, is a significant leap for the Nordic-Baltic countries. The new regulations pose higher levels of security, trust services, interoperability, and functionality, implying that the Nordic and Baltic countries must undertake substantial efforts to align with these enhanced standards.

The changes required by eIDAS 2.0 are not just incremental improvements; they involve comprehensive updates to the digital identity and authentication ecosystem within the EU. The introduction of the EUDIW, for example, is a pivotal element that reinforces user control over personal data, enabling secure cross-border electronic transactions, and supports selective disclosure of personal information. Such a system promotes advanced technical requirements and legal frameworks that may be challenging to implement, especially considering the diverse landscape of existing national systems and levels of digital maturity across Member States.

The eIDAS 2.0, therefore, can be seen as a catalyst for significant digital transformation within the EU's digital identity landscape, pushing Member States to both modernize and standardize their approaches to digital identity and trust services. The regulatory impact is expected to be extensive, fostering a digital single market that is more secure, efficient, and user centric.

Single Digital Gateway Regulation 2017/1724, including Once Only Technical System

The SDGR entered into force in December 2018, and three different implementation periods apply, with the general implementation deadline being December 2020. The objective of the SGDR is to establish a single-entry point where EU natural and legal persons can access information about relevant rights, rules and obligations across Member States.

Digital Level Required by the Regulation

The regulation aims to establish rules for creating a single digital gateway (SDG), providing natural and legal persons easy access to high quality information, to efficient procedures, effective assistance and problem-solving services regarding Union and national rules applicable to national and legal persons exercising or intending to exercise their rights derived from Union law in the field of the internal market. Additionally, the use of procedures by cross-border users and the implementation of the "once-only" principle, cf. (EU) 2018/1724 art. 1.

The following three subjects in the regulation are of greatest importance to cross border PoA use and is described in further detail in appendix 3 below:

i. Your Europe Portal
ii. Access to information
iii. Once-Only Technical System (OOTS)

Digital Level Before the Regulation

The Your Europe portal has existed since 2006, providing access to citizens and businesses information on EU- and national rights. However, prior to the SDGR there has been no single-entry point, with the result that EU countries often struggle to understand which rules that apply in the concrete example, or which steps are required to carry out the procedures.

As a result, looking up information was a complex and time-consuming process scattered across different websites and with various levels of quality. To combat this problem the European Parliament and the Council of the European union adopted the SDGR.

Effect of the Regulation

Assessing the distance between pre-existing levels and the required compliance standards of the SDGR, including the OOTS, it appears that Member States are facing a substantial journey ahead. The regulation aims to provide a centralized digital single-entry point for a range of services and information, procedures,

assistance services, and problem-solving mechanisms, which is a major undertaking.

Transforming the existing infrastructure to be conform with the SDGR, demands significant modifications to how information is presented and accessed online. This includes, the streamlining and digitalization of cross-border procedures, and the implementation of the "once-only" principle to reduce administrative burdens on citizens and businesses. The principle ensures that citizens and businesses only need to provide certain standard information to public administrations once, which then is reused in future interactions. The Your Europe portal will provide easy access to relevant Union and national webpages across the Member States. These elements of the regulation will have a considerable effect on the Member States, with regards to simplifying and unifying digital access to a wide range of services and information across the EU.

In summary, the SDGR including the OOTS, represent an ambitious and challenging regulation, that will lead to a shift in how citizens and businesses interact with public administrations. The regulation will have a positive impact on improving the digital single market's accessibility and efficiency, resulting in reduced administrative burdens, increased transparency, promote participation in the internal marked and likely boost cross-border activity. Consequently, the change in regulations will have comprehensive implications for the landscape and activities of cross-border PoA in the Nordic-Baltic area.

Proposals: European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL)

At the time of delivery of this report, the EHDS and UDCL constitute proposals for a regulation and a directive, respectively, and are therefore not yet finally adopted at the EU level. Thus, the effects of the proposals are described together and not in detail.

Digital Level Required by the Regulations

European Health Data Space (EHDS)

The objective of the regulation is to create a common framework for sharing and using health data across the Union (single market). It will enable individuals to take control over their health data and facilitate the exchange for healthcare delivery across the EU.

The current status of the EHDS is that the members of the European Parliament approved the creation on 24 April 2024. The provisional agreement still needs to be formally approved by the Council. Once published in the Official Journal of the EU, it will enter into force 20 days later and then applied two years after (with certain exceptions).

The following two subjects in the regulation are of greatest importance to cross border PoA use and is described in further detail in appendix 3 below:

i. Primary use of data
ii. Secondary use of data

Upgrading Digital Company Law (UDCL)
The UDCL is a proposal for a directive. The objective of the directive is to improve transparency regarding EU companies by making more information available on a cross-border basis. To enable cross-border use of trustworthy company data and lastly to modernize EU company law.

The European Commission published a proposed directive for UDCL in March 2023. The next steps regarding the UDCL involve negotiations between the Council and the European Parliament. If the directive gets adopted each EU member state will have two years to transpose it into national legislation.

The UDCL will make companies' data more easily available, enhance trust and transparency in companies across the Member States. This will create a more connected public administration and reduce unnecessary restrictions for companies and other relevant stakeholders in cross-border situations.

The following three subjects in the regulation are of greatest importance to cross border PoA use and is described in further detail in appendix 3 below:

i. Information about companies
ii. Digital EU power of attorney

Digital Level Before the Regulations

Regarding, the EHDS, there was no specific regulation prior to the proposal that addresses the cross-border sharing and use of health data. Regarding, the UDCL, there have been other EU initiatives, with the goal of digitalizing company law in the EU Member States, such as the directive (EU) 2017/1132. The UDCL is an expansion and improvement of the use of digital tools and processes in company law, with the aim to accelerate the process of digitalization in company law for EU Member States.

Both proposals will centralize data and information sharing cross-border in the EU, creating a framework that will significantly improving the efficiency and accessibility to data. Despite the Member States being in the early stages of implementing the proposals, similar national initiatives regarding EHDS and UDCL already exist. In Denmark for instance, it is possible to view health data about yourself on *Sundhed.dk*, and on *Virk.dk* you can access various company data, such as registration number, address and ownership.

Effect of the Regulations

Considering the scope and implications of the proposals, the EHDS and UDCL, the journey from the status quo to the level required imposed by the initiatives is likely be considerable and complex for the Member States. However, some of the Nordic-Baltic countries already have national registries within health data and business information, which is likely to ease the implementation process.

Shifting from the existing national efforts to being compliant with the proposals, EHDS and UDCL, will naturally require adjustments. For instance, Member States will have to ensure that individuals can exercise control over their health data and that this data can be seamlessly and securely exchanged for healthcare and research purposes. This requires substantial advancements in national digital health infrastructures, including interoperable electronic health records and robust data protection measures to uphold individual rights. Additionally, Member States will need to implement mechanisms for a standard digital EU PoA and ensure that company data is easily accessible and trustworthy. This necessitates updates to national commercial registries, legal frameworks to support digital PoAs that are compatible with the EUDIW, and systems that can validate and uphold the interoperability of these digital tools across the EU.

In conclusion, the implementation of the EHDS and UDCL proposals will have a significant impact on Member States, necessitating major infrastructural and technological enhancements. These enhancements must align with elevated standards of data governance, security, and cross-border interoperability, signalling a substantial transformation of the digital landscape within the Member States. Importantly, this transformation will include the evolution of Powers of Attorney (PoA), as these regulatory changes will implicitly shape the future framework and processes for PoA, strengthening their security, validity, and recognition across the EU.

Description of PoA use-cases

This section explores how the European Digital Identity Wallet (EUDIW) can enhance cross-border PoA processes across member states. The following two use cases are analysed:

1. Company A in Country X grants a PoA to Company B in Country Y for tax or business matters.
2. Company A in Country X grants a PoA to Company B in the same country to handle business matters for a branch in Country Y.

The sections below unfold the identified PoA use cases. The application of EUDIW and OOTS frameworks are described in the use cases as fully implementable. This is for illustrative purposes and does not reflect the maturity level or success of the relevant solutions

Use case 1: Using PoA for cross-border tax handling

Figure 2 illustrates a use case where Company A, located in Country X, requires assistance from Company B, based in Country Y, to handle its tax or business matters, such as viewing or editing tax data. This scenario highlights the potential of using EUDIW to manage and authenticate cross-border tax matters within the EU framework. The process is divided into four distinct phases.

This use case demonstrates how the EUDIW, combined with interoperable frameworks such as OOTS and eIDAS Nodes, could facilitate secure, efficient, and transparent management of cross-border business processes, ensuring mutual recognition and legal equivalence across EU member states.

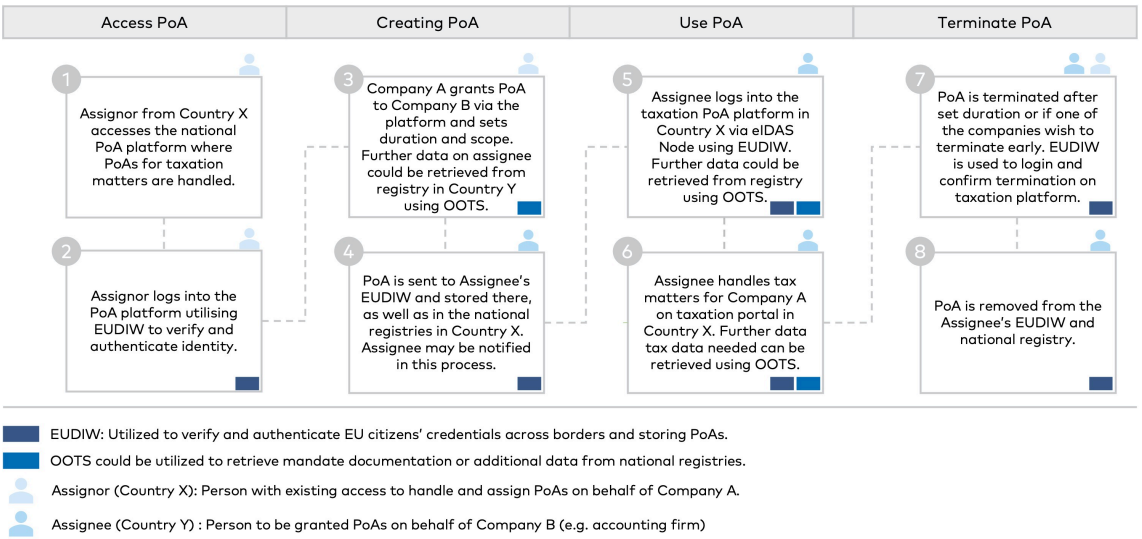

Figure 3. Company A in Country X needs Company B in Country Y to handle its tax or business matters (e.g. view/edit tax data)

1. Accessing PoA

The process begins with the assignor from Country X, who already has access rights to handle and assign PoAs on behalf of Company A, accessing their national PoA platform. This platform facilitates the management of PoAs specifically for taxation matters.

To securely log into the PoA platform, the assignor uses the European Digital Identity Wallet (EUDIW), which verifies and authenticates their credentials through

the stored digital identity, which is added when setting up the wallet via using the national eID. The EUDIW ensures secure cross-border authentication of the assignor's identity.

2. Creating the PoA

Through the PoA platform, Company A (represented by the assignor) grants a PoA to Company B (represented by the assignee) to handle specific tax-related tasks. The assignor defines the duration and scope of the PoA, ensuring that the delegation of authority is precise and limited to the agreed parameters.

As part of the process, additional information about the assignee, such as professional or business credentials, could be retrieved from the authentic source in national registries in Country Y via the Once-Only Technical System (OOTS). Once the PoA is finalized, it can potentially be securely transmitted to the assignee's EUDIW and stored there. Additionally, the PoA is registered in the national PoA registry in Country X, and the assignee may receive a notification about the granted authorization.

3. Using the PoA

When the assignee from Company B in Country Y needs to act on behalf of Company A, they log into the taxation PoA platform in Country X. This is achieved through an eIDAS Node, which enables seamless and secure authentication using the EUDIW.

While managing tax matters on behalf of Company A, the assignee may need additional documentation or mandate data. Such information could be retrieved efficiently from the relevant national registries via the OOTS framework. This ensures that all necessary data is accessible to the assignee without unnecessary duplication of effort.

With access granted, the assignee proceeds to handle tax-related tasks for Company A on the taxation portal in Country X. The platform provides secure and streamlined access to tax data, ensuring compliance with relevant regulations and preserving data integrity. If further tax-related information is required during the process, it could be retrieved using OOTS.

4. Termination of PoA

The PoA is terminated either automatically after the predefined duration expires or manually if one of the parties decides to end the agreement earlier. To confirm the termination, the involved party logs into the taxation platform using the EUDIW for secure authentication.

Once the PoA is terminated, it is removed from both the assignee’s EUDIW and the national registry in Country X. This ensures that the authorization is no longer valid, safeguarding against unauthorized use of the now-terminated mandate.

Use case 2: Using locally assigned PoA for cross-border tax/business handling

Figure 22 illustrates a use case where Company A, based in Country X, requires Company B, also based in Country X, to handle business matters (e.g., financial reporting) for its branch in Country Y. The process utilizes the European Digital Identity Wallet (EUDIW) to manage, authenticate, and validate a PoA for these tasks securely.

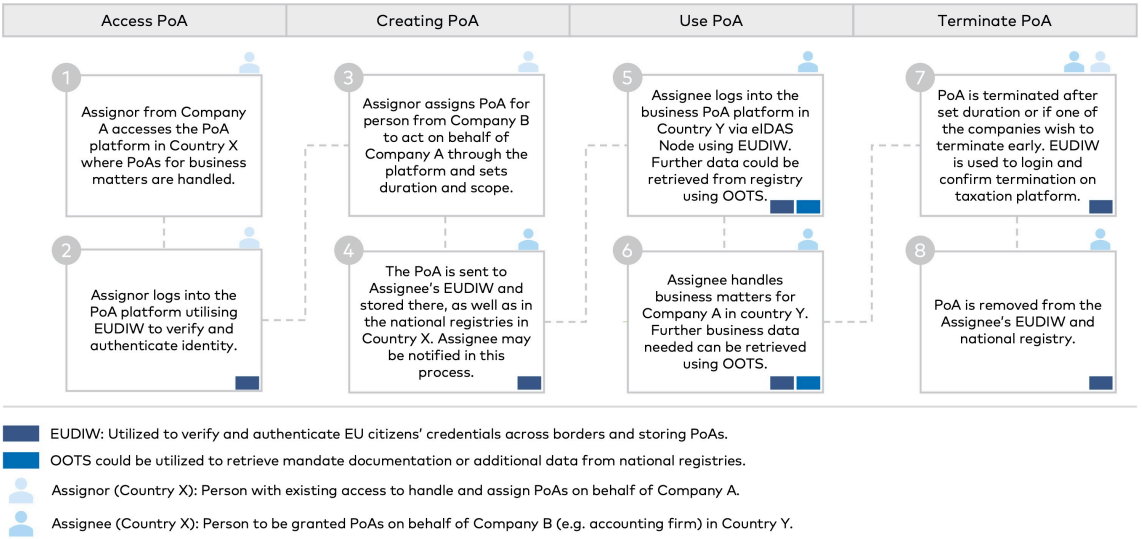

Figure 4. Company A in country X needs Company B in the same country to handle business matters (e.g. financial reporting) in branch in Country Y

1. Accessing PoA

The process begins with an authorized representative (assignor) from Company A accessing the PoA platform in Country X, which manages authorizations for business matters.

The assignor logs into the platform using EUDIW, which provides a stored verified and authenticated digital identity that is added when setting up the wallet via using the national eID. The platform validates the assignor's credentials and confirms their mandate to act on behalf of Company A. Once authenticated, the assignor is granted access to initiate the PoA process.

2. Creating the PoA

On the PoA platform, the assignor defines the PoA by selecting a representative (assignee) from Company B to act on behalf of Company A. The assignor specifies the scope and duration of the PoA, ensuring it is tailored to the specific business needs in Country Y.

Once confirmed, the PoA is securely stored in the national registry of Country X and sent to the assignee's EUDIW. The assignee is notified of the PoA and may be required to acknowledge or accept it within their EUDIW to complete the authorization process. This ensures transparency and readiness for subsequent steps.

3. Using the PoA

The assignee logs into the business PoA platform in Country Y using EUDIW through an eIDAS Node, enabling cross-border interoperability. EUDIW securely verifies and authenticates the assignee's identity, and the PoA platform confirms their authorization to act on behalf of Company A.

If additional business data or documentation is required to carry out tasks in Country Y, the platform could retrieve this information seamlessly through the Once-Only Technical System (OOTS). This ensures efficient access to relevant data while maintaining compliance with data-sharing regulations.

4. Termination of PoA

The PoA remains active until its set duration expires or until either party—Company A or Company B—initiates early termination. To terminate the PoA, the assignor logs into the PoA platform using EUDIW to authenticate their identity and confirm the termination.

Once confirmed, the PoA is removed from the national registry in Country X and the assignee's EUDIW, ensuring the authorization is no longer valid. This step maintains the security and integrity of the PoA process, ensuring no unauthorized actions can occur after termination.

Proof of Concept in the EUDIW framework

To support and validate the identified use cases for PoA, a detailed Proof of Concept (PoC) has been developed. This PoC outlines the processes each actor, human and non-human, goes through and highlights key technical and procedural observations relevant to integrating the European Digital Identity Wallet (EUDIW) into a pan-European solution architecture. The PoC focuses on demonstrating how EUDIW can facilitate and enhance PoA management, while identifying technical perspectives to guide future implementation. It involves four core stages: accessing, creating, using, and terminating PoAs, and features four key actors, the assignor, assignee, EUDIW, and the PoA platform.

The PoC revolves around the use of EUDIW to authenticate and verify digital identities, ensuring secure, seamless interactions. Additionally, the Once-Only Technical System (OOTS) is included as a potential interlinking mechanism to

retrieve mandate documentation or supplementary data from national registries, supporting cross-border operability. Furthermore, this Proof of Concept demonstrates the potential of EUDIW to streamline and secure the management of PoAs. By leveraging verified credentials, robust authentication methods, and systems like OOTS, the PoC showcases how EUDIW can potentially enhance efficiency, interoperability, and trust in PoA processes. This approach supports a unified digital identity framework, facilitating both national and cross-border interactions in a secure and user-friendly manner.

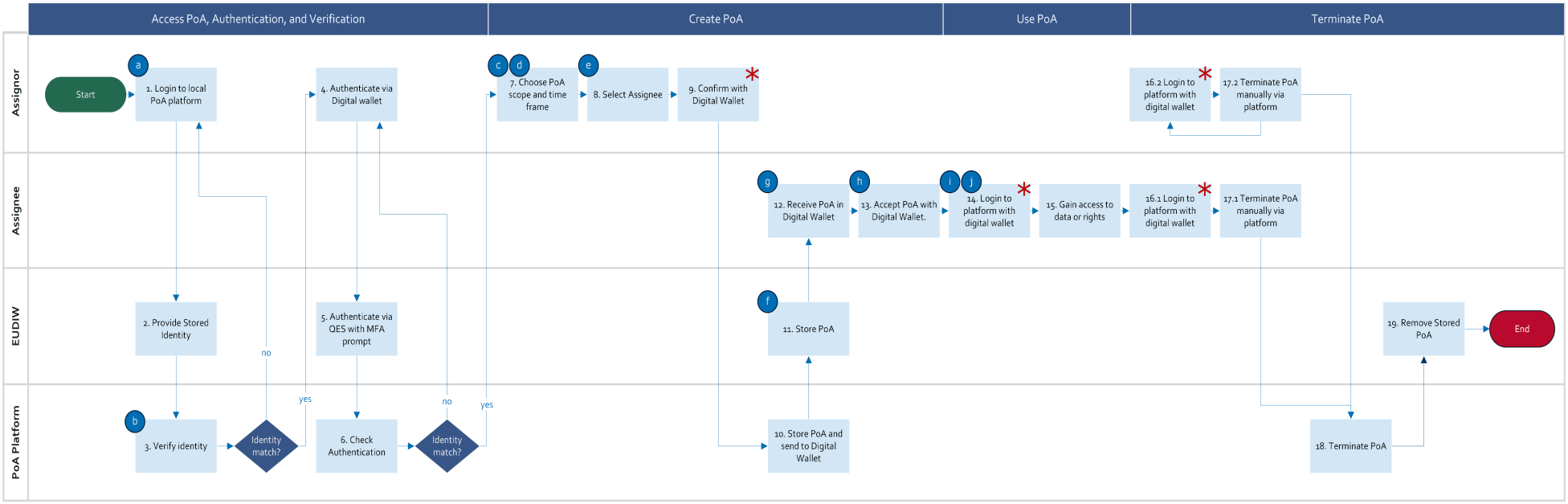

Figure 5. Proof of Concept in the EUDIW framework

Key observations

This section outlines key observations derived from the Proof of Concept (PoC) analysis, which explores the processes and challenges associated with creating, managing, and using digital PoA across borders. The observations shed light on critical areas for improvement, based on the two use cases outlined, such as cross-border identity matching, digitalization of PoA creation, identification of international assignees, data retrieval mechanisms, and the role of notifications and acceptance in PoA workflows. These findings are integral to understanding how the European Digital Identity Wallet (EUDIW) and interlinking systems can facilitate seamless cross-border PoA solutions.

(a) Login with EUDIW as a repeated process to verify and authenticate digital identity

The current login landscape requires EU-notified eID solutions, which are available in many, but not all, countries. In the target state, national EUDIWs would incorporate such eIDs as part of the solution, enabling the storage of digital identities.

In the Access phase of the PoC, the complete process for verifying and authenticating the assignor's identity using EUDIW is described. The process begins with the assignor logging into the designated PoA platform using EUDIW. EUDIW provides a verified digital identity along with the necessary attestation of attributes, allowing the platform to authenticate the user. This involves validating the assignor's identity and mandate to act, often through queries to national registries, such as business or personal registries.

Once the identity and mandate are verified, the assignor can proceed to authenticate using secure methods. These methods include Qualified Electronic Signatures (QES) with Multi-Factor Authentication (MFA) or Public Key Infrastructure (PKI). If verification fails, access is denied, and the user is prompted to restart the process. This sequence can be repeated and applied by both the assignor and the assignee at various steps, specifically steps 9, 13, 14, 16.1 and 16.2, which are marked with a red asterisk.

However, the login process differs in step 14 compared to the initially outlined procedure, as this step presents challenges related to matching cross-border identities and mandates. These challenges are elaborated in Key Observations 9 and 10.

(b) Further examine attestation of attributes to implement PoA

Currently, the attributes required to verify identities and create PoAs vary significantly between countries, with the only consistent ones being those

mandated by EU-notified eIDs. The specific attributes required also depend on the operation being performed. For instance, logging into a PoA platform generally requires basic attributes such as family name, first name, date of birth, and person identifier. However, creating and assigning a PoA demands more specific attributes, including legal status, powers, and mandates to represent legal entities.

As highlighted in section Legal Topics, member states are responsible for ensuring the provision of the required attestation of attributes. EUDIW is anticipated to accommodate most of the necessary attestations for both PoAs and cross-border PoAs. In Step 14, matching the powers and mandates to the identity of the assignee is crucial. Any additional attributes required by a local PoA provider that are not already stored in the Wallet could potentially be sourced via OOTS from local registries, but this aspect requires further investigation.

It is important to note that not all countries currently have EU-notified eIDs, and EUDIW solutions are still in development. As a result, the general maturity of these systems will need to improve in the coming years to fully enable the proposed PoC.

For reference, the attributes required for PoAs and EUDIW align with the specifications outlined in the eIDAS 2.0 Regulations 2024/1183.

(c) EUDIW May Necessitate Streamlined Digital PoA Maturity

Step (7) entails choosing PoA scope and time frame, which is already possible for domestic purposes in many countries. Ideally, standardized PoAs could be assigned, e.g. for handling tax matters, which could also underpin the validity of utilizing the PoA in another country, which is the case in *use case 2* (*Key observation d*).

However, today some Nordic and Baltic countries still rely on manual processes for creating PoAs. These processes often involve drafting PoAs as PDF documents and manually uploading them to national platforms. To speed up implementation of PoAs in EUDIW, it could thus be investigated whether EUDIW could enable the *creation* steps (7–9) and *storage* step (11) of PoAs in PDF-format, and if such could be used to validate the mandate granted to prove rights and whether the validation process can be digitalized. Moreover, it is important to understand whether the PoA would be valid in a different country, such as is required in *use case 2*. If not, it may be necessary to strengthen the digital maturity levels of PoA in some member states, e.g. enable pre-determined PoAs for rights to edit or view taxes.

Furthermore, in some jurisdictions, PoAs for tax or business matters require notarized approval, adding complexity and delay to the process. This would require the PoA to be stored on the EUDIW after notarization, adding another step to the process, or consider new possibilities for notarized PoAs in a digital perspective. For instance, increasing the level of digital PoA maturity in such countries could include the notarization process within the PoA platform. Transitioning to fully digital

platforms for PoA creation will not only enhance efficiency but also support interoperability with EUDIW, thereby enabling seamless cross-border collaboration. Considering all of this could also inform priorities on which countries to test the PoA implementation with EUDIW, and which challenges to solve in the long run.

(d) Consider how to include a foreign organisation in the PoA scope

In step (7), when the assignor needs to choose PoA scope and time frame, certain challenges can be pointed out. In *use case 2*, the assignor in country X needs to assign a PoA to a legal entity from the same country. However, the assignee must be able to use the PoA in a different country, hence, it should be considered how to include the foreign organisation (e.g. branch of the company in country Y) to the scope of the PoA on the platform (in country X). Currently, it is not possible to digitally assign a PoA in one country granting rights to access or view information related to an organizational branch in another country on a national PoA platform, unless this is outlined in a self-developed PDF.

This raises similar challenges to *use case 1* that should be considered, as data on foreign organisations could be necessary to retrieve from the local platform, when selecting a foreign entity in step (8), which is elaborated in *key observation e*. This could be achieved via the OOTS, retrieving data from relevant foreign registries. OOTS is elaborated in *key observation f*.

(e) Solve Identification and Matching of International Assignees

In step (8), the assignor selects the assignee of the PoA. This process differs from *use case 1* to *2*.

In *use case 1*, the assignor needs to assign the PoA to a foreign legal entity or natural person with existing rights to act on behalf of the company. However, creating cross-border PoAs requires mechanisms to identify and assign international assignees within national PoA platforms. Current systems often lack this functionality, which limits the ability to handle international transactions efficiently.

One potential approach to retrieve the international identity and additional details about the assignee is via OOTS from relevant international registries, ensuring interoperability between systems. Another could be to enable international assignees to log into the assignor's national platform, e.g. via an eIDAS node to request a PoA using the assignor’s business identity number (e.g., national unique identifier). This process could simplify the identification and assignment of international assignees by leveraging existing identity frameworks while ensuring the validity of the PoA.

This has no real effect on *use case 2*, as the assignor selects an assignee from the same country and using their national PoA platform, as is currently the norm.

(f) Possibility of Retrieving PoA-related Data Using the OOTS

In step (11), the proof of concept proposes that the PoA is stored locally in the assignee and assignor's EUDIW. Key data relevant to PoAs is typically stored in national registries, and in some cases, dedicated PoA registries. While EUDIW could store credentials, documents and PoAs, additional documentation may be required during the initial use of PoAs across borders. The Once-Only Technical System (OOTS) offers a potential solution by enabling the retrieval of relevant data directly from national registries, ensuring that the information is accurate and up to date. This would, however, require a link between the local registries and OOTS. Moreover, manual validation of OOTS-retrieved data may initially be necessary to confirm its accuracy. Over time, the system could be optimized to allow retrieved data to be stored securely in EUDIW, reducing redundancy, and streamlining cross-border PoA processes.

(g) Decide on Notifications

Effective notification mechanisms could be critical for ensuring that assignees are aware of PoAs assigned to them. In current systems, assignees are typically notified through national platforms, such as digital mailboxes or directly within PoA platforms. In some countries, however, there are no notifications enabled, leaving the responsibility to inform other parties (e.g., assignee) about the PoA to the assignor. To enhance this process, notifications could be integrated with EUDIW, providing assignees with direct and secure updates regarding their assigned PoAs. For instance, in step (12), once the PoA is stored securely in a national registry and assignee receives it in its EUDIW, it could be decided to implement notifications as effective communications. Moreover, this could have implications for step (13) if the assignee must accept the PoA (elaborated in *key observation h*). Regardless of the method, ensuring prompt and reliable notifications could underpin the successful adoption and operation of cross-border PoA systems.

(h) Clarify Requirements to PoA Acceptance by Assignee

In many countries, the process of creating a PoA includes an acceptance step, where the assignee must confirm their role, such as in step (13) of the PoC. This step is usually performed through the PoA platform, requiring electronic signature or eID verification. Including an acceptance phase could provide a potentially critical safeguard against errors, such as incorrectly assigned PoAs, and strengthens trust in the system. Moving forward, it should be determined whether the acceptance step is necessary. If this is the case, it would be necessary to clarify the requirements to whether acceptance should occur within EUDIW, on the local PoA platform, or through a hybrid approach. Consideration must also be given to the user experience, ensuring that the acceptance process remains intuitive and secure while serving as an effective failsafe mechanism.

(i) Investigate Cross-Border Identity matching

In both use cases, the assignee must log into a foreign platform via the EUDIW in step (14). Accessing the PoA platform locally today requires utilization of a national eID, which will be integrated into the EUDIW at the target state. However, a fundamental challenge in enabling cross-border PoAs is the validation and matching of foreign identities. While several countries already support foreign users through eIDAS login, PoA platforms and national registries often lack the capability to verify these users' identities reliably. This limitation hinders seamless international transactions and collaborations.

Implementing the eIDAS framework in conjunction with EUDIW across all participating nations holds promise for bridging this gap. The interoperability provided by EUDIW could enable secure identity matching, ensuring that assignors and assignees from different countries are validated effectively. Notably, the CBDS Programme under the Nordic Council of Ministers is addressing this issue by seeking to create practical solutions for cross-border identity matching.

(j) Resolve Cross-Border PoA Mandate Matching

In step (14) for *use case 2*, the local PoA platform must, in addition to matching a foreign identity described in observation (i), retrieve information about the PoA created in a foreign country for use on its local platform. As the PoA has been created in a different country, this constitutes a few challenges. First, the local PoA platform must be informed of the PoA, which could be achieved via EUDIW storing the PoA and presenting it to the local platform upon the assignee logging in. Second, the PoA should be compatible with the local requirements in that country, so that all the required information is presented upon request. If all requirements are not met via the PoA and attestation of attributes stored on EUDIW, additional information could be provided through the OOTS. Alternatively, a way to share PoAs across borders might be explored earlier in the process, such as in step (13), when assignee accepts the PoA, or step (10) when the local platform stores the PoA. Some of the possibilities around PoA storage are highlighted in *key observation f*. Finally, it is important to note that legal requirements for PoAs may differ from country to country and streamlining these may be key to *use case 2*.

CONCLUDING REMARKS

The Nordic-Baltic region faces challenges in creating a cross border digital PoA landscape. Specifically, the region faces an implementation of the revised eIDAS, including the European Digital Identity Wallet (EUDIW), and its integration with cross-border solutions such as the Single Digital Gateway Regulation, including the Once Only Technical System (OOTS), as well as the soon-to-be-adopted European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL). In addition, the region must address the issues identified in the As-Is analysis to meet these regulations and improve the cross-border integration of digital PoAs, with a focus on ensuring that digital PoA systems are socially inclusive and accessible to all citizens, including those from vulnerable groups.

This section synthesizes key insights from the analysis of PoA use cases and Proof of Concept, building on the As-Is analysis, shedding light on the most pressing challenges and opportunities for implementing cross-border digital interactions within the framework of the European Digital Identity Wallet (EUDIW). The findings highlight areas for further investigation and may aid in forming the foundation for shaping the next steps toward realizing a seamless and socially inclusive cross-border digital PoA landscape.

1. **PoA Compatibility:** Ensuring PoA formats and attributes across countries are compatible with the EUDIW and each other is important. Such efforts can reduce fragmentation and enhance efficiency in cross-border digital interactions regarding PoAs.
2. **Public-Private Collaboration:** The nature of the PoA solutions and maturity levels within countries require collaboration between public and private actors. Ensuring such a collaboration may be important to the eventual success of the use cases and proof of concept for the EUDIW.
3. **Legal and technical harmonization needs:** There is a need for harmonizing the legal and technical aspects of PoAs across the EU – on the one hand ensuring the same framework to be implemented in all countries, and on the other hand ensuring a uniform implementation of such framework. This includes standardizing the attributes required for identity verification and PoA creation to ensure consistency and reliability.
4. **Policy and guidance development:** Develop clear policies and guidance for both domestic and cross-border PoA practices to address issues such as mandate matching, identity verification discrepancies, and the need for additional attributes in the PoA process.

5. **Gradual Implementation:** Small, incremental steps focusing on manageable use cases, such as PoA management in limited tax or business contexts, can help uncover critical lessons while minimizing risks and complexity.
6. **Pilot Opportunities:** Countries with higher levels of digital PoA maturity are well-positioned to serve as test cases for Proof of Concepts. These can serve as proof of concepts to provide valuable insights into addressing interoperability challenges and scaling solutions regionally.
7. **Component Testing:** Testing individual elements of the EUDIW, such as attribute attestation or notification mechanisms, can provide targeted insights and inform broader system development.
8. **Interoperability Challenges:** Addressing issues related to identity matching and attribute verification across borders is fundamental. Exploring various solutions to tackle these challenges is essential, including investigating how they can be best resolved. The OOTS offers potential future solution by enabling the retrieval and alignment of data from national systems, fostering seamless cross-border processes.

By focusing on these areas, the NCM can develop a nuanced understanding of the steps needed to advance digital collaboration across the Nordic region while laying a strong foundation for scalable and sustainable solutions.

APPENDIX 1: COUNTRY REPORTS

Appendix 1 contains separate reports on each country included in the project. The reports elaborate on the topics described in the main report and include more detailed descriptions of the country-specific variations. The report follows a structured approach, first describing the key insights, and then a thorough description of the digital landscape of each country, followed by the legal dimension, and then the social dimension. Each dimension is accompanied by a visual model, as shown across countries in section Mapping of the current PoA landscape in the Nordic-Baltic Region, that assesses the progress of each country across digital, legal, and social aspects.

1. Denmark (incl. Greenland and the Faroe Islands)

The findings of the as-is description of the digital PoA landscape in Denmark show a general maturity in the country's effort across legal, digital, and social parameters, presenting a great foundation to learn from. Meanwhile, the Faroe Islands have a similar PoA landscape to Denmark with a more developing level of maturity. Greenland, on the other hand, has yet to adopt digital PoAs, hence the country was excluded from the mapping exercise.

With a consolidated platform solution for public PoAs incl. health, along with two separate platforms for taxation and business matters, Denmark showcases several advantages for the domestic handling of digital PoAs. In Denmark PoAs are widely adopted in health tax and business affairs, backed by legal frameworks like the Danish Agreement Act, and integrated with the *MitID* system. Moreover, the country is in the planning phase of implementing key EU legislation, such as *eIDAS 2.0*, *OOTS*, while *SDGR* and *EUDIW* are in the pilot phases or partly implemented. Furthermore, the identified key parameters for demonstrating social inclusion have all been partly or fully implemented across all sectors examined.

Despite mature technical standards of the digital PoA solutions, there are still challenges in 1) assigning PoAs to legal or natural persons with no strings attached to Denmark, and 2) Danish non-residents doing tax matters.

1.1 Digital and process

This section examines the maturity of technical standards and barriers across access, authentication, verification, and integration of digital PoAs in Denmark, the Faroe Islands, and Greenland.

1.1.1 Technical Standards and ID Infrastructure: Advantages and Disadvantages

The table below summarises the maturity for technical standards and barriers regarding access, authentication, verification, and integration, alongside cross-border interoperability to highlight advantages and disadvantages in Denmark, Faroe Islands, and Greenland. In the following sections, the different technical aspects are described and assessed in a country-specific context.

Table 8. Maturity for technical standards and barriers regarding access, authentication, verification, integration and cross-border interoperability

Digital	Basic	Intermediate	Advanced	Fully integrated
Access to handle PoAs		✓	✓	
Verification				✓ ✓
Authentication			✓ ✓	
Integration		✓	✓	
Cross-border interoperability	✓	✓		

✓ = Faroe Islands ✓ = Denmark

Access to handle PoAs

In **Denmark**, the PoA landscape is relatively consolidated comprising only a few central access points to various digital PoAs within healthcare, business, and taxation sectors. The key platform solution is *Digital fuldmagt* (public PoAs incl. for healthcare and business PoAs when accessing from *Virk*), along with *tastselvborger* and *tastselverhverv* (taxation), as well as *MitID Erhverv* and *Virk* (business). To a large extent, PoAs can be handled, stored, and used digitally.

Danish citizens can access and manage PoAs related to the **healthcare sector** (along with a range of other public PoAs), through the platform solution, *Digital fuldmagt*, developed by the Danish Agency for Digitalisation.

Danish **taxation** matters are divided into two platform solutions for citizen and business respectively. For citizens and residents, taxation PoAs are handled and managed on *tastselvborger*, while businesses handle them on *tastselverhverv* (from here "*TastSelv*"). On these platforms, users can choose to login to their own account or that of someone from who they have been assigned a PoA to access.

For the **business sector**, businesses can assign PoAs to employees, other organisations, and external consultants (e.g. accountants or lawyers) on the platform solutions *MitID Erhverv and Virk*. MitID Erhverv is its own solution, from which PoAs can be granted and managed, whereas *Virk* directs users to a business version of *digital fuldmagt*, working identically to *digital fuldmagt,* but with

business oriented PoAs. The PoAs can grant varying levels of access and authority, e.g. access to financial reporting, execution of business transactions or signing contracts. Within the platforms, there are different variations of PoAs. For example, a CEO may grant an accountant the right to submit tax filings or financial reports, while a legal representative may be given the power to sign contracts or register company changes. Moreover, it is possible to authorize a person to make major business decisions, such as signing contracts or establishing a subsidiary. Lastly, a business authorisation solution where, typically, a representative of a small business can grant authorisations to other organisations and employees in other organisations. The platform solutions for the business sector are rather mature since businesses have their own digital identity via *MitID Erhverv*, although this involves complexity (see verification). Additionally, the presence of two platforms increases complexity as well.

Digital fuldmagt and *MitID Erhverv* provide national solutions compiling access to many public and business PoAs for users in a simplified way, with shared infrastructure components. However, not all sectors are covered, such as taxation and other public authorities. Nevertheless, it is in the process of being implemented across all public authorities. Overall, this complexity creates challenges, as citizens sometimes must contact individual authorities separately. Moreover, the separated solutions for taxation and business matters creates additional complexity. However, *tastselvehrverv* is in the process of transitioning to MitID Erhverv, which may help reduce some of the complexity.

In the **Faroe Islands**, there are distinct platforms for each sector, *Vangin* for healthcare and public matters, *Borgaragluggin* for taxation matters and *Vinnugluggin* for business, all require the national eID, *Samleikin* for access. From *Vangin* users can manage PoAs, view digital mail, view and perform online tasks related to public services. For healthcare matters, PoAs can be accessed, granted, viewed, and used on *Vangin*, demonstrating a high level of maturity for healthcare.

Taxation matters on the other hand require a more manual process involving filling out a PDF and signing with an electronic signature, then sending to the tax authority. After processing, assignee and assignor are notified via *Minboks*, in *Vangin*, from here, the assignee can view and utilise the PoA in *Borgaragluggin* and sign in as the assignor.

For business related matters, users must log into *Vinnugluggin*, the business equivalent of *Borgaragluggin*, from here business PoAs such as power to act on behalf of a company can be granted. However, similarly to taxation matters, this is also done via the submitting of a form, rather than fully on the platform. As a result, the maturity level is high for healthcare matters, slightly lower for taxation matters and business matters, resulting in intermediate maturity for the PoA landscape in the Faroe Islands.

In **Greenland** there is, as of today, no digital PoA solution. All PoAs are analogue and signed manually. *MitID*, the Danish national eID is however in use for online Banking.

Verification

In Denmark, the verification and authentication methods are standardised for handling PoAs, as they all require the national, EU-approved eID, *MitID*. It exists in two forms, *MitID Privat* (for private citizens and residents) and MitID Erhverv (for businesses). MitID is used to access all government institutions, PoAs, as well as used to verify identity and authenticate for private services such as banking and business PoAs.

MitID Privat necessitates a national identity number (CPR), which is required for all Danish citizens and residents. When first acquiring *MitID Privat*, verification is required via a physical picture ID such as a passport or driver's license, which serves as a proof of identity. This method is characterised as a qualified electronic signature, that is the highest level of maturity. Moreover, a login with MitID to PoA services thus verifies the digital identity automatically. *MitID Privat* can also be used for business, when citizens are given rights to view or handle a business's information by logging in to *Virk or MitID Erhverv.*

MitID Erhverv is the authorization solution for businesses. It enables employees, owners, or other organisations to act on behalf of the company by logging into *MitID Erhverv* with their personal *MitID or MitiD Erhverv* identity. The eID entails different solutions, depending on various factors such as ownership. To get *MitID Erhverv*, businesses must have a company registry number, a leadership representative and additional documentation. After the first login, administrators and user rights are assigned on the platform.

In the Faroe Islands, verification to digital PoA solutions is handled through *Samleikin*, the national e-ID. *Samleikin* works similarly to *MitID privat* in Denmark, in that it provides access to all online public services. *Samleikin* is a trusted service provider and complies with the euIDAS, despite not being a member of the EU. Additionally, *Samleikin* uses QES to ensure the highest level of security when processing PoAs and other activities requiring an electronic signature. As a result, the Faroes Island's solution for verification follows a similar level of maturity to Denmark.

Authentication

In Denmark, the identity of both the assignor and assignee is authenticated using *MitID*, which acts as a centralized authentication solution. Accessing a PoA platform solution with *MitID* requires multifactor login, involving user ID to launch the *MitID* app on the phone, submitting a password or biometrics in the app, followed by approval in the app. This ensures that only the authorized individuals

can create and use PoAs. Additionally, encryption and data security measures are built in to protect personal information throughout the entire process. The authentication level can also be considered highly secure and thereby also demonstrates an advanced level of digital PoA maturity.

In the Faroe Islands, access to *Samleikin* requires the Faroese social security number, (p-tal), full name, telephone number, and a picture ID such as passport or driver's license. *Samleikin* is required for access to PoAs and therefore follows the same level of authentication maturity as Denmark.

Integration

In Denmark, the main PoA solution (Digital fuldmagt), along with the two others described (TastSelv and MitID Erhverv) integrate with other relevant third-party platforms to some extent. For instance, *Digital fuldmagt* aggregates PoAs across various sectors, and integrates healthcare PoAs to relevant platforms and entities, such as *Sundhed.dk*. This allows assignees to view the assignor's health data if a PoA has been granted via *Digital fuldmagt*. However, the solutions face challenges as the they do not sufficiently support representation by third parties. For example, it is currently not possible to grant complex PoAs, even though citizens have the right under administrative law to authorize someone in specific cases. Furthermore, Denmark is currently exploring general authorizations that are not specific, but cross-cutting to encompass both the public and private sectors. Considering the above, the Danish PoA landscape is yet to be fully integrated into a one-stop-solution but is highly advanced.

When the assignee interacts with a third party, such as a public authority or service provider, the third party verifies the validity of the PoA by checking it through the Digital Fuldmagt system. This can involve scanning a QR code, accessing the PoA digitally, or viewing documentation that confirms the assignee's authority. In this way, the third party can see the details of the PoA, such as its scope and duration, ensuring that the assignee has the correct permissions to act on behalf of the assignor.

In the Faroe Islands, the national eID *Samleikin* is integrated across public and private platforms for verification and authentication. Additionally, some integration from taxation and healthcare PoAs is possible via the *Vangin* platform, however, any further integration availability is either lacking or unknown. Therefore, integration maturity for the Faroe Islands is relatively low, except for the national eID.

Cross-border interoperability

Non-Danish eID holders can access Danish e-services like PoA solutions by linking their eID to a Danish CPR number, as a part of the implementation of the eIDAS-Node. Yet, non-residents face hurdles, as Denmark lacks a system to reliably

identify and authorize individuals without a CPR number despite some EU countries having effective registries, which presents security and identification challenges. Establishing such a system is complex and costly.

In relation to the EU's new regulations (eID, EHDS, etc.), Denmark is thus facing the challenge of integrating additional elements into its existing solutions and creating connections to other EU countries. However, the Danish PoA and MitID solutions are considered feasible to continuously be the backbone of the Danish implementation of these regulations. Even if credentials for the right to represent a party is issued in a digital wallet (i.e. EUDIW), there will still be a need for sources to verify these credentials, and the existing authorization solutions are trusted to be well-suited for this purpose.

Additionally, processing tax matters for non-residents is challenging. Despite non-residents being liable for Danish taxes and partially served by TastSelvBorger, authorizing, and registering them in the system is fraught with difficulties, complicating accurate management of their tax-related information.

For the Faroe Islands, integration with Danish systems is not currently available, however, citizens with a Danish CPR number can acquire Samleikin, the national e-ID, to access Faroese platforms. While the Faroe Islands has an e-ID compliant with eIDAS, the Faroe Islands are not an EU member state and therefore cross border integration is unlikely. Cross border integration maturity in the Faroe Islands is therefore low.

1.1.2 PoA Process

This section outlines the general process and user journey for the assignors and assignees of PoAs in Denmark.

Access & verification

Danish citizens access *Digital fuldmagt*, *TastSelv*, or *MitID Erhverv*. They log into the platforms using *MitID*, which also verifies and authenticates their digital identities.

Faroese citizens access *Vangin* or *Borgaragluggi*. They log into the platforms using *Samleikin*, which also verifies and authenticates their digital identities.

Create PoA

The three Danish platforms generally present solutions that allow citizens to assign, request, and view PoAs. Citizens can grant or request PoAs, which involves selecting assignee or assignor, defining the scope of the PoA, and setting the time limit.

For Faroese citizens, *Vangin* allows granting of PoA to view health data and other matters. Requesting PoA remains unclear. Taxation and business matters require processing of a form filled out and sent to the authorities via PDF format and signed with an electronic signature (*Samleikin*).

Use PoA

In Denmark, once a PoA is assigned to a natural person or legal person, they will receive a notification in their digital inbox (e-Boks). Thereafter, assignees can view and use the PoA within the defined scope by logging into the needed service using their own private *MitID*.

In the Faroe Islands, once a PoA is assigned, they will receive a notification in the digital inbox (*Minboks*) on *Vangin*, excepting business matters, which is unclear. Thereafter, the PoA can be used by assignees from the needed service by logging in with their *Samleikin*.

Terminate PoA

In Denmark the PoA will terminate automatically within the after the define time limit is expired.

1.2 Legal Aspects

The following section will first present an overview of legal topics, followed by a review of EU initiatives.

In Denmark and the Faroe Islands, digital powers of attorney (PoAs) are used across various sectors like health, taxation, and business, with platforms providing specific services such as vaccine registrations or tax filings. In Denmark, PoAs have a legal basis in acts such as the Danish Agreement Act, and both natural and legal persons using MitID which is a Danish eID solution. Assignors are legally bound by PoAs as long as assignees act within given permissions, but there can be liability issues if actions fall outside of these boundaries. Conditions for granting PoAs include age and mental competence requirements, and businesses need to supply additional details like CVR numbers. In the Faroe Islands, digital identity and PoAs are accessible to citizens from 13 years of age with a Faroese civil registration number. Denmark is in the planning phase of implementing key EU initiatives, such as eIDAS 2.0, OOTS, while SDGR and EUDIW are in the pilot phases or partly implemented.

1.2.1 Legal Topics

This section covers the legal topics also included in the main report: semantics, types of PoAs, legal basis, liability, and legal barriers.

Semantics

In Denmark, e.g. Danish Health Authority, SKAT (Tax Authority), the Danish Business Authority (Erhvervsstyrelsen) municipalities, or other public institutions

that provide online services through platforms like sundhed.dk, borger.dk, or su.dk as well as financial service providers or institutions, e.g. banks.

In the **Faroe Islands**, a third party could be Samleikin (National Digitalisation Programme), Minboks/Vangin (National Digitalisation Programme) and TAKS (The Faroese tax authority).

Table 9. Assignor and assignee roles across sectors

	Health sector	Taxation sector	Business sector
Assignor	Danish citizen or resident who needs assistance in managing their interactions with public authorities online.	Danish taxpayer, pensioner, or anyone with tax obligations in Denmark.	The legal entity or company.
Assignee	Family member, friend, or trusted person.	Family member, friend, or trusted person - Alternatively, an accounting company or individual capable of managing tax returns and such.	An employee, such as a CFO, an external accountant or lawyer.

Types of PoAs

The most frequently used PoAs in Denmark are specific/limited powers of attorney allowing the assignee to act on behalf of the assignor in specific matters.

For the health sector, the collected data include i.e. registering and viewing vaccinations, accessing health journals, and managing doctor's appointments. For the tax sector, the data shows citizens authorizing assignees to access their tax records, submit annual tax returns, and handle various tax-related tasks online. For the business sector, the collected data include authorizations for natural persons to execute business transactions, such as filing reports, applying for permits, or conducting administrative tasks.

Legal basis

In Denmark, the legal basis for entering and handing PoAs in general include, i.a. the Public Administration Act "Forvaltningsloven", the Agreement Act "Aftaleloven" and the unwritten legal principle "Freedom of contract" which states that all natural and legal persons as a starting point have the freedom enter into all types of

agreements. The Agreement Act is applicable in all kinds of agreements that are legally binding, however, the Public Administration Act is applicable when a PoA is used between a public administration and a citizen which ensures comprehensive coverage of representation rights.

Fundamentally, when both citizens and businesses grant a PoA, it is binding. It covers exactly what has been agreed upon. Thus, if e.g. a municipality wants to modify its authorization solution to include additional functionalities beyond what was initially intended, the existing authorization must be deleted and a new one created.

Specifically, for businesses, all authorization solutions are based on the MitID and NemLogin Act, Section 11. The law serves three purposes:

1. granting authorizations to use the solution,
2. granting permissions to make the solution available to all other authorities, and
3. exempting authorities from the competition requirement in this area, meaning they are not required to put tasks out to tender but can directly approach businesses to meet their needs.

Regarding the health and taxation sectors, there are no specific regulation besides the legal acts mentioned above. The data available to the country experts regarding legal basis regarding PoAs in Greenland and the Faroe Islands has been limited.

Liability

In Denmark a distinction is made between authorization (Danish: "Legitimation") and empowerment (Danish: "Bemyndigelse"). The authorization forms the framework for the external aspects of the PoA, while the empowerment encompasses the internal aspects of the PoA. Provided that the assignee acts within the boundaries of the PoAs empowerment and authorization, the assignor is legally bound by the agreement. However, if the assignee acts outside of the empowerment and authorization granted, the assignor will not be legally bound by this agreement - regardless of whether the third party acted in good faith.

However, there may also be a case where the assignee acts outside the empowerment but within the authorization granted. In such cases, the assignor will have entered into a legally binding agreement with the third party, provided that the third party acted in good faith. These instances will require further assessment of the specific circumstances.

Legal barriers

In Denmark, the conditions for using Digital Fuldmagt involves several criteria related to the assignor, the assignee, and the usage of the PoA itself. Below are the key conditions for the assignee/assignor of PoAs across all sectors related e.g. to age, mental health, nationality etc.

- **Age:** The assignor must be at least 15 years old to grant a digital PoA. The assignee, or the person who is going to act on behalf of the assignor, must also be at least 15 years old. An example of a specific challenge regarding age regulation was discovered during the COVID period, where permanently incapacitated children in the age 15 to 17 couldn't access their children's test results or vaccination certificates, as, according to health law, children become independent at 15. However, parents can't apply for guardianship until the child turns 18, leaving a three-year gap.
- **Mental Health:** Both the assignor and the assignee must be mentally capable of understanding the implications of granting and using a PoA. If an assignor is not mentally competent, they cannot grant a digital PoA. In such cases, other legal arrangements, like guardianship or a future PoA, might be necessary.
- **Nationality:** There are no specific nationality requirements for using Digital Fuldmagt. However, the assignor and assignee need to have access to MitID, which is a Danish eID.
- **Employment Status:** There are no specific employment status requirements for using Digital Fuldmagt. It is available for any individual who meets the other conditions as mentioned above, regardless of whether they are employed, self-employed, or unemployed.

For *businesses*, the assignor must provide the CVR number and specific information about the organization to which the assignor wants to grant the authorization, as well as the names of the individuals who will be assigned the authorization.

In the **Faroe Islands** in order to obtain a Samleikin log-in which is the Faroese eID and is required to access Borgaragluggin or for businesses: Vinnugluggin, which is the self-service sites for citizens and businesses, the citizen needs to be 13 years of age and have a Faroese civil registration number ("p-number"). To obtain a p-number or temporary p-number, the citizen needs to register with the Citizens Service in a given municipality or apply through TAKS for a temporary p-number. Further, it is stated in the Digital Identity Act, section 6, that persons who are at least 13 years old, have a Faroese p-number and can document their physical identity, have the right to become users of the digital identity. However, The Governor General may authorize persons other than those mentioned above to become users with full or limited rights to the digital identity, cf. section 6, para 2.

1.2.2 Status of implementation of relevant EU initiatives

The table below summarises the implementation status for each regulative in the Danish context. The content is unfolded in the section below.

Table 10. The implementation status for each regulative in the Danish context

Legal	Have not started	Planning implementatio	Pilot phase or partly implemented	Fully implemented
Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)		✓		
Once Only Technical System (OOTS)		✓		
EU Single Digital Gateway Regulation (SDGR)			✓	
EU Digital Identity Wallet (EUDIW)			✓	
The European Health Data Space (EHDS)		✓		
Upgrading Digital Company Law (UDCL)			**N/A**	

Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)

According to the Danish Digitalization Agency, the revised version of eIDAS is being implemented towards 2026. However, the fact that the regulation is being implemented towards 2026 doesn't state much about the status of the implementation which is why the score given is indefinite.

Once Only Technical System (OOTS)

The collected data shows the once-only principle became operational in Denmark in December 2023. However, in the European Commission's "June 2024 version of the

OOTS Acceleratormeter" it is currently in a preliminary phase where the development and integration has started.

EU Single Digital Gateway Regulation (SDGR)

According to the Danish Digitalization Agency, Denmark is working towards connecting NemLog-in with the Danish eID-gateway which is assumed to be completed in H2 2025. However, the Danish national authorities have implemented this obligation through the portals lifeindenmark.dk and BusinessInDenmark.virk.dk.

EU Digital Identity Wallet (EUDIW)

- According to the data collected, Denmark is participating in three pilot projects including EU Digital Identity Wallet Consortium (EWC), POTENTIAL and DC4EU. These projects were launched in April 2023 and cover use cases such as digital driving licenses, payments, and educational and professional qualifications. Denmark is currently in a pilot phase testing the solution and has not yet fully implemented the EU Digital Identity Wallet.

The European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL)

Grades for the implementation of EHDS and UDCL are not included, cf. paragraph **Error! Reference source not found.** above. The Danish Health Data Authority participates in two projects related to the EHDS.

1.3 Social inclusion

In the table below, it is visualized what the status is for Denmark's work with ensuring digital inclusion, while the following text elaborate what kind of measures Denmark has implemented. The table also shows what the status is on the different measures, as some of them are fully implemented while others are partly implemented. The general picture for Denmark is, however, that most of the identified measures have already been implemented in the public sector.

Table 11. Status of Denmark's work with ensuring digital inclusion

Social	Have not started	Planning implementation	Partly implemented	Fully implemented
Options for physical PoAs				✓
English language options available				✓
Information Systems for people with impairments				✓
Alternative access to digital ID			✓	
Spokesperson/ representation of other people to obtain a PoA				✓
Education, support-service and facilitators to obtain a digital PoA			✓	

1.3.1 Options for physical PoAs

Denmark has implemented options for physical PoAs which are used in cases where it is not possible for a person to issue a digital PoA. This can be in cases where elderly people are unable to create a digital PoA through a digital platform due to the lack of digital skills and/or health status. In these cases, it is necessary to have the possibility of granting a physical PoA through physical presence of, which are then digitized by an authority figure. The Agency for Digitalization has made an agreement with municipal service centers, so it is now the citizen services in municipalities that handle this task on behalf of the administration if an elderly person have struggles in the PoA process.

In the Faroe Islands, physical documents can be used when digital PoA creation is not possible. Through Borgaragluggin and Vangin it is possible to upload documents with a physical PoA.

1.3.2 English language options available

For non-Danish speakers, a version of the digital citizen platform "borger.dk" is available in English. The English version of the platform "lifeindenmark.dk" also contains links to digital attorney forms described in English.

This is the same in the Faroe Islands. On both Vangin and TAKS, English language options are available. Physical PoA documents can likewise be accessed in English.

1.3.3 Information Systems for people with impairments

Since 2007, Denmark has implemented website accessibility.[2] In 2018, the EU Web Accessibility Directive, which mandates compliance with EN 301 549, was effectively implemented. The part of EN 301 549 that covers web is WCAG 2.1 Level AA, ensuring that public sector websites, mobile apps, and other digital content are accessible to people with disabilities. Denmark's Agency for Digitization oversees the enforcement of these accessibility laws, and organizations are required to maintain accessibility statements and provide feedback mechanisms for users who encounter issues.

The Faroese digital infrastructure, including Vangin and Borgaragluggin, complies with the Web Content Accessibility Guidelines (WCAG) 2.1, ensuring high contrast, keyboard navigation, and screen reader compatibility.

1.3.4 Alternative access to digital ID

Certain institutions, such as psychiatric wards, are authorized to establish or renew patients' digital ID (MitID), reducing stress and saving resources by eliminating the need for patients to visit municipal offices. This decentralized approach to digital ID has been partially implemented, offering a more convenient and less anxiety-inducing experience.

If you live in the Faroe Islands, it is mandatory to have a P-number. If you have a P-number, you can access all digital PoA services.

1.3.5 Spokesperson/representation of other people to obtain a PoA

For citizens unable to manage their digital tasks, systems are in place allowing relatives or guardians to handle PoAs on their behalf. Through the digital PoA system, the designated representative can act for the assignor using their own digital ID (MitID). This system is fully implemented in the public sector.

---

2. Web Accessibility in Europe: The Full Compliance Guide (2024)

In the Faroe Islands, representation for creating PoAs is possible under specific guidelines. Borgaragluggin allows citizens to assign PoA for tax-related tasks, either through its portal or via physical documentation. A Samleikin ID and P-tal are required, and PoA validity is typically up to three years, with renewal options available.

1.3.6 Education, support-service and facilitators to obtain a digital PoA

Several municipalities have introduced advisory services to help citizens and their families understand and create digital PoAs. These services often involve structured, well-organized meetings to ensure that vulnerable individuals and their relatives receive the support they need. While education and support services are available, their implementation varies across municipalities.

In the Faroe Islands, some training videos have been developed for creating digital powers of attorney. Some are fully implemented, while others are awaiting final approvals before being made public.

2. Estonia

The findings from the examination of Estonia's digital PoA frameworks show a nuanced level of maturity in the country's efforts across technical, legal, and social parameters, creating a notable basis for comparison and learning.

Estonia possesses a diverse array of platform solutions to manage PoAs, including specialized systems for handling healthcare, taxation, and business matters. There is a commendable level of technical advancement with the integration of Estonia's ID infrastructure with PoA systems, supporting access, authentication, verification, and cross-border interoperability; though the entire landscape is noted to be fragmented and could benefit from further integration.

In terms of legal frameworks, Estonia operates under a detailed regulatory environment governing PoAs, with a focus on liability based on good and bad faith, and specific constraints ensuring that PoA transactions are limited to individuals with valid eID tools. The country also demonstrates active participation in EU initiatives, with full implementation of Once Only Technical System (OOTS), while other initiatives like eIDAS 2.0, SDGR, and EUDIW are in varying stages of planning and pilot implementation.

Estonia has also made significant strides in promoting social inclusion, with services available in multiple languages, systems tailored for people with impairments, and support mechanisms for those seeking to obtain or act under a PoA.

Nevertheless, Estonia is facing particular challenges with: 1) the establishment of PoAs for non-residents or entities outside of Estonia due to the current system's requirement for an Estonian personal identification code; and 2) the verification and trust issues concerning international PoAs where no centralized EU registry is present to facilitate seamless cross-border authorization.

2.1 Digital and process

This section examines the maturity of technical standards and barriers across access, authentication, verification, and integration of digital PoAs in Estonia.

2.1.1 Technical Standards and ID Infrastructure: Advantages and Disadvantages

The following describes the maturity for technical standards and barriers regarding access, authentication, verification, and integration, alongside cross-border interoperability to highlight advantages and disadvantages in Estonia.

Table 12. Estonia's maturity for technical standards and barriers

Digital	Basic	Intermediate	Advanced	Fully integrated
Access to handle PoAs		✓		
Verification				✓
Authentication			✓	
Integration		✓		
Cross-border interoperability			✓	

Access to handle PoAs

In Estonia, the PoAs are handled separately with each service provider (e.g., for an accountant in the e-Tax Board, citizens in the Health Portal). Citizens who possess an Estonian personal identification code can also use the Central Authorization Management System *Pääsuke*, which is built into the State Portal, *eesti.ee*. However, this platform solution currently only provides access to handle healthcare related matters. Moreover, the most common practice in Estonia is to issue PoAs via digitally signed documents, which are often sent by e-mail (e.g., in PDF format). Thereby, the PoA landscape is fragmented onto several platform solutions, which currently only enables a few PoA services end-to-end. Thus, the access can be considered between basic access to slightly advanced solutions, to which the maturity level of access to handle PoAs can be considered at the intermediate level.

In the **Healthcare sector**, patients can log into the Health Portal, *terviseportaal.ee*, or *Pääsuke* to grant PoAs.

Companies' **Taxation matters** can be performed within the Tax and Customs Board e-services environment (e-Tax Board, eMTA). The legal representative of the

company (management board member) or the access rights manager in the e-Tax Board environment can from here grant a person PoA within the scope of e.g., the accountants data package, including individual rights. The Management Board Member can also assign the rights as access rights manager.

For **Business matters**, generally a board member automatically is granted the right to act on behalf of the company, since this data is publicly available in the business register. To this, PoAs can be granted within separate platform solutions, e.g. to submit annual reports or for mandatory statistical data to state (managed in *eSTAT*).

For businesses, a solution for authorizing is also under development, which would allow these to grant PoAs to information in public registry related to their company to another company. Although this could reduce administrative tasks for companies, many are reluctant to incorporate such a service into their business processes due to concerns about data leakage. Particularly, when data is related to sensitive business information.

All platform solutions are accessible on various devices, including computers, smartphones, tablets, and other smart devices. They support all major operating systems, including Windows, macOS, Linux, iOS, and Android.

Verification

In Estonia, citizens are granted with a personal identification number (from here: ID-code) from the government, representing individuals both physically and digitally. Moreover, they receive a mandatory physical ID card, along with eID carriers such as the mobile ID, Smart-ID and Digi-ID card additionally. These covers all the mandatory attributes of EU-approved eIDs (i.e. Family name, First name, Data of birth, Person identifier). Citizens cannot acquire a digital ID without first having gone through the identification process for the physical ID.

The ID card uses a PKI solution where a private key is generated and stored within a chip, used to sign and authenticate, which is protected with respective pin codes. The eID is used for e-identification, e-signing, and a secure transfer of sensitive data. It allows to securely use a multitude of public and private sector e-services. Using the eID is a qualified electronic signature, which is the equivalent of signing a document physically, hence, the solution is highly mature.

Estonian citizens incl. representatives of businesses (e.g. board members) log into the respective PoA solutions by using one of the eID methods to verify their identity. Here, the attestation of attributes entails the Estonian personal identification number. To be granted a PoA requires name and ID-code (citizens), or name and registry code (companies). For business PoAs in the LHV self-service platform, it is also possible to login using PIN-calculator, password, or biometrics. If citizens have been granted the right to represent a legal entity via PoA, they can perform actions on behalf of the legal entity automatically.

Authentication

In Estonia, the authentication is done via the eID cards (i.e. Smart-ID, Mobile-ID, etc.). Encryption and data security measures are built in to protect personal information throughout the process. This authentication method, integrated across private and public services, can thus be considered highly secure, demonstrating an advanced level of authentication.

For companies, there is no dedicated eID tool, but authentication certificates are issued, which are primarily used for server-to-server authentication.

The X-Road environment (a secure data exchange between public databases), the state's authentication service TARA, and the LDAP protocol for identity verification work together with the state's Single Sign-On (SSO) service (GovSSO). For end-user interaction, the system utilizes UserNt. The content management of the state portal is handled by the Grav-CMS software, while the data exchange is facilitated by the Ruuter component.

Integration

In Estonia, the existing ID infrastructure and databases used by the PoA solutions comprise the Business Register, TARA, X-Road, the Population Register, *State Portal*, and *Pääsuke*. The rest of PoAs are handled on a case-by-case basis, as PoAs generally must be granted separately in each database in cases where such possibilities exist.

The PoA platform solutions are not integrated with a central registry from which national databases can pull authorization information. Thus, Estonia currently relies on granting authorizations separately in each database as the only solution. One exception is the central Authorization Management System, *Pääsuke* which currently only integrates with a few data registries, such as the Health Portal. The only other case is for publicly available data of company board members listed in the Business Register, which integrates with the related platforms using APIs.

All the most frequently used digital PoAs integrates through APIs. For some taxation and business matters, manual entry is necessary if the processes have not yet been automated.

The integration with eID is strongly advanced, as it is applicable across all PoA solutions (alongside most other public services). The eID can identify individuals against the Population Register.

Cross-border interoperability

In most cases, PoAs can only be granted to individuals who possess an Estonian personal identification code. This includes PoAs in the Health Platform. However, Estonia is a part of a cross-border initiative, digital prescription, which addresses

this limitation to make prescriptions available in certain EU other countries (e.g., Finland). This service allows a patient to buy prescribed medicines in a pharmacy of another EU country that is a part of the service.

Moreover, Estonia takes part in another cross-border initiative that enables the exchange of patients' health data across borders. In a nutshell, it is possible to forward a summary of the health data allowing the transmission of the most important medical information of a patient to a healthcare professional in some specified EU countries. Lastly, healthcare professionals from the EU automatically have access to the patient's Health Portal.

For some taxation and business matters, it is possible to grant access rights across borders (e.g. a foreign accounting firm), but this requires the foreign company to register in Estonia as a non-resident, since authorizations cannot be granted to an unregistered person or entity. As for citizens, all company-related operations require an Estonian ID-code. Similarly, a PoA to legally represent the company for tax matters can be granted to a foreign individual, but an account must first be created in the e-Tax/e-Customs system. Use cases related to third countries are not currently resolved.

Countries within the eIDAS framework can gain access through the eIDAS Node to e.g. *Pääsuke*, but the PoA solution is not supported. According to the data collected, it is practically impossible to verify the validity of international PoAs, as this is a question of trust in the system itself. For Estonian individuals, it is straightforward to validate whether the signature is valid or not. For PDF signed PoAs, this poses a challenge to validate signatures and PoAs. Signatures can only be verified through the DigiDoc solution. Nevertheless, not all signatures are accepted.

The eIDAS Node will be complemented by the upcoming EUDIW solution once it has been implemented. To correctly identify individuals, the eIDAS Node should be accessible, and further steps would depend on a case-by-case basis, determining how and if databases are integrated.

EUDIW would allow a natural person to act on behalf of a company, but in Estonia this is still a technically immature topic, therefore it is too early to make assessments.

The eIDAS 2.0 initiative is considered necessary infrastructure to enable cross-border PoAs. However, to distribute a digital PoA within information systems or Wallets, a system or registry for validating and defining authorization rights is paramount. Such a system could generate an attestation of attributes. However, there is also a challenge regarding how the individual would use the PoA from a Wallet solution. If the individual upload their data into a Wallet solution to be shared with other systems, this would either require a registry, alongside an API integration for service providers to e.g. generate the attestation of attributes and distribute the PoA.

Further, the primary challenge is currently establishing a PoA. Since there is no central EU registry recording authorization data, it is complex to verify the identities of the assignor or assignee. Moreover, data protection comes into play, as the sensitivity of information varies across different systems and countries. It needs to be considered how the authorization is presented, or whether there is simply a hint that Person A can, for example, retrieve a prescription on behalf of Person B with a specific number (from the pharmacy). There is a need to evaluate how data sensitivity is currently protected and how it could be handled in the future when, for example, a Wallet is implemented.

2.1.2 PoA Process

Access & verification

Citizens and businesses log into the platform solution needed, e.g., *Pääsuke*, *terviseportaal.ee*, *e-Tax*, *LHV*, or *eSTAT*, *e-Äriregister*. When entering the platform, they are prompted to use an eID mean, such as Smart-ID, Mobile-ID, or an ID card. For business PoAs in the LHV self-service platform, it is also possible to login using PIN-calculator, password, or biometry.

In most cases, the assignor can set the scope of rights within a given PoA (e.g., which health data the assignee can view, or which specific tasks one can perform related to tax matters).

Create PoA

Citizens create PoAs in the separate platform solutions, e.g. a patient can authorize trusted representatives to act on their behalf, e.g. pick up medicine or view health data, in the Health Portal, *terviseportaal.ee*. However, it is not possible to request a PoA (by the assignee's initiative). The rights of the assignee (such as document viewing permissions) can be restricted on a case-by-case basis for individual documents). Notifications are not provided in the health portal.

Company board members listed on the company registration card automatically has access and may grant PoAs in the State Portal. It is not possible to request authorizations or add rights to oneself. For *LHV*, the board members receive notifications to the company account, meaning the bank's self-service portal inbox, or to the board member's email.

Since none of the PoAs are notarized, no fees apply.

For most of the solutions, the process for refusing or accepting consent to the PoA does not exist. For instance, if the assignor has granted the PoA to an assignee, the assignor's data automatically appears in the assignee's view in the Health Portal.

Use PoA

Assignees of PoAs related to viewing health data will be able to view the assignor's health data in the Health Portal.

To pick up medicine at pharmacies, the pharmacist checks the data's accuracy based on the personal identification code through the prescription centre. For online pharmacy matters, the PoA is proved upon logging in with an eID method to verify the identity of the assignee.

For businesses, upon first use the legal representative of the company must register as a user in eSTAT. After that, the user with the CEO profile can submit data and manage (add, modify, block) data submitters. The CEO can create and delete main user, data submitter, and password-protected data submitter rights in *eSTAT*. The PoA acceptance/rejection process does not exist.

Terminate PoA

The assignor can revoke health PoAs in the authorization management information system. Some PoAs, e.g. pick up medicine or view health data is per default without expiration date, however, the patient or their fully authorized representative in the Health Portal can revoke the PoA at any time.

For business purposes, PoAs can be granted indefinitely or for a specified period (with a start and end date). Management board members of access right managers can modify or revoke these PoAs.

A management board member's PoA (automatically granted by the e-Business Register) remains valid as long as the company is registered in the Business Register. When actions related to a PoA (granting, revocation, renunciation, delegation of PoA) are performed, the system sends notifications about the changes to the relevant parties (legal entities or individuals) through the national mailbox. The national mailbox forwards all messages to the email addresses that the individual or legal entity has designated for their national mailbox.

2.2 Legal Aspects

The following section will first present an overview of legal topics, followed by a review of EU initiatives.

In Estonia, specific, limited and general powers of attorney (PoAs) are used across the health, taxation and business sectors. There are several regulations that governs the different sectors, but generally PoA matters are regulated by the General Part of Civil Code Act (Tsiviilseadustikuüldosa seadus, TsÜS) or the Law of Obligations. Liability in Estonia is assessed based on good and bad faith, where it is

e.g. assessed if the assignee has made a human error or exceeded to scope of the PoA. Generally regarding barriers within the health, taxation and business sectors, the individual must have a valid Estonia eID tool, and not being underage or of limited legal capacity. Overall Estonia is doing well with the implementation of the different EU initiatives and seems to be among the countries that have reached the furthest with the implementation. Estonia is currently in the process of implementing key EU initiatives, having already implemented the OOTS, while being in the planning phase or participating in a pilot project for the others.

2.2.1 Legal Topics

This section covers the legal topics also included in the main report: semantics, types of PoAs, legal basis, liability, and legal barriers.

Semantics

Table 13. Role descriptions of various sectors

	Health sector	Taxation sector	Business sector
Assignor	The physical person who is either the recipient of the prescription or patient	The legal representative of the company, such as a management board member and access rights manager, or the Estonian Tax and Customs Board (EMTA)	The legal representative of the company, such as a management board member
Assignee	A delegated person, usually family or close relative of the person granting the authorization. In case of guardianship, a social worker from the local municipality	The legal representative of a company or the company accountant/accounting service provider	Natural person like an accountant or whom the legal entity has granted rights for entering/submitting the annual report. Could also be the company's main user

Types of PoA

Regarding prescription rights, rights to view or a combination within the health sector, the PoA can both be limited and specific. It can also be a general PoA when the assignor grants the assignee full representation rights. When viewing and updating data related to the incapacity for work certificate or viewing the patient's health data in the health portal the PoA used is either limited or specific.

For taxation matters, the PoAs used for the accountant's access rights for performing operations in the e-services environment are limited or specific PoAs. A general PoA is used for access rights for board members within the e-services environment. With regards to the business sector the general PoA is used for PoAs for performing actions in a bank or submitting statistical reports in the Statistics Office, when operations are performed by a company's authorized representative (such as a CEO or system main user). A specific or limited PoA are used when a board member authorizes someone to perform company-related operations in the self-service environment. The PoA for entering and submitting the annual report is general if it concerns a PoA valid for the CEO and limited or specific if it concerns a data submitter and/or data entry person or in case of another role.

Legal basis

Within the health sector, the collected data mentions several relevant regulations such as the General terms of the Central Authorization Management Information System Pääsuke, Regulation of the Central Authorization Management System's Database, Public Information Act.4, Health Information System Regulation, for guardianship-related topics. These are governed by the Family Law Act (Perekonnaseadus, PKS) and the Code of Civil Procedure (Tsiviilkohtumenetluse seadustik, TsMS), cross-border service data structure. The data sets agreed upon for the cross-border service are defined in the regulation "Piiriülese andmevahetusplatvormi vahendusel töödeldavate andmete koosseis, andmevahetuse korraldus ja logide säilitamise tähtaeg". Generally, PoA matters are regulated by the General Part of the Civil Code Act (Tsiviilseadustiku üldosa seadus, TsÜS).

For taxation matters, the collected data mention a combination of specified legal references, such as the TsÜS § 118, subsection 2. Taxation Act (Maksukorralduse seadus) § 26 and § 48, subsections 3 and 4. Taxpayers Register Regulations (Maksukohustuslaste registri põhimäärus) § 62, subsections 1, paragraph 2, and subsection 2. Advocacy Act (Advokatuuriseadus) § 41, subsection 1, paragraph 5, and subsection 2.

For the business sector, the collected data show legal obligations arising from the anti-money laundering and counter-terrorism financing law. There is a legitimate interest in verifying the accuracy of the customer-provided data and mitigating risks. Generally, the legal regulation to PoAs is regulated in the Law of Obligations Act/Civil Code Act (TsÜS), but specific PoAs can also be regulated by the National Statistics Act.

It seems that the legal basis Estonia is very regulated by the legislation. On one hand this gives clear guidelines, but on the other hand it also limits the flexibility within PoAs. In this report it is assumed that the law in Estonia is based on old contractual customs, however this cannot be determined on the data provided.

Liability

The data collected by the country experts show the assessment of liability in Estonia depending on the relevant mistake and whether returning to the pre-contractual situation (i.e., reversal) is possible. If returning to the pre-contractual situation is not easily possible, but the assignee has made a human error and exceeded the scope of the PoA, the exceeding of the PoA falls under civil liability. If the person has acted in bad faith and committed fraud, the action will be processed under criminal proceedings. The legal framework in Estonia uses the assessment "good faith" and "bad faith" to determine the concrete case.

If this issue goes to court, the court may compare how a "normal" person would have acted in the assignor's position. The assignor should also exercise due diligence in such cases: they should trust the person to whom they grant the PoA and have an overview of how the power is being used. Naturally it is difficult to limit all instructions to the scope of the PoA.

Barriers

For PoAs within the health sector the assignor is a representative of an Estonia registered company with a valid eID tool. The assignee is an individual with an Estonia personal identification code and a valid eID tool. The system automatically checks the person register and denies individuals who are underage or deceased.

For the taxation sector minors cannot perform actions themselves, they only have viewing rights. This also applies to persons of limited legal capacity, where rights have been revoked (can however be restored). If a legal entity goes bankrupt, the board member loses their rights and a ruling is sent to the EMTA, which restricts the board member's rights. Death or termination of access rights automatically ends the access rights.

Regarding the business sector, the assignor is a representative of an Estonia registered company with a valid eID tool. The assignee is an individual with an Estonia personal identification code and a valid eID tool. In order to verify their identity, the user needs a valid Estonian ID (such as mobile ID or Smart-ID). If a foreign board member is listed in the commercial register, they cannot assign a data entry person. As an example, if an accountant submits a report on behalf of a foreign board member, it is not possible for the board to sign it digitally.

2.2.2 Status of implementation of relevant EU initiatives

The table below summarises the implementation status for each regulative in the Estonian context. The content is unfolded in the section below.

Table 14. The implementation status for each regulative in Estonia

Legal	Have not started	Planning implementation	Pilot phase or partly implemented	Fully implemented
Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)		✓		
Once Only Technical System (OOTS)				✓
EU Single Digital Gateway Regulation (SDGR)		✓		
EU Digital Identity Wallet (EUDIW)			✓	
The European Health Data Space (EHDS)			**N/A**	
Upgrading Digital Company Law (UDCL)			**N/A**	

Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)

The score of eIDAS 2.0 for Estonia is fairly uncertain. There is no information regarding this in the data collection. However, according to the webpage of The Information System Authority (RIA), who manages the development of the digital wallet. The revised version of eIDAS is being implemented towards 2026. Therefore, it is assumed that Estonia must be at least in the planning implementation stage, because the full implementation is time consuming. The score is therefore set at 2, but this is an assumption and with a level of uncertainty.

Once Only Technical System (OOTS)

According to the data collected by the country experts, the OOTS is fully implemented in Estonia. However currently the PoA ecosystem does not benefit from this, as there is no central registry to view or pull PoA-related information into other databases. Most PoAs are still in physical form or sent as a PDF.

EU Single Digital Gateway Regulation (SDGR)

According to the RIA, who handles developing central technical solutions for the Estonian network; the current situation of the SDG is that the analytics and feedback of eesti.ee, to ease to communication towards the European Commission, has been improved. An Article Repository is being developed (simplifies meeting the requirements for new networks). SDG technical system solutions are currently being planned.

EU Digital Identity Wallet (EUDIW)

Estonia is participating in the pilot project POTENTIAL for the development of a technical solution for testing digital driver's license. Estonia is participating in the project together with, among others, Germany, France and Lithuania. The RIA manages the development of the Estonian digital wallet, and the solution should be completed no later than 21 November 2026.

The European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL)

Grades for the implementation of EHDS and UDCL are not included, cf. paragraph **Error! Reference source not found.** above.

2.3 Social inclusion

In the table below, the status of Estonia's efforts to ensure digital inclusion is visualized. The following text details the measures Estonia has put in place. The table indicates whether these measures are fully or partly implemented. Overall, Estonia has taken significant steps to implement most of the identified measures in the public sector.

Table 15. Estonia's efforts to ensure digital inclusion

Social	Have not started	Planning implementatio	Partly implemented	Fully implemented
Options for physical PoAs				✓
English language options available				✓
Information Systems for people with impairments				✓
Alternative access to digital ID		**N/A**		
Spokesperson/ representation of other people to obtain a PoA				✓
Education, support-service and facilitators to obtain a digital PoA		**N/A**		

2.3.1 Options for physical PoAs

Estonia allows for the use of both digital and physical processes in most situations. For instance, individuals without digital skills can submit in physical form. Additionally, a representative of a vulnerable group can seek help from a local government social worker to ensure they can take necessary actions. Furthermore, beyond digital processes, physical methods can be used, such as submitting a physical PoA to validate authorizations for actions in a non-digital setting.

2.3.2 English language options available

Public services in Estonia are provided through the platform www.eesti.ee. The platform can also facilitate collaboration between the public, private, and third (non-profit) sectors within the framework of providing public services[1]. The platform and its services are available in both Estonian, English and Russian.

2.3.3 Information Systems for people with impairments

The e-Tax/e-Customs system has been designed and developed to comply with the European Union digital accessibility standard EN 301 549 and WCAG 2.1. Consequently, public digital environments must offer opportunities for vulnerable target groups. This means that certain technical tools and content creation principles have been used to help users with visual, hearing, physical, speech, cognitive, language, learning, and neurological disabilities consume website content. For example, changing website colours, increasing content size, screen readers (audio), etc.

2.3.4 Alternative access to digital ID

No grade included above, as sufficient data was not available to the country expert.

2.3.5 Spokesperson/ representation of other people to obtain a PoA

In the context of a PoA, a representative for a vulnerable person can be appointed if a court order limits the individual's legal capacity. This information is available in the Business Register if the system is connected to it. For health-related matters, the process is more complex when the guardian is a local government entity, as legal entities lack ID codes, preventing data from moving between registers. A person with limited legal capacity, due to mental illness or intellectual disability, can only make limited transactions, with their guardian (appointed by the court) handling contracts. Local government social workers can also assist, especially if family members are unavailable, such as when children live abroad.

2.3.6 Education, support-service and facilitators to obtain a digital PoA

No grade included above, as sufficient data was not available to the country expert.

3. Finland

The as-is analysis of Finland's digital PoA landscape reveals a strong foundation across legal, digital, and social dimensions, highlighting a relatively advanced level of maturity that positions Finland as a model for best practices. While Finland's PoA solutions provide substantial support across public and private sectors, further progress is anticipated as the country refines and broadens its digital PoA framework, including strengthening its verification and authentication processes.

Finland has implemented a central platform supporting various PoA uses, with sector-specific solutions in areas such as healthcare, taxation, and business, creating a cohesive structure for the domestic administration of PoAs. In Finland sector specific PoAs are common in health, tax and business, and the Contracts Act seems to provide the legal framework for PoAs. The country is also aligning with key EU regulations and initiatives, such as eIDAS 2.0 and OOTS, while progressing towards full implementation of the EUDIW. Finland has made significant advancements in social inclusion across its digital PoA systems, with essential parameters either fully or partially integrated.

Despite Finland's robust digital infrastructure, challenges remain in addressing cross-border PoAs, particularly in simplifying access for foreign nationals and supporting Finnish non-residents with tax-related PoAs.

3.1 Digital and process

This section examines the maturity of technical standards and barriers across access, authentication, verification, and integration of digital PoAs in Finland.

3.1.1 Technical Standards and ID Infrastructure: Advantages and Disadvantages

The following describes the maturity for technical standards and barriers regarding access, authentication, verification, and integration, alongside cross-border interoperability to highlight advantages and disadvantages in Finland.

Table 16. Finland's maturity for technical standards and barriers

Digital	Basic	Intermediate	Advanced	Fully integrated
Access to handle PoAs				✓
Verification		✓		
Authentication		✓		
Integration			✓	
Cross-border interoperability			✓	

Access to handle PoAs

In Finland, all handling of digital PoAs across sectors are compiled into a single platform solution, *Suomi.fi-valtuudet* (from here, *Suomi.fi e-Authorizations*), which is developed by *Digi-ja Väestötietovirasto* (DVV), the Finnish Digital and Population Data Services Agency. The solution allows to verify a person's or organization's authorisation, to mandate the right to use digital services on behalf of another person or organisation. This provides a single interface for Finnish citizens and businesses, and the solution is generally considered to be strongly well-functioning by specialists and end-users. The *Suomi.fi e-Authorizations* solution is web-based and is thereby widely available if the device is connected to the internet. There are no competing solutions currently.

Within the platform solution, Finnish citizens and businesses (assignors and assignees), can create, request, and grant a PoA by setting the scope of PoA, time duration and assignee/assignor. The PoA is established in from a list of pre-set PoA themes (e.g. Conduct pharmacy business or View health information in OmaKanta.fi).

The solution is mandatory by law to use by all public sector organisations in Finland. In the healthcare district of Pirkanmaa, it is mandatory to use Suomi.fi for digital PoAs and authorizations. The location of all PoAs in one digital platform indicates a fully integrated level of maturity for access in PoA.

Verification

In Finland, there is not yet a central EU approved eID. Instead, citizens log into *Suomi.fi* using their bank credentials, *mobiilivarmenne* (Mobile ID certificate) or an ID-card issued by the police. Further, the digital identity is then verified through API integration with the Finnish Population Information system, where everyone has been assigned a personal identity number (Henkilötunnus).

When requesting or creating a PoA, the suomi.fi e-Authorization platform draws upon data from several national databases and registers to verify credentials. Examples of credentials in the registers include age, family relations (e.g. child & parent), date of death (to ensure the person is still alive), legal capacity, whether a company is registered into the trade register, status of company, and representation rights. Based on a rule engine of public portals (e.g. Maisa or MyTax), PoA requests are verified against the attestations of attributes in the Mandate Register. For instance, when acting on behalf of a company, the PoA (i.e. mandate to represent a company) is validated in real-time against the trade register. The third parties accepting digital PoAs may set their own rules for which attributes are checked using the suomi.fi rule engine.

Authentication

Authentication is based on strong identification through banking codes, Mobile ID (mobiilivarmenne) or the Citizen Certificate. These authentication methods can all be used to confirm the identity at login to *Suomi.fi e-Authorizations*.

Banking codes are identification tokens granted by different Finnish banks, and can be used for e-identification, both for citizens and companies.

Mobile ID is offered by some mobile operators and are used for authentication purposes. Strong authentication requires a mobile token, activated on the phone's SIM card, which is the user's eID. To get the mobile certificate, citizens must have a phone contract with an offering mobile operator, along with Finnish banking codes, and a SIM card that supports Mobile ID.

Citizen Certificate is an ID card that can be used to prove the identity of citizens when logging in to public e-services, such as Suomi.fi.

In case of citizens acting on behalf of a company (i.e. for taxation or business purposes), the natural persons log in using one of the above identification methods, whereafter their rights are checked in real-time against the trade register and the PoA database.

Authentication options in Finland are varied but lack the strong central eID of some other EU nations. It is confirmed that Finland is working on an eID and a pilot for the EUDiW, which will strengthen authentication and verification in the future. As a result, maturity is currently at an intermediate level.

Integration

The main platform, *Suomi.fi e-Authorizations*, provides an integrated solution across public sectors, but also integrates with third-party solutions. The solution operates behind various e-services managed by different public authorities, verifying that individuals have the necessary authorization or rights to represent another party within the service. For instance, to pick up medicine on behalf on someone else, assignees can provide its own and the assignor's personal identification number to pharmacies, which have a system to check authorization in real-time against the Suomi.fi database. For handling general healthcare matters, the PoA is verified from the PoA database upon log in.

For taxation matters, the PoA is automatically checked when doing business on the MyTax platform (the Finnish Tax Administration's e-service for taxpayers: "vero.fi"). This works for both businesses and citizens.

Suomi.fi e-Authorizations relies on several national systems which are used to verify users (e.g. based on existence, age), and to validate existing authorizations (e.g. family relation, position at company) to perform tasks. Databases include Population Information System, Guardianship Information System, Association Register, Trade Register, and Business Information System, which are all connected to a Mandate Register. The databases used depends on the specific scope of the PoA. In this way, the validity of PoAs can be checked in real-time, which enhances the security and reduces the risk of fraud.

The *Suomi.fi e-Authorizations* solution integrates with other public platforms to access and deliver data using APIs or the *Suomi.fi- palveluväylä* (Data Exchange Layer).

Cross-border interoperability

Currently, Finland's infrastructure poses as rather advanced to accommodate cross-border interoperability, however, there a several challenges to grant or receive PoAs to or from foreign individuals and businesses. To grant and receive Suomi.fi authorisations, foreign individuals must have a Finnish personal identity code and a Finnish identification method (i.e. banking codes, Mobile ID, or Citizen Certificate). This is because the solution is based on Finnish registers and databases, hence, the utilisation of local eIDs from other countries is not possible, as identities cannot be matched reliably, while differences in definitions of rights are not available (e.g., rights of a CEO). If the foreign individuals do not have a Finnish personal identity code or other way to identify themselves, they cannot either grant or receive PoAs, and thus they must e.g. handle tax matters by filing paper forms.

Foreign individuals can access Suomi.fi using the eIDAS portal allowing to log in via a national eID. However, the e-Authorization module of the platform cannot be

used in this regard, as the service is based on Finnish registers and databases. Foreign individuals can thus not grant PoAs unless it is related to business matters. Instead, foreign individuals must apply for a user identifier (UID), followed by an application to the Finish Authenticator service (app) provided by DVV. Foreign companies can grant a representative the right to act on behalf of the company if they either have a Finnish eID or a foreign unique identifier UID, as well as *Suomi.fi* authorisation (see verification). The company can then apply to grant a PoA for an individual representative to act on its behalf using this UID.

Foreign companies wanting to grant the right to act on behalf of the company without a Finnish personal ID must request a foreign UID, which entails downloading the Finnish Authenticator App, and uploading verification such as passport. Having established a UID, a request must be submitted for *Suomi.fi* authorisation separately. If a Finnish Business ID has been issued to the foreign company, this should be used to request the Suomi.fi authorisation.

However, it is already possible to transmit prescription information to some EU countries, including Estonia, while the transmission of patient data across EU borders is being worked on. It is unclear whether other countries also have non-disclosure systems for personal data, along with personal identity code practices that are similar to Finland. The use of *suomi.fi e-Authorizations* in a cross-border setting would require a way to identify the related persons and real-time access to databases in other countries (identity matching). In theory, this could currently be possible with Estonia, but this would still require manual check of identity by DVV-officials.

Currently, EU wallets (EUDIW) are being prepared. The purpose is to use this to identify yourself instead of using banking credentials. Finland has considered the attestations of attributions necessary to prove the appropriate transaction.

The OOTS has not been implemented as a finished product in Finland, but the basic principles are followed in the Soumi.fi platform. Foreign companies wanting to grant the right to act on behalf of the company without a Finnish personal ID must request a foreign UID, which entails downloading the Finnish Authenticator App, and uploading verification such as passport. Having established a UID, a request must be submitted for Suomi.fi authorisation separately. If a Finnish Business ID has been issued to the foreign company, this should be used to request the Suomi.fi authorisation.

Foreign individuals can access Suomi.fi using the eIDAS portal allowing to log in via a national eID. However, the e-Authorization module of the platform cannot be used in this regard, as the service is based on Finnish registers and databases. Foreign individuals can thus not grant PoAs unless it is related to business matters. Instead, foreign individuals must apply for a user identifier (UID), followed by an application to the Finish Authenticator service (app) provided by DVV. Foreign companies can grant a representative the right to act on behalf of the company if they either have a Finnish eID or a foreign unique identifier UID, as well as Suomi.fi

authorisation (see verification). The company can then apply to grant a PoA for an individual representative to act on its behalf using this UID.

Overall, Finland demonstrates a higher degree of infrastructure for cross border PoA solutions but similarly to other nations, is missing some of the final touches. The current integration with Estonia and other nations for healthcare matters demonstrates the advanced level of cross border readiness.

3.1.2 PoA Process

Access & verification

Citizens and businesses log into the Suomi.fi e-Authorizations platform solution to handle PoAs. Gaining access requires strong verification via Finnish banking codes, Mobile ID, or Citizen Certificate. All information is checked against national registers for both identity and rights to act on behalf of another party.

Create PoA

On the *Suomi.fi e-Authorizations* platform, citizens and businesses can request or grant PoAs. The PoA is established from a list of pre-set PoA themes. All PoAs are free of charge.

If a PoA is requested, the request can be accepted (or rejected) by logging into the portal.

All authorizations (PoAs) are stored in a cloud-based authorization register (Mandate register), hosted on AWS servers.

Use PoA

All PoAs can be viewed on the *Suomi.fi e-Authorizations* platform solution. To e.g. use the PoA to pick of medicine at the pharmacy, no device is needed, while it is only necessary to use the personal identity numbers of the assignee and the assignor. For e-services, such as MyTax, the assignee can login to the platform directly to be able to act on behalf of the assignor.

Third parties (e.g. pharmacies) can access the Mandate Register to ensure validity of PoAs in real-time.

Terminate PoA

The PoA is always in force for a set duration and can be terminated at any point through the *Suomi.fi e-Authorizations* platform enabled by the real-time based system. A suomi.fi warning message may be sent when the PoA term is coming to an end.

In the event of change or revocation, the PoA is updated in real-time into the register.

3.2 Legal Aspects

The following section will first present an overview of legal topics, followed by a review of EU initiatives.

In Finland, PoA types is often sector-specific, with limited or restricted versions being the most prevalent. In healthcare, PoAs are used mainly for pharmacy and health-related matters, while in the taxation field, they are utilized for tax declarations and real estate tax issues. In the business realm, PoAs facilitate salary processing, custom clearances, and applications for company funding. Although no explicit legal basis for PoAs is mentioned in the data, Finland's Contracts Act appears to provide a relevant legal framework. Liability issues are mitigated by the suomi.fi valtuudet service, which verifies PoAs in real-time but details on liability are unclear due to insufficient data. Lastly, barriers to granting PoAs include age and guardianship restrictions, as well as the need for representation rights in the trade register for legal person assignors in both taxation and business sectors. Finland is also aligning with key EU regulations and initiatives, such as eIDAS 2.0 and OOTS, while progressing towards full implementation of the EUDIW.

3.2.1 Legal Topics

This section covers the legal topics also included in the main report: semantics, types of PoAs, legal basis, liability, and legal barriers.

Semantics

Table 17. Role description of various sectors

	Health sector	Taxation sector	Business sector
Assignor	Physical person, based on the collected data assumptions include residents in need of assistance in managing their interactions with public authorities online.	Physical person, private entrepreneur or company	The assignor is a company
Assignee	Physical person	Physical person, private entrepreneur or company	The assignee can either be a natural or legal person

Types of PoA

The most commonly PoAs used are limited/restricted PoAs. Within the health sector are PoAs for pharmacy matters and to handle health and social care related matters. For taxation matters, the most commonly used PoA is for tax declaration and to handle real estate tax matters. Within the business sector, PoAs are mostly used for processing salary information, custom clearance and applying for company funding.

Legal basis

According to the data collected there are nothing stated regarding the legal basis for PoAs. However, as a result of desk research made by the core team, there is a Finnish Contracts Act (Act: 228/1929) which seems to be at least slightly similar to the Scandinavian Agreement Acts and includes sections regarding PoAs in chapter 2.

Liability

The suomi.fi valtuudet service naturally decreases the risk of misuse and fraud, as it real-time checks the validity of the PoA. For these PoAs the use cases are well defined by the third party (although not on the level of which medicine). Due to the inadequate data collected, additional information on liability is unfortunately not available.

Barriers

For PoAs within the health sector, the assignor must be over the age of 18 and not in a guardianship in order to grant a PoA to an assignee.

Within the taxation sector, the assignor must be over the age of 18 and not in a guardianship in order to grant a PoA to an assignee. Furthermore, in case of a natural person signing the PoA on behalf of a legal person they must have representation rights registered in the trade register called PRH (Finnish patent and registration office).

If a natural person is signing a PoA on behalf of a legal person within the business sector, the assignor must have representation rights registered in the trade register.

3.2.2 Status of implementation of relevant EU initiatives

The table below summarises the implementation status for each regulative in the Finnish context. The content is unfolded in the section below.

Table 18. The implementation status for each regulative in Finland

Legal	Have not started	Planning implementatio	Pilot phase or partly implemented	Fully implemented
Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)		✓		
Once Only Technical System (OOTS)		✓		
EU Single Digital Gateway (SDGR)			**N/A**	
EU Digital Identity Wallet (EUDIW)			✓	
The European Health Data Space (EHDS)			**N/A**	
Upgrading Digital Company Law (UDCL)			**N/A**	

Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)

According to the Finish Digital and population data services agency, a project implementing the revised version of eIDAS has been launched and the project term runs until 31 December 2026.

Once Only Technical System (OOTS)

Described in the European Commission's June 2024 version of the "Once-Only Technical System Acceleratormeter as "Production ready", more specifically as "Technically ready" entailing that Finland is finalizing the configuration. At the moment, the collected data shows OOTS not currently being in use as a product, however the main principles are used in the Suomi-fi-service.

EU Single Digital Gateway Regulation (SDGR)

No grade included above, as sufficient data was not available to the country expert.

EU Digital Identity Wallet (EUDIW)

According to the data collection, Finland is participating in three pilot projects, including POTENTIAL, EWC, and the DC4EU consortium. These projects were launched in April 2023 and cover use cases such as digital driving licenses, digital identities/wallets, and higher education diplomas and student data. Finland is currently in a pilot phase and therefore yet to fully implemented the EU Digital Identity Wallet, which is expected in 2026.

The European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL)

Grades for the implementation of EHDS and UDCL are not included, cf. paragraph 3.3.2 above.

3.3 Social inclusion

The table below illustrates the status of Finland's efforts to ensure digital inclusion, with the following text explaining the specific measures implemented. The table highlights which measures are fully or partially in place. Overall, Finland has implemented most of the identified measures.

In some areas, Finland exceeds basic requirements, offering features like multiple language options, services for web accessibility complaints, and a robust system for digital powers of attorney managed by trustees or spokespersons.

Table 19. The status of Finland's efforts to ensure digital inclusion

Social	Have not started	Planning implementatio	Partly implemented	Fully implemented
Options for physical PoAs				✓
English language options available				✓
Information Systems for people with impairments				✓
Alternative access to digital ID				✓
Spokesperson/ representation of other people to obtain a PoA				✓
Education, support-service and facilitators to obtain a digital PoA			✓	

3.3.1 Options for physical PoAs

In cases where a citizen does not have the necessary digital skills to generate a digital PoA, PoAs can be given and accepted physically at DVV-offices (Digital and Population Data Services Agency) and then in turn registered in the online database allowing for digital usage. If the vulnerable person is not able to visit DVV offices, they can use an assistant to help them. The assistant has to identify themself on the suomi.fi-platform and physically deliver the signed PoA to a DVV-office. The process takes place in the form of an application for PoAs and the accepted PoAs are registered in approx. one week.

3.3.2 English language options available

The official website for citizen matters, Suomi.fi, is available in both Finnish, English and Swedish, which is the official language in Åland. The several language options are to avoid discrimination of non-Finnish speakers.

3.3.3 Information Systems for people with impairments

EN 301 549 was effectively implemented in Finland by 23 September 2018, as part of the transposition of the EU Web Accessibility Directive into Finnish law.

The Regional State Administrative Agency for Southern Finland oversees the accessibility of digital services nationwide, covering public sector operators and parts of the private sector. Under new accessibility regulations, the agency will also monitor digital services offered to users.[3]

These requirements extend beyond EU standards, affecting both public and private providers offering services or products covered by accessibility laws. Finland's legislation introduces two key points: Websites must offer an accessible feedback channel, including details on how the feedback will be used. Providers must supply documentation for services lacking accessibility, explaining alternatives and providing contact information for further inquiries.[4]

3.3.4 Alternative access to digital ID

The instructions on the authorization application form indicate the other ways in which the assignor can prove his or her identity if he or she does not have a valid identity document. For example, a trustee or private guardian can make an application for a PoA and ask the person, who appointed him/her, to sign it. In addition to the signature, a copy of the assignor's identity document must be attached to the authorization application in palace of the digital ID.

3.3.5 Spokesperson/ representation of other people to obtain a PoA

If the assignor is no longer able to understand the matter, a trustee or private guardian can sign the application on their behalf. However, only matters that fall within the trustee's or guardian's legal authority can be included in the application.

A certified copy of the PoA from the Office for Digital and Population Information, or a copy of the guardianship order, must be attached when a trustee or guardian acts on the assignor's behalf.[5]

If the assignor is ineligible to establish a PoA, such as being underage, a PoA cannot

3. New accessibility requirements | Traficom
4. Web Accessibility in Europe: The Full Compliance Guide (2024)
5. https://www.suomi.fi/ohjeet-ja-tuki/valtuudet/henkilon-valtuudet/nain-valtuutat-jos-et-voi-kayttaa-sahkoisia-palveluja

be created. This can cause challenges in healthcare settings for minors and their parents, or for individuals with conditions like dementia who lack full decision-making capacity. In these cases, a trustee is appointed to manage their affairs.

3.3.6 Education, support-service and facilitators to obtain a digital PoA

The national association for seniors in Finland, Senioriliitto, organizes educational workshops in digital skills for elderly people. The organization is nationwide, but for members only, which means that some groups without membership and digital skills are not included for the trainings.

4. Iceland

The examination of Iceland's current digital PoA infrastructure shows a developing landscape with room to improve in integrating digital, legal, and cross-border aspects to enhance accessibility and efficiency.

Iceland has adopted a centralised digital platform approach, namely *Ísland.is*, serving public administration needs, including PoA management, which integrates sector specific PoA solutions for healthcare, taxation, and business. This integration facilitates the authentication and issuance of PoAs within these domains, leveraging Iceland's eID system which enjoys wide adoption amongst residents. Nevertheless, PoA data exchange across sectors remains absent.

Challenges persist particularly with cross-border compatibility and accessibility for foreign nationals. While the country works to align with EU regulations like *eIDAS 2.0*, progress towards full integration is ongoing, with key initiatives like the *OOTS* still under technical development. This reflects a broader trend towards enhancing digital PoA frameworks and striving for better data exchange systems consistent with European standards.

In terms of social inclusion, Iceland demonstrates a commitment to ensuring that digital PoA services are accessible to people with impairments and has implemented options for physical PoAs. Efforts are also being made to ensure that information systems accommodate non-Icelandic speakers and enable representation for individuals needing assistance in PoA transactions.

The legal landscape around PoAs in Iceland is sector-specific, with regulations such as the Children's Act facilitating guardians' access to minors' health data. The business sector operates under a mix of formal laws and customs, with clear implications for liability and adherence to Icelandic agency and contract laws.

As Iceland continues to enhance its digital PoA offerings, it faces the imperative to reconcile rapid digitalization with the need to prevent the exclusion of vulnerable citizens, ensuring that the transition to a more automated and electronic system leaves no one behind.

4.1. Digital and process

This section examines the maturity of technical standards and barriers across access, authentication, verification, and integration of digital PoAs in Iceland.

4.1.1 Technical Standards and ID Infrastructure: Advantages and Disadvantages

The following describes the maturity for technical standards and barriers regarding access, authentication, verification, and integration, alongside cross-border interoperability to highlight advantages and disadvantages in Iceland.

Table 20. Iceland's maturity for technical standards and barriers - No data on EU Digital identity Wallet.

Digital	Basic	Intermediate	Advanced	Fully integrated
Access to handle PoAs			✓	
Verification				✓
Authentication			✓	
Integration		✓		
Cross-border interoperability	✓			

Access to handle PoAs

In the **Healthcare sector**, patients (assignors) can log into the Health Portal, *Heilsuvera*, to assign PoAs. eIDs are the only means of authentication and identification of the security standard required for electronic identification into electronic healthcare in Iceland.

Companies' **Taxation matters** can be performed within *Skatturinn*, to gain access to PoAs for Tax returns, payroll tax obligations etc. The PoA will then be sent to legal domicile of the company by mail. It is furthermore possible to call the Service Center at Skatturinn and ask for it there. On the *skatturinn* website there are several templates for PoAs.

For **Business matters**, PoAs can be accessed through the platform solution *Ísland.is*, which integrates with a variety of services, such as tax filings, company registration services, and other government portals, allowing the assignee to access these

services on behalf of the company. The assignor and the assignee log in to the platform using their eID.

PoAs are not housed in a single, centralized database but are integrated into various sector-specific services, accessible through *Ísland.is*. The system supports secure authentication of PoA delegations for tasks such as tax filing, healthcare decisions, and legal matters. Therefore, the system supports digital access to handle PoAs to a strong degree.

Verification

Registers Iceland (*Þjóðskrá*) holds the National Registry and manages National Identification Number (*Kennitala*), which are crucial for verifying both natural and legal persons involved in PoAs. It ensures that legal rights, such as PoAs, can be validated securely. This number is used to link your identity to the electronic ID and verify your personal information against the national registry.

Electronic IDs are the only means of verification and identification of the security standard required for electronic identification into electronic healthcare, taxation, and business matters in Iceland. Verification of access to digital PoAs are therefore fully supported.

Furthermore, the following attributes are linked to the verification:

- National Identification Number (Kennitala) This number is used to link your identity to the electronic ID and verify your personal information against the national registry.
- Agreement with the Certified Provider *Auðkenni*, which is the main issuer of eIDs in Iceland. This involves registering your details and verifying your identity in person at a service centre, typically a bank or a mobile service provider's office.
- Biometric Identification (for some services). For initial registration or certain high-security actions, biometric identification (such as showing a passport or other official ID document in person) is required to establish your identity. This ensures that the eID is securely linked to the rightful individual.

Authentication

National ID Database are integrated with the eID system, this database authenticates identities via national eIDs, which are used to authorize PoAs digitally. This infrastructure ensures secure authentication and access to documents related to PoA agreements.[6]

The PoA platforms (*Heilsuvera, Skatturinn* and *Island.is)* leverages the secure authentication mechanisms provided by the national eID system (*Rafræn skilríki*) to

6. https://www.government.is/topics/information-technology/public-services/

a strong degree and involves two-factor authentication. It is widely adopted by the public and private sectors as well as approximately 97% of the eligible population (aged 13 or older). The eID system is built on secure cryptographic protocols, offering authentication and digital signature functionalities. Citizens use their eIDs via smartcards, SIM-based solutions, or mobile apps for secure access to various services. It is utilized for various services, including banking, government portals, healthcare, education, and digital signatures. Iceland's eID has not yet been notified by the EU under the eIDAS regulation.

Authentication for accessing, e.g., the *Heilsuvera* platform or initiating Digital PoA Transaction involves PIN codes, eIDs, and multi-factor authentication (MFA) for assignor and assignee. This PIN code is required every time you authenticate using the eID. It serves as a security measure to confirm your identity during login and digital signing processes.

Integration

Iceland has a centralized digital platform called *Ísland.is*, which serves as the primary gateway for public administration services. Managed by Digital Iceland, this platform brings together services from over 250 public agencies and municipalities, allowing individuals and businesses to interact with various government functions in one place. Citizens can access a wide range of services such as tax filings, health records, and more, all through their eID, making it a one-stop solution for many life events.

While there is no single, dedicated PoA platform, the *Ísland.is* portal allows individuals to manage and authenticate PoAs related to different sectors. This central platform offers access to PoAs in areas such as tax services, healthcare, and legal matters. By using the eID, users can authenticate their authority and access relevant PoAs linked to specific government services.

For now, the data collected do not suggest integrations enabling data exchange outside each sector. Nevertheless, Iceland is in the process of implementing the Once-Only Technical System (OOTS) as part of its broader digital transformation initiatives. The core of Iceland's implementation of *OOTS* is through *Straumurinn*, a national data exchange platform that builds on the X-Road interoperability framework. This system will allow secure and efficient data exchanges between public and private sectors and is a significant step toward fully realizing the once-only principle for digital services in Iceland.

Cross-border interoperability

For healthcare, the existing legal framework is outdated (dating back to the 1930s) and does not align well with modern data privacy regulations like GDPR. In the data collected, a need for synchronized European laws and the flexibility to grant different types of PoA for different matters was emphasized. The healthcare

system lacks funding to implement comprehensive digital solutions. The banking sector has reduced number of branches and moved services online, using significant resources to ensure customer accessibility and security. The healthcare sector, however, struggles to implement similar features due to financial limitations. The *Heilsuvera* platform is designed to comply with the EU's *eIDAS* regulation, which allows for the use of electronic identification from other European Economic Area (EEA) countries.

When using PoA in regard of taxation or business matters, in cross border transactions the most challenging task is to be able to map the roles and rights for both the assigner and the assignee, i.e. who is who and what is the assignee allowed to do.

For the platform solutions and PoAs to be available across country borders, two infrastructure elements are needed. First, Iceland's eID must comply with eIDAS, allowing EU citizens to authenticate using their national eIDs for cross-border transactions, including PoAs. This infrastructure will enable the verification of identities and authorizations across borders.

Second, PoA documents and related legal agreements must be accessible and verifiable across borders, requiring secure database integration with EU systems through cross-border databases. For instance, (1) BRIS (Business Registers Interconnection System): Relevant for legal entities across borders, ensuring that PoAs related to business activities are recognized, and (2) European Health Data Space (EHDS): For health-related PoAs, this sector-specific infrastructure will allow for cross-border access to medical records.

4.1.2 PoA Process

Access & verification

Healthcare: For medical Prescriptions, the assignor's identity is verified at the time of logging into *Heilsuvera* to ensure that the correct person is authorizing the delegation of rights. This process requires the assignor to log in using their eID (*rafræn skilríki*), ensuring their identity is verified. The assignee's identity is also verified when logging into the system to accept the PoA. The assignee is also required to show proof of identity, typically done through an ID card, driver's license, or any other legally accepted form of identification when picking up the medicine. Pharmacies also require proof of the PoA which is automatically updated in the *Heilsuvera* portal.

For guardians to have access to My pages on *Heilsuvera.is*, the assignee's access is verified against the national registry, which contains information on parent-child relationships. This ensures that the person claiming to be a guardian has a legal connection to the child. The assignee's identity is also verified when logging into the *Heilsuvera* portal.

For taxation and for business matters, the identity of the assignor and the assignee is verified when logging into the *skatturinn* web portal or *Ísland.is* using the eID. The eID is linked to national identification, which is validated through secure channels by Icelandic authorities, typically during the registration of the eID. This ensures that both the assignor and assignee are verified before the PoA is granted or accepted.

Create PoA

PoAs for medical Prescriptions are created and established through 'My pages' on the *Heilsuvera* portal. This authorization can specify if the assignee is empowered to pick up any medication on behalf of the prescription holder for an indefinite period or just a single medication for a limited amount of time. For taxation, a request for a PoA can be created on the web portal *skatturinn.is* and the PoA will then be sent to the legal domicile of the company by mail. Templates to PoAs can be found on the *skatturinn* website. For business matters, the PoA is established by the assignor (e.g., the legal representative of the company) through the *Ísland.is* platform.

The assignor within the health area can create and accept the PoA digitally through the *Heilsuvera* platform. The digital authorization is recorded in the system, making it accessible to pharmacies. The assignee also needs to log in with their eID to confirm their acceptance of the authorization. This ensures that the assignee is fully aware of their role and agrees to take on the responsibilities involved.

No information for accepting PoAs for taxation or business matters was collected.

Use PoA

When using the PoA, it can be found digitally by logging into either the *Heilsuvera* platform, a centralised system accessible to all pharmacies in Iceland, or Icelandic tax administration's web-portal etc.

Third party actions happen by checking whether the PoA is active in the e-prescription gateway for medical prescriptions. And verifying the identity of the assignee (1). When a guardian accesses *Heilsuvera*, they are logged into the portal using eID. The *Heilsuvera* system itself acts as the authority that validates the PoA based on verified data from the national registry (i.e., the link between the guardian and the child, and the child's age) (2). The same happens for taxation as the reliance on eID as a secure form of authentication not only confirms the assignee's identity but also ties the action directly to a specific authorization, preventing unauthorized access. For business matters, the usage of the authorization portal service provided by *Ísland.is* the holder of the PoA can give access to various parts of the service website in question.

Terminate PoA

Within health a system integration and real time verifications scans if the PoA still are valid. The PoA are terminated when the child turns 16, and for medical prescriptions either by specifying a time limit for the PoA when creating it, or by logging in and terminating the PoA on the Heilsuvera portal.

For business matters, the assignor can access the active PoA in the 'My Pages' section at *Ísland.is* and edit the PoA to change the scope, duration, or other details (e.g., assigning new rights or changing the assignee), and lastly, it is possible to Revoke/terminate the PoA entirely, ending the rights granted to the assignee.

4.2 Legal Aspects

The following section will first present an overview of legal topics, followed by a review of EU initiatives.

In Iceland, specific or limited PoA documents are commonly used across various sectors. The Children's Act (Act no. 76/2003) governs PoAs in health, allowing guardians to access minors' health data on Heilsuvera.is, with no other health sector PoA regulations identified. The business sector relies on a mix of formal laws and customs, requiring adherence to Icelandic agency and contract laws. Liability concerns hinge on the good or bad faith of the PoA actor, with digital services demanding providers accommodate PoA users, thus heightening liability risk. Each sector has unique barriers, such as minimum age requirements, legal capacity, and the necessity for an Icelandic electronic ID for transactions in business and taxation sectors.

4.2.1 Legal Topics

This section covers the legal topics also included in the main report: semantics, types of PoAs, legal basis, liability, and legal barriers.

Semantics

Table 21. Role description of various sectors

	Health sector	Taxation sector	Business sector
Assignor	The individual who holds a prescription or guardians for their child up to the age of 16	Person with legal authority over the company, such as owners, partners or board members	The holder of the power of procurement (usually the CEO of the company)
Assignee	The individual who is authorized to act on behalf of the assignor or the individuals with official parental responsibility/guardianship	A (authorized) representative, often an accountant, payroll administrator or tax agent/advisor	Could be an employee, a legal representative, or any other designated individual who is given the authority to access the company's digital services

Types of PoA

In general, the most frequently used PoAs for Iceland, cf. across all the three sectors, specific/limited PoAs are the most frequently used.

Legal basis

The Act no. 76/2003, Children's Act (Barnalög) outlines the rights and duties of parents regarding their children's upbringing and welfare. This act regulates the PoAs where guardians have access to "My pages" on Heilsuvera.is which is a site where you can access health data. According to the data collected, there are no other acts regulating PoAs within the health sector.

Due to lack of data, there are no laws mentioned within the taxation sector.

Regarding the business sector, the legal basis for PoAs is a combination of formal laws and established customs. The PoA must comply with Icelandic laws governing agency relationships, while also adhering to the basic principles of contract law (such as clarity, consent, and specificity).

Liability

When considering liability in Iceland good/bad faith matters when someone acts on a PoA. This also applies when the PoA and the solutions used to act are digital.

A difference between the PoA for digital services and a general PoA is that the service provider is required to adapt their solutions to enable someone who has a PoA to use them, which increase the risk of mistakes leading to liability disputes.

Barriers

Within the health sector, there are limitations with regards to age, where the assignee has to be at least 16 years old, to have access to the Heilsuvera.is platform. Additionally, within the health sector, the only limitation to the general PoA, is that parents cannot make decisions about organ donation on behalf of their children.

For the taxation sector the limitations include age and employment status, but the country expert was not able to collect data specifying the further extent thereof.

Regarding the business sector the age of both the assignor and assignee must be at least 18 years of age. Further, both parties must have the mental capacity to understand the legal implications of the PoA. Further, the assignor must be recognized as a legal representative in Iceland and the assignee must have an Icelandic electronic ID. Additionally, the assignor must be an authorized representative of the company, while the assignee does not need to be an employee but must be capable of fulfilling the role. Lastly, both the assignor and the assignee must use and Icelandic Electronic ID.

4.2.2 Status of implementation of relevant EU initiatives

The table below summarises the implementation status for each regulative in the Icelandic context. The content is unfolded in the section below.

Table 22. The implementation status for each regulative in Iceland

Legal	Have not started	Planning implementatio	Pilot phase or partly implemented	Fully implemented
Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)		✓		
Once Only Technical System (OOTS)		✓		
EU Single Digital Gateway Regulation (SDGR)			**N/A**	
EU Digital Identity Wallet (EUDIW)		✓		
The European Health Data Space (EHDS)			**N/A**	
Upgrading Digital Company Law (UDCL)			**N/A**	

Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)

According to the data collected, Iceland has a national eID, Rafræn Skilríki. The revised version of eIDAS is being implemented towards 2026. As Iceland must implement the eIDAS 2.0, it is likely that some planning has begun, thus stage 2 has been assumed above.

Once Only Technical System (OOTS)

In the data collected it is stated that Iceland is currently in the process of implementing the OOTS as part of its broader digital transformation initiatives. The core of the implementation of OOTS is through Straumirinn, a national data exchange platform that builds on the X-Road interoperability framework.

EU Single Digital Gateway Regulation (SDGR)

No grade included above, as sufficient data was not available to the country expert.

EU Digital Identity Wallet (EUDIW)

There is no information on this matter in the analytical framework. However, desk research on www.island.is shows Iceland participating in a multi-country consortium, with some of Europe's most trusted identity experts, where the aim is to deliver a cross-border payment pilot strongly aligned with the aims of EUDIW. Therefore, a stage 2 is most likely.

The European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL)

Grades for the implementation of EHDS and UDCL are not included, cf. paragraph 3.3.2 above.

4.3 Social inclusion

In the table below, the status of Iceland's efforts to ensure digital inclusion is shown. The table highlights which measures that are fully or partially implemented. The following text explains which measures that have been implemented so far and how they are implemented. Overall, Iceland has fully implemented some of the identified measures. In some areas, Iceland is in the development stages, while they in other areas exceeds basic requirements, offering, especially, disabled people a rather handhold assistance tailored the specific needs through the Disability Rights Protection Office.

However, some concerns have been addressed during interviews with key stakeholders pointing that the digitalization is moving too quickly with the risk of leaving vulnerable citizens behind.

Table 23. Iceland's efforts to ensure digital inclusion

Social	Have not started	Planning implementation	Partly implemented	Fully implemented
Options for physical PoAs				✓
English language options available				✓
Information Systems for people with impairments				✓
Alternative access to digital ID		✓		
Spokesperson/ representation of other people to obtain a PoA				✓
Education, support-service and facilitators to obtain a digital PoA				✓

4.3.1 Options for physical PoAs

Individuals without an eID, can deliver a physical PoA document in order to give another individual access to e.g. their digital inbox[1].

4.3.2 English language options available

The national Icelandic citizen website, Ísland.is, is available in English. Also, the website explaining how to grant a PoA in the name of a person or a company is described in English to support the inclusion of non-Icelandic speaking people.

4.3.3 Information Systems for people with impairments

EN 301 549 has been implemented in Iceland, even though Iceland is not a member of the EU. This is because Iceland is part of the European Economic Area (EEA), which includes EU member states and three EFTA (European Free Trade

Association) countries: Iceland, Norway, and Liechtenstein. The EU Web Accessibility Directive (Directive (EU) 2016/2102), which references EN 301 549, has been incorporated into EEA legislation. As a result, Iceland is obligated to implement the same accessibility requirements for public sector websites and mobile applications as EU member states.

4.3.4 Alternative access to digital ID

In Iceland, efforts to ensure inclusion for vulnerable assignors in the PoA process are still in developmental stages. Some of the measures that have been discussed to be implemented are alternative access to digital ID.

There has been ongoing dialogue about enabling municipalities to provide electronic IDs, as e.g. social workers are familiar with their clients' situations. This could help streamline access to necessary digital services for vulnerable individuals.

Also, there are considerations for alternative methods of authentication beyond traditional PINs, such as using fingerprints, facial recognition, or even emojis. However, details on the implementation of these alternatives are still unclear.

4.3.5 Spokesperson/ representation of other people to obtain a PoA

Individuals with disabilities can appoint personal spokespersons, persónulegir talsmenn, allowing them to make decisions independently. However, the access to decision-making is somewhat restricted due to the potential risk of fraud, e.g. by having access to bank accounts. To represent a vulnerable assignor, a spokesperson must be officially authorized by the Rights Protection Office, regardless of the assignor's personal preferences, such as appointing a family member. This ensures that the representative is deemed suitable to act in the best interest of the assignor.

The Disability Rights Protection Office can also assist digital vulnerable people to make an agreement with someone they trust to become their personal spokesperson if they need support to exercise their legal capacity and to be recognized as persons before the law.

The office provides documentation confirming the role as representatives of the vulnerable person. However, there are challenges with financial institutions, such as banks, which may not recognize these documents.

4.3.6 Education, support-service and facilitators to obtain a digital PoA

This overview presents Icelandic initiatives dedicated to improving digital competencies through education, training, and support services, including digital PoA facilitation.

Fjölmennt offers specialized digital training for individuals with intellectual disabilities, while Tölvumidstöd (TMF) provides IT counseling and courses. Public libraries also support digital literacy through free workshops. Fræðslumiðstöð atvinnulífsins enhances employability through digital upskilling, while the Digital Competence Cluster collaborates with institutions to promote digital skills nationwide. Private initiatives like TV and Akademias offer ICT training for both individuals and companies, contributing to Iceland's growing digital literacy.

5. Latvia

The key impressions from the analysis of the digital infrastructure for Powers of Attorney (PoA) in Latvia underline a nationwide solution that handles technical standards, verification processes, and cross-sector integration, including health, tax, and business sectors, with ongoing development towards full integration and cross-border functionality.

In the healthcare sector, the use of PoA requires access to the *e-veseliba* platform, while for tax matters access to the relevant tax platforms is necessary. Digital identification via EU-notified national eIDs support access and legitimates users across these platforms in Latvia. In the business sector, PoAs are managed through the company register platform, which allows for powers to give access and manage company profiles and transactions.

Across borders, Latvia faces challenges in validating PoAs due to a lack of coherence in the practices of different sectors and identification systems, complicating the potential for international interoperability. Meanwhile, there are ongoing initiatives, such as *eIDAS*, which is yet to be technically implemented, and the pilot project involved in *EUDIW*, indicating a shift towards the consolidation of digital PoA structures and improved data exchange in line with European norms.

The legal basis for PoAs in Latvia is spread across the sectors and influenced by specific legislation governing patient rights, tax, and business, as well as notary and civil laws. These regulations determine the extent of liabilities and ensure conformity with Latvia's legal principles related to agency and contractual agreements.

Socially, Latvia is actively working to make digital PoA services accessible to individuals with disabilities and has introduced mechanisms for manual PoAs. This is complemented by bilingual support features on digital platforms, aiding users who may not speak Latvian, and ensuring representation for those requiring assistance with PoA engagements.

As Latvia improves its digital PoA landscape, it becomes necessary to balance technological progress with social equity, ensuring the digital transition includes proper support for all citizens in order to promote an inclusive, electronically supported legal environment.

5.1 Digital and process

This section examines the maturity of technical standards and barriers across access, authentication, verification, and integration of digital PoAs in Latvia.

5.1.1 Technical Standards and ID Infrastructure: Advantages and Disadvantages

The following describes the maturity for technical standards and barriers regarding access, authentication, verification, and integration, alongside cross-border interoperability to highlight advantages and disadvantages in Latvia.

Table 24. Latvia's maturity for technical standards and barriers

Digital	Basic	Intermediate	Advanced	Fully integrated
Access to handle PoAs		✓		
Verification			✓	
Authentication			✓	
Integration		✓		
Cross-border interoperability	✓			

Access to handle PoAs

In Latvia, each sector has separate platform solutions for handling PoAs.

To grant or request PoAs in the **healthcare sector**, such as for picking up prescribed medicine or to make treatment-related decisions for patients, citizens must access the *e-veseliba* (e-veseliba.gov.lv) platform solution and log in through one of various ID methods. Here, the patients can set the PoA scope and determine the time duration of the PoA.

For **taxation** matters, citizens and companies must access the platform solution, *EDS* (Electronic Declaration System) and log in using one of various ID solutions. Additionally, a citizen can use the platform solution, *DigiNotārs*, using the same ID

infrastructure, as well as other ID-solutions, to log in through the national platform *latvija.lv*. This platform also provides a service to check the validity of the PoA and verify whether it has been revoked. In all cases, taxation PoAs can be handled in the platform solutions, but the creation itself involves uploading a self-created, digitally signed PoA, in some cases involving a notary, which is then validated manually by the authorities. This makes the access to handle PoAs less standardized both across and within each sector and thereby the maturity less advanced.

Moreover, the infrastructure solutions for accessing tax related PoAs implies an administrative burden on the *SRS*. Since there are no predefined scope of PoAs, the content differs widely and there is no automation. Further, the necessary notarization for the citizens PoA is not handled within the *EDS* platform. However, the lack of structure in scope allows for specific and complex PoAs, while users do not have to search to find the adequate PoA.

For **business** matters, the most activities related to PoAs are carried out through the platform solution of the Enterprise Register (registrs.ur.gov.lv). For companies to grant a PoA to an individual person to access and handle a company's profile, an existing representative of the company (e.g., a board member) can delegate full or restricted access and set the duration. Then, the assignee can login to perform tasks within the scope of the PoA.

In other PoA cases, companies can either grant a procuration or commercial PoA for individual persons to conclude transactions or perform commercial activities on behalf of the company. For procuration, the PoA must be applied for through the publicly available commercial register with a wide scope of authorization. For third parties, the scope is determined by law. The application for a procuration PoA must be submitted by the board or a person authorized by the board on the Enterprise Register platform or by post (notarized approval is required for the latter).

If the company wants to grant a PoA to perform specific legal activities, this must be specified in a commercial PoA, which is not recorded in the Commercial Register. This must be done on a digitally signed paper (which requires notarization for some services). The commercial PoA will thus not be carried out in the Enterprise Register solution.

Generally, the different gateways and processes around gaining access to handle PoA solutions varies from basic (e.g. digitally signed PoAs through notarization and send by post) and intermediate levels of maturity (e.g. *e-veseliba* and *EDS* allows for PoA overview and basic handling for health and taxation matters separately). Due to the existing infrastructure with dedicated platform solutions the level of maturity can be considered intermediate.

Verification

In Latvia, the national infrastructure for ID is built around the *eID card*, which works as a personal identification document used to sign documents through the built in eParaksts (eSignature) function. The eParaksts card is a smart card that contains eParaksts certificates for both signing documents and identity proof (eID) in a digital environment. Moreover, some platforms accept ID methods such as eParaksts Mobile, while others also accept SMART-ID and internet bank methods. The eParaksts, eParaksts Mobile, and eID card are all EU-notified and thus valid across the EU, which showcases an advanced verification infrastructure. However, as of 1 November 2022, the eParaksts card is not issued, but instead eParaksts mobile or *eID card* is suggested to be used. Lastly, other than the mentioned ID-cards, *EDS* accepts signing in using *Latvija.lv* (the unified authentication solution of the State Digital Development Agency) or *EDS* local username and password.

The mandatory attributes for the eID card include family name, name or names, personal code, citizenship or legal status in the Republic of Latvia, gender, date of birth, as well as the height of the person in centimetres.

Authentication

Authentication methods includes eID card, eParaksts, eParaksts mobile, and SMART-ID. When submitting a PoA, additional authentication is not necessary. Since the national personal code is used as credentials to authenticate the identity of an individual person, it does not work across borders.

For health care, citizens can authenticate through the "delegations" attribute (WS protocol, WS-security). Rights are delegated through SAML token as XML. All system activity is protected in the same way by a token that is attached to each of the platform's messages and is controlled at several levels.

For authorizing into the service portal of the *Enterprise Register*, authorization standards apply to *Latvija.lv* (WS-Federation or OAuth 2.0) or *eParaksts* (OAuth 2.0 user authorization and authentication standard).

Generally, Latvia has various authentication methods in play, providing a rather complex setup. However, strong authorization standards have been reported, and with an EU-notified eID, used for authentication, the maturity level can be considered advanced.

Integration

Generally, all PoAs are bundled by sectors, and mostly the assignor or assignee is responsible for the PoA and for informing the relevant institutions about the agreement. No third-party can thereby access a PoA unless it is shared by one of the actors. Further, there are currently several challenges to integrate and link data

with other institutions, as each sector uses its own platforms, systems, and databases.

For business PoAs, the Enterprise Register is integrated with other platforms through an API to ensure the availability of data, but it is usually not related directly to procurations. There is, however, a project (DAGR) to create a unified platform at the state level, where it is expected that state institutions will connect their information systems and then each institution will receive the information they need through this platform. Moreover, integrations with the Enterprise Register checks the right of representation in the company.

Some integration aspects of the digital PoA landscape in Latvia can thus be characterized as basic, given the manual processes and lack of data exchange between systems or third parties, while no advanced integrations have been detected. Due to the integrated ID infrastructure and important integrations, e.g. with the Enterprise Register, integrations reach an intermediate level of maturity.

Cross-border interoperability

In Latvia, the PoA practices differ widely throughout the sectors at the national level. Some interviewees state that for the country to facilitate or partake in cross-border PoAs, these practices must be streamlined. For instance, there are several challenges identified in linking the information across different state institutions, which is perceived to further increase complexity for cross-border PoAs.

For one, the *e-veseliba* platform is only available for individual persons with a national personal code. Hence, no cross-border PoA practices can performed within the healthcare sector. Moreover, the *EDS* platform only accepts Latvian authentication methods. Currently, non-Latvian citizens can create an account by generating password and username by applying to the SRS. Yet, this option will be phased out due to security concerns, while foreign authentication methods are not supported by the platform. Moreover, without a Latvian personal code, the *EDS* solution cannot link the individual persons with other data sources. For example, different public authorities, banks, etc. utilize differentiated identification methods, such as banks specifying information about birth data, name, and surname, which cannot be integrated with *EDS*.

For procuration registered in the *Enterprise Register* solution, the procurator can be a foreign person. However, since there are difficulties in registering with the existing methods for foreigners, the e-signed format must be recognized in Latvia. In such cases, paper format is used.

Generally, Latvian specialists are not confident about how to technically implement cross-border PoAs, since ongoing initiatives, e.g. eIDAS, face various challenges. These are related to identity matching and to regular updates and configuration systems across EU-countries. Moreover, each sector-specific platform can assign

the same non-Latvian individual with differing identification codes. For instance, for a company, a personal code assigned in the Enterprise Register starts with 38, while it starts with 32 for an individual person when assigned in the Office of Citizenship and Migration Affairs. Consequently, the same person could have two separate personal codes which cannot be linked within the databases. Further, some are sceptical about the possibility of creating an integrated system among different countries with respect to where the data is stored on Latvia's side. According to these interviewees, this is likely to only be relevant for a small group individual people working in Latvia. Thus, it is by some perceived to be easier and more economically feasible to handle this individually by country rather than creating a new system.

While the Latvian eIDs incl. *eParaksts* are valid in EU countries, there are situations in practice where other countries cannot verify an e-signed document. Moreover, there are still situations where representatives from Latvia are not able to open e-signed documents from Scandinavian countries. Through *Diginotārs*, PoAs are valid in all EU countries where *eParaksts* can be read. Ultimately, these e-signed solutions can be characterized as basic or intermediate, which increases complexity digitally enabling integrated, cross-border solutions for PoAs.

The implementation of OOTS has been initiated, however, there is no information on how PoAs can benefit from this. The main challenge regarding this solution is that different countries store different types of data, e.g. the information in birth certificate may differ between the countries which hinders linking the data.

Furthermore, the current pilot project for EUDIW with Denmark, Germany, Iceland, Italy, and Norway has raised challenges related to difficulties in mapping the information on how and which institution will process the data, and which attributes will be stored.

5.1.2 PoA Process

Access & verification

Citizens and businesses can access the separate platforms (*e-veseliba*, *EDS*, and *Enterprise Register*) by logging in using one of various eID methods.

The identity is in most cases verified and authenticated when logging in with an eID method. For digitally signed PoA documents, the validity of the signature can be validated by the institution's notary online at *eParakst*.

Create PoA

Generally, the creating of PoAs varies across the sectors. For health, the assignor either informs the medical institution about an authorization or makes a corresponding entry of the authorization in the *e-veseliba*, which makes it available for health care workers. No specific authorization is necessary when submitting the

PoA on the platform. To grant a PoA for picking up medicine, the assignor (patient) can set the scope of the PoA and determine the duration.

For tax matters, PoAs can neither be created, nor handled, but only submitted via the "Communication" section in EDS, which passes the information to State Revenue Service (SRS). For citizens, the PoA to view taxation data, the PoA is created through a notary, which is digitally signed. These can contain various aspects as there is no structured format, which means every case is individual. For companies, the general practice is to attach a digitally signed PoA via the "Communication" section in *EDS*.

Business PoAs are mostly created by an authorized person, delegating access via the Enterprise Register platform. Procuration PoAs require application through the commercial register, submitted by an authorized person on the Enterprise Register platform or by post (post requires notarization). Commercial PoAs are outlined specifying the scope and signed digitally on paper (which requires notarization).

In cases involving notarization, there will be a cost for the notary (e.g. £20–120).

Generally, it is the responsibility of the assignor to pass the digitally signed document to the assignee. For taxation, both can view active PoAs in *EDS*. For healthcare, the assignor can see a list of people who have viewed the information in *e-veseliba*, but the assignee is not required any additional actions. For some business matters, the assignee is notified by e-mail that a PoA has been granted, but the person is not required any actions. Assignee never has to accept PoAs.

Use PoA

When picking up medicine on behalf of someone else, the first and last name of the assignor must be given, and the identity document must be presented by the assignee. When purchasing medicine for the minor child, it is necessary to also state the child's name and surname. Representatives of medical institutions and pharmacy branches have accesses to the health information system to check the validity and verify the identity through *e-veseliba* which is connected to the pharmacy checkout system.

For taxes, the assignee can add the PoA in *EDS* (when notarized). The SRS receives the PoA within the *EDS* and evaluates its validity; however, no additional interactions happen if everything is correct. If there are any ambiguity in the PoA, the SRS communicates in writing within the *EDS* or by phone.

For business, in cases where third parties interact, it is either checked in the Enterprise Register (e.g. if the person is a procurator), or a digital signature is validated in *eParaksts*.

Terminate PoA

For most PoAs, the assignor can set the duration of validity (fixed or indefinite) and can revoke it at any time. In some cases, the assigned delegation can be edited on the portal, where it is also possible to edit the deadline for the delegation. For case-by-case business PoAs, the PoA usually ends with mutual agreement, completion of the given task, or expiration of the PoA.

5.2 Legal Aspects

The following section will first present an overview of legal topics, followed by a review of EU initiatives.

In Latvia, PoAs varies from sector to sector. The main within the health sector being picking up medicine or decision and viewing power. For taxation PoAs are primarily used for viewing power (to look in taxation data) and for business the uses of PoAs relate to the viewing-, execution- and decision power, such as applying for a permit or establishing a subsidiary. The legal basis for the health sector is regulated by the Law of the Rights of Patients. Taxation and business are both regulated by the Notarial- and Civil Law, and taxation is supplemented by basic contract customs, while business is supplemented by the commercial law. Regarding liability the assignor is fully liable for PoAs, however the specific details are unclear due to insufficient data. Barriers to granting PoAs include age restrictions within the sectors, however additional barriers such as mental health is unclear due to insufficient data. Lastly, the implementation of the different EU initiatives in Latvia is doing well with the EUDIW, but still in the planning phase with some of the other initiatives.

5.2.1 Legal Topics

This section covers the legal topics also included in the main report: semantics, types of PoAs, legal basis, liability, and legal barriers.

Semantics

Table 25. Role description for various sectors

	Health sector	Taxation sector	Business sector
Assignor	The patient that makes an entry in the eveseliba.gov.lv	Natural person – PoA must be notarized	The merchant or the merchant's legal representative
Assignee	The natural person who has been assigned by the patient	It is determined by the assignor, but usually an authorized representative such as an accountant	It is determined by the assignor, but usually authorized representative

Types of PoA

Within the health sector, the PoA used for decision and viewing power (treatment-related decisions for the patient and receiving medical information) is the general PoA. When picking up medicine, the PoA used is specific or limited.

In the taxation sector in Latvia, there are general and specific or limited PoAs which is used for viewing power (access to look in taxation data) for natural persons.

For PoAs in the business sector, specific or limited PoAs are used for viewing power (checking a company's data in a register), execution power (applying for a permit) or decision power (e.g. establishing a subsidiary).

Legal basis

The legal basis for PoAs within the health sector is regulated by the Law on the Rights of Patients.

Taxation is regulated by the law (Notarial Law and Civil Law) establishing the rules of types of PoA and how a notary verifies persons. Additionally basic contracts customs are used when requiring, e.g. sufficient clarity and consent in agreements.

Within the business sector, the commercial law sets the general principles on the procuration, while Notarial Law and Civil Law establishes the rules of the types of

PoAs and how a notary verifies persons. Furthermore, the overall functions of the Enterprise Register – Law on the Enterprise Register of the Republic of Latvia.

Liability

Within all of the three sectors, the assignor is fully responsible for PoA, including informing about the PoA assignee, as well as third parties. When a PoA is notarized additional vulnerability aspects are taken into consideration. If the assignee exceeds the limits of the PoA, the assignor can commence legal action in accordance with the Civil Law.

Barriers

The Civil Law states that a person under the age of 18 lack the capacity to act. However, at age 14 the person can start to act legally, e.g. to receive eParaksts, to pick up their prescribed medication. For other health PoAs, the assignee and assignor must have to capacity to act – at least age 18. In the business and taxation sectors there are barriers regarding employment, the person can be employed from age 15 (before that the person needs permission from one of the parents). A person under age 18 cannot start a business, and there may be some exceptions, with the earliest being age 16.

For business matters, according to the Commercial Law, board members and the auditor of the company, and board members of the dominant undertaking in a group of companies may not be board members (or procurators).

Regarding mental health, it is limited if the person lacks the capacity to act. However, it can be possible for someone with limited capacity to pick up medication with a delegation, this is if the assignor has delegated this person (with limited capacity).

5.2.2 Status of implementation of relevant EU initiatives

The table below summarises the implementation status for each regulative in the Latvian context. The content is unfolded in the section below.

Table 26. The implementation status of each regulative in Latvia

Legal	Have not started	Planning implementatio	Pilot phase or partly implemented	Fully implemented
Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)		✓		
Once Only Technical System (OOTS)		✓		
EU Single Digital Gateway Regulation (SDGR)			**N/A**	
EU Digital Identity Wallet (EUDIW)			✓	
The European Health Data Space (EHDS)			**N/A**	
Upgrading Digital Company Law (UDCL)			**N/A**	

Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)

The score of eIDAS 2.0 for Latvia is fairly uncertain. There is no information regarding this in the data collection. The revised version of eIDAS is being implemented towards 2026. It is therefore assumed that Latvia must be at least in the planning implementation stage because the full implementation is time consuming. The score is therefore set at 2, but this is an assumption and with a level of uncertainty.

Once Only Technical System (OOTS)

The implementation of OOTS has already started, and the testing will soon be launched, there is no information on how PoA benefits from this. Described in the European Commission's June 2024 version of the "Once-Only Technical System Acceleratormeter as "Production ready", more specifically that "The services are rolled out and ready to be used by citizens and/or businesses. The main challenge regarding this solution is that different countries store different type of data.

EU Single Digital Gateway Regulation (SDGR)

No grade included above, as sufficient data was not available to the country expert.

EU Digital Identity Wallet (EUDIW)

Latvia is participating in the NOBID consortium, a project where to aim is to deliver a large-scale pilot project of the EU Digital Identity Wallet together with Denmark, Iceland, Norway and others. The focus of the project is especially on the cross-border payment use case. EUDIW are currently facing challenges related to difficulties in mapping the information on how and which institution will process the data, which attributes will be stored etc.

The European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL)

Grades for the implementation of EHDS and UDCL are not included, cf. paragraph 3.3.2 above.

5.3 Social Inclusion

Latvia offers mixed options for PoA management across various sectors. In the health and tax realms, individuals can complete PoA processes via paper forms, while digital-only PoA submissions are increasingly standard in the business sector due to the Enterprise Registry's transition to online services. Regarding language accessibility, e-health services are available solely in Latvian on E-veselība.lv, whereas public services on Latvija.lv offer both Latvian and English, covering PoA services.

In compliance with EU accessibility standards EN 301 549 and WCAG 2.1, Latvia strives to make digital services including PoAs accessible to individuals with disabilities. While the e-veseliba portal requires a secure digital ID for complete access, support is provided for citizens through phone or email to navigate the system and manage PoAs.

The responsibility of holding and distributing a PoA lies solely with the creator, keeping with strict confidentiality norms that prevent notaries from sharing such sensitive documents. To support this system, the National Health Service, via Unified customer service centers and latvija.lv's helpdesk, aids those with limited digital skills. Although no specific PoA educational resources are available, general system guidance is provided by various sectors and detailed PoA information can be found through the Council of Sworn Notaries of Latvia and their notary events.

Table 27. Status of efforts in ensuring digital inclusion

Social	Have not started	Planning implementation	Partly implemented	Fully implemented
Options for physical PoAs			✓	
English language options available			✓	
Information Systems for people with impairments				✓
Alternative access to digital ID				✓
Spokesperson/ representation of other people to obtain a PoA	✓			
Education, support-service and facilitators to obtain a digital PoA			✓	

5.3.1 Options for physical PoAs

In the health and taxation sectors, options for establishing a physical PoA are available, allowing individuals to fill out and submit paper forms as required. Contrarily, within the business sector, as the Enterprise Registry shifts fully to digital operations, all actions must be undertaken via digital means, leaving no room for physical PoA processes.

5.3.2 English language options available

The website, E-veselība.lv, administrates national e-health services for medical treatment institutions and pharmacies is only available in Latvian. Whereas the platform Latvija.lv, administrating public services electronically is available in both Latvian and English, which also includes PoA services.

5.3.3 Information Systems for people with impairments

As an EU member state, the EN 301 549 and WCAG 2.1 regulations are implemented for public websites. These standards are part of Latvia's commitment to accessibility under the European Union directives, and they set guidelines for making websites, mobile applications, and ICT products accessible to people with disabilities. Both standards are essential for public sector organizations and increasingly apply to private sector services as well.

5.3.4 Alternative access to digital ID

To access the e-veseliba system, users must authenticate using a qualified electronic identification tool, as this is required to perform tasks such as managing PoAs. Without proper authorization, only the public section of e-veseliba is accessible, where PoA functions are not available. Citizens can contact the support service by phone or email for assistance with using the e-veseliba system, including completing procedures related to PoA. Support staff will guide users through the necessary steps to ensure proper access and completion of tasks within the system.

5.3.5 Spokesperson/ representation of other people to obtain a PoA

The creator of a PoA bears full accountability for its management, which involves relaying it to other individuals or entities as needed. Notaries are bound by confidentiality and are not permitted to disseminate this document or its details to any third parties. Thus, the dissemination of a PoA to others can only occur through direct provision from its originator, ensuring that the PoA is obtained exclusively from the person who formulated it.

5.3.6 Education, support-service and facilitators to obtain a digital PoA

The National Health Service has enhanced support for citizens with limited digital skills, especially regarding the use of the e-veseliba platform, by collaborating with Unified customer service centers. These centers facilitate assistance in managing authorizations and delegations of rights among other services.

They offer consultations both in person and remotely, complementing the direct phone and email support from latvija.lv's service desk. While educational materials specific to the PoAs are not available, each sector provides resources for system use overall, such as the State Revenue Service's guides on various system components. For comprehensive PoA guidance, the Council of Sworn Notaries of Latvia provides fundamental information. Additionally, the annual 'Notāru dienas' event offers an opportunity for free consultations on diverse matters, including PoAs.

6. Lithuania

The primary insights from the report on Lithuania's digital framework for PoAs depict a segmented system that varies across healthcare, taxation, and business sectors, with an advancement towards complete integration still pending.

In the healthcare sector, Lithuania relies on the *e-sveikata* platform for PoA processes, whereas in taxation, users engage with *VMI*, the state tax authority's platform. In the business realm, PoAs are overseen through the *Registrucentras*, facilitating company related PoA management.

Digital identification in Lithuania is anchored by tools like *iPasas* and *VIISP*, bolstering security and legitimacy for users on various platforms. However, these options present diverse authentication methods which could raise security questions and impact the ease of cross-sector and cross-border interoperability.

Internationally, Lithuania grapples with the challenge of cross-border coordination due to the idiosyncrasies inherent in the national registry integration for PoAs, thus complicating EU interoperability. Despite this, the nation is engaged in pilot initiatives such as *OOTS* and *EUDIW*, hinting at progression towards unified digital PoA standards and better alignment with EU digital initiatives.

Legally, sector-specific regulations delineate the creation, use, and termination of PoAs in Lithuania, with legal responsibilities and limitations framed by internal policies, tax legislation, and business law. This defines the liabilities involved and aligns with national legal frameworks governing representation and agency.

On the social front, while strides have been made towards ensuring digital PoAs are accessible to all, the procedures lack complete inclusivity and uniform support across sectors, with tailored adjustments still in development to cater to individuals with disabilities. Despite language support for non-native speakers and guardianship provisions, Lithuania's PoA digital services currently focus predominantly on the business sector, suggesting the need for broader education and facilitation in digital PoA processes for individuals.

As Lithuania advances its digital PoA infrastructure, it faces the dual task of harnessing technological advancements while ensuring social inclusiveness, striving for a harmonized system that addresses all citizen needs in transitioning to a holistic, digital-legal structure.

6.1 Digital and process

This section examines the maturity of technical standards and barriers across access, authentication, verification, and integration of digital PoAs in Lithuania

6.1.1 Technical Standards and ID Infrastructure: Advantages and Disadvantages

The following describes the maturity for technical standards and barriers regarding access, authentication, verification, and integration, alongside cross-border interoperability to highlight advantages and disadvantages in Lithuania.

Table 28. Lithuania's maturity for technical standards and barriers

Digital	Basic	Intermediate	Advanced	Fully integrated
Access to handle PoAs			✓	
Verification		✓		
Authentication		✓		
Integration		✓		
Cross-border interoperability		✓		

Access to handle PoAs

In Lithuania, each sector has separate platform solutions for handling PoAs.

To grant or request PoAs in the **healthcare** sector, such as for picking up prescribed medicine on behalf of another, or managing another person's health related matters, citizens must access the *e-sveikata* platform solution and log in through one of various ID methods. Here, citizens can set PoA scope, choose assignee and determine the duration of the PoA. For the *e-sveikata* platform, concerns have been raised in the public regarding the usability of existing functionality, however, the criticism extends to the e-service platform as a whole, i.e. ESBPI, which is considered less user friendly.

For **taxation** matters, citizens must access the state tax authority's platform solution, *VMI* and log in using on of various ID methods, using the same ID infrastructure as for healthcare matters. On the platform, citizens and companies have full availability of PoA options through various interconnected systems, including selecting roles and exact forms that assignee's have access to read, edit, send, or receive on behalf of the person or company, as well as setting expiration date for the PoA. *VMI* administers several interconnected systems, of which *Mano VMI* is the main to order digital services, including the issuance of PoAs. *EDS* and *i.MAS* are systems for declaring taxes and administrating tax-related information, separately, which the PoAs can be used for. No single PoA can enable an individual person to represent a company in all *VMI* systems.

For **business** matters, most activities related to PoAs are carried out through *Registrucentras*, the (State Enterprise Center of Registers). From here, companies can grant a PoA to an individual to act on behalf of the company, as well as to other legal entities. Assignors can select an assignee, exact services provided to assignee, expiration date and more. Scope and type of PoAs may vary according to industry and type of legal entity.

Overall, the Lithuanian PoA landscape is split into sectors, with access to healthcare, taxation, and business matters occurring on separate platforms. The ease of access to these and sector specificity, indicate an advanced level of maturity regarding access to PoAs.

Verification

In Lithuania, there is one true national ID, which is a personal ID card, the EU-notified *AKT* eID, used with an integrated chip reader or using NFC functionality, linking the chip-enabled card within the mCard LTU application. Verification occurs on VIISP, through the online verification service *iPasas* or an independent identification service, such as bank credentials, state registry, or digital signature when accessing PoA platforms.

VIISP (The State Information Resources Interoperability Platform) is a public system designed to provide a one-stop-shop for individuals to access public and administrative digital services, among other things enabling data exchange and digital identification of a person. To create a PoA, one must login to the specific PoA platform required via *VIISP*. Verification is provided automatically by the system integrating with the national registry data and *VIISP*, using personal code, name, surname for health PoAs. For taxation, the same is needed plus state code to establish identity, as well as email and phone number to ensure communication for taxation. For business, the attestation of attributes includes name, surname, personal identification number (or birth certificate), address of the place of residence, and legal entity code. If an organisation from a foreign country is involved, the name and registered office in country where legal entity is registered would also be necessary.

These are established regardless of which digital identification tool is selected by the user to log in, demonstrating a higher degree of maturity. While the eID is EU-notified, it remains manual in situations needing a card reader for utilisation. Moreover, the variety of ID methods available and the security of identity verification in combination with this can be considered more complex, and thereby less advanced. Thus, verification can be considered at an intermediate level.

Authentication

Authentication in the Lithuanian PoA landscape occurs through the *iPasas*, *VIISP* or taxation identification services. The *iPasas* service can be used for authentication to the healthcare and business platforms for PoA, *e-sveikata* and *Registrucentras* respectively. *iPasas* offers the option to authenticate using a variety of options, these include LTid, text message verification with personal identification number, cryptographic USB, the physical AKT eID chip card, or through electronic banking credentials. Similarly to *iPasas*, the *VIISP* Platform allows authentication via a series of options, which include text message verification with personal identification number, cryptographic USB, physical chip card, eID via browser extension, contactless ID card via QR code, or through electronic banking log in. *VIISP* identification service is used for login to *e-sveikata* and integrates with VMI via API calls. For taxation, *VMI* has its own authentication portal, offering similar authentication options to *iPasas* and *VIISP*. The taxation identification service allows authentication via cryptographic USB, physical chip card, text message through personal identification number, or through electronic banking log in. Similarly, *VMI* integrates to the national registry to verify users upon login.

Overall, the authentication landscape for digital PoAs in Lithuania is extensive and provides many options for login to access PoAs and public digital services. While this gives citizens the liberty to choose authentication option, it also leaves room for compatibility and security concerns. Generally, login via text message authentication has been deemed too insecure, in favour of other forms of multifactor authentication (MFA). The security of login via banking services was not possible to verify and what the physical forms of authentication (cryptographic USB and card), were unclear in terms of what the login is combined with, though physical forms of MFA are generally highly secure. The establishment of a national eID and the integrations across platforms to ensure verification and authentication are positive signs however, and the underlying infrastructure seems to be in place to take the next step in terms of maturity. Currently however, the maturity can be considered intermediate.

Integration

In Lithuania, the PoA landscape is separated distinctly by sectors, with healthcare occurring on one platform, taxation another, and business a third. From the data collected, there was no indication of direct integration between the PoA platforms.

However, there are underlying integrations via *VIISP* and the *State Enterprise Center of Registers*, which administrate the state registers for population, legal entities, PoAs and more. These are used for verification of identity of legal and natural persons first and foremost, as well as the registration of PoAs.

Additionally, the Lithuanian PoA landscape integrates with various forms of authentication. For health, the assignee must show its ID at a pharmacy, but no data informs whether the third-party can verify the validity of a PoA. Nevertheless, the PoA is visible on *e-sveikata*. For taxation, the PoA can only be used for self-service (public e-services) via the platform (*Mano VMI*). When signing in, the user automatically checks the individual's PoA, however, third parties do not need to inspect the PoAs. For business, there is a public search engine allowing to identify POAs in the registry by providing identification number and PoA ID. Overall, the level of integration indicates an intermediate level of maturity.

Cross-border interoperability

In 2023, Lithuania has successfully implemented of the functional capabilities of the electronic identification eIDAS node, which meet the requirements of the *eIDAS* regulation, in the Lithuanian national electronic identification information system. A foreigner may thereby login to public information systems, incl. PoA platforms, by using a foreign *eIDAS* certified ID through *iPasas* on *VIISP*. However, this has not been integrated and does not work in practice yet. Additionally, the verification to access PoAs across sectors requires an integration with the Lithuanian national registry and therefore requires a Lithuanian personal identification number.

The development of an EU approved eID also marks a step in the right direction for eventual cross-border PoAs. Moreover, while EUDIW is being tested, this has currently no relation to PoAs technically, however, the results of the pilot may serve as a breeding ground for future integration. Generally, experts have doubts about implementing cross-border PoAs, as existing initiatives such as eIDAS encounter numerous challenges regarding identity matching, while EU countries frequently update and adjust their systems. This makes the solution potentially unfeasible. Moreover, the findings suggest that some representatives believe cross-border solutions cannot work effectively, due to varying personal ID formats or authentication methods, which can cause challenges when connecting cross-border register. Lithuania does not have a centralised PoA solution today, which means each institution provides, stores, and utilises the PoAs according to internal rules, which would be difficult to align without having a centralised solution within the countries.

Further, despite the OOTS being implemented, facilitating 'once only' principles for digital services to EU citizens, there are currently no perceived benefits for dissemination of cross-border PoAs. Overall, Lithuania can provide access to foreigners with the *eIDAS* portal implemented, but the internal infrastructure is still

not capable for cross-border integration with regards to digital PoAs. With signs of development through, e.g., through EU initiatives, the cross-border interoperability maturity can be considered intermediate.

6.1.2 PoA Process

This section outlines the general process and user journey for the assignors and assignees of PoAs in Lithuania.

Access & verification

Citizens and businesses can access the separate PoA platforms (*e-sveikata*, *VMI*, and *Registrucentras*) by logging in via one of the many authentication methods (methods include: LTid, text message verification with personal identification number, cryptographic USB, physical chip card, contactless ID card via QR code, or through electronic banking log in, depending on the platform). Identity is verified when logging in via integrations with the citizen registry or the use of an eID.

Create PoA

Creation of PoAs occurs on the separate PoA platforms. Generally, the platforms follow very similar steps for creating PoAs. Following access and verification, users can create PoAs according to sector, choose an assignee, for healthcare always a natural person, for taxation and business either natural or legal person, select type of PoA, for taxation and business this goes down to type of forms able to access, edit or send/receive, and select length of PoA. Creation of PoA requires no additional verification or authentication. When creating business related PoAs there is a nominal fee involved depending on the type of PoA, around €4.00, no other PoAs have any costs. For business, there is no act of accepting PoAs, as it is treated as a one side agreement by the Assignor.

Use PoA

Digital use of PoAs generally occurs on the same platform the PoA is created when the assignee logs in to the platform. From here they can access, view, edit, and/or send/receive data depending on the specific PoA. This is however different for Taxation, where the PoA is used on *separate systems, e.g. i.MAS or EDS* for taxation matters, from where accountants or other assignees can use their PoA for matters on behalf of the assignor.

Physical use of a digital PoA is different depending on the sector. A digital PoA for taxation cannot be used when physically visiting the state tax authority but can be used to log in digitally at their local self-service PCs. For physical healthcare PoAs, such as picking up prescribed medicine for someone else, the assignee must show their physical personal ID to utilize the PoA.

For Business cases, there is no distinction between digital and physical PoAs. However, in the situation that notary services may be required, the PoA can no longer be provided digitally, as notary services are not provided digitally.

Terminate PoA

For all PoAs, the assignor can set the duration of validity, fixed or indefinite and PoA is terminated automatically when the date is reached. Termination before expiration date of PoA could not be determined for healthcare matters. For taxation, the both the assignor and assignee can terminate the PoA. For business PoAs, they can be terminated at any time, but must be done physically.

6.2 Legal Aspects

The following section will first present an overview of legal topics, followed by a review of EU initiatives.

In Lithuania, PoAs varies from sector to sector with the specific or limited PoA being the most used. Within health, PoAs are used to view a patient's referrals or picking up medicine, for taxation PoAs can be used for granting access to look at taxation data or submitting tax related forms. For business PoAs are used for e.g. checking a company's data in a register or establishing a subsidiary. According to the data collected the legal basis for health is internal documentation. The legal basis for taxation is the Internal State tax inspectorate legal acts and information system Ts&Cs and for business the legal basis is general provisions regulated by law. Regarding liability the assignor holds the full responsibility, but the specific details are unclear due to insufficient data. Barriers to granting PoAs within the three sectors in Lithuania include age and mental capacity. Lastly, Lithuania is in the pilot phase for OOTS and EUDIW, but still in the planning phase or yet to being with implementing the other EU initiatives.

6.2.1 Legal Topics

This section covers the legal topics also included in the main report: semantics, types of PoAs, legal basis, liability, and legal barriers.

Semantics

Table 29. Role descriptions of various sectors

	Health sector	Taxation sector	Business sector
Assignor	Anyone	For legal persons: Head of the company For physical persons: Anyone	Head of the company
Assignee	Any physical person with a Lithuanian ID number	Any physical or legal person registered in Lithuania (has Lithuanian ID number)	Any physical or legal person registered in Lithuania (has Lithuanian ID number)

Types of PoA

Regarding the viewing power to view a patient's referrals and execution power e.g. picking up medicine the PoA used is specific or limited, which allows the assignee to act on behalf of the assignor in specific matters. For taxation the PoA used is either specific or limited, for viewing power e.g. access to look at taxation data, execution power e.g. submitting tax related forms or decision power e.g. possibility to add assignees. For business the PoA used is also either specific or limited for viewing power e.g. checking a company's data in a register, execution power e.g. competing and providing electronic sets of financial reports or decision power e.g. establishing a subsidiary.

Legal basis

According to the data collected by the country experts, the legal basis for PoAs within the health sector is internal documentation (internal procedural documents approved by the Ministry of Health or the Registry centre) These documents work as low-level documents defining certain internal procedures. Based on the other sectors which are regulated, it is assumed that there must be some legislation that regulated PoAs within the health sector.

Regarding the taxation sector, the legal basis is the Internal State tax inspectorate legal acts and information system Ts&Cs, with which the user must be familiarized and must confirm.

For business matters, the legal basis is a combination of general provisions, that are regulated by law, and special matters that are regulated by the institution or company to which PoA is submitted.

Liability

The assignor holds full responsibility for the PoA, including notifying about the PoA assignee and informing third parties. When the PoA is notarized, additional security considerations are addressed. The data collected on liability is limited, and it is therefore assumed that liability in Lithuania is regulated similarly to the other countries.

Barriers

Regarding the health sector, the assignor, and the assignee (the user) must be 18 years old or older, or legally emancipated. For taxation matters the assignor and assignee (user) must be 18 years or older, additionally it is assumed that the person must be of appropriate legal capacity. Within the business sector, both parties (the user) must be 18 years or older and be of appropriate legal capacity.

6.2.2 Status of implementation of relevant EU initiatives

The table below summarises the implementation status for each regulative in the Lithuanian context. The content is unfolded in the section below.

Table 30. The implementation status for each regulative in Lithuania

Legal	Have not started	Planning implementatio	Pilot phase or partly implemented	Fully implemented
Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)		✓		
Once Only Technical System (OOTS)			✓	
EU Single Digital Gateway Regulation (SDGR)	✓			
EU Digital Identity Wallet (EUDIW)			✓	
The European Health Data Space (EHDS)			**N/A**	
Upgrading Digital Company Law (UDCL)			**N/A**	

Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)

The score of eIDAS 2.0 for Lithuania is fairly uncertain. There is no information regarding this in the data collection. The revised version of eIDAS is being implemented towards 2026. Therefore, it is assumed that Lithuania must be at least in the planning implementation stage because the full implementation is time consuming. The score is therefore set at 2, but this is an assumption and with a level of uncertainty.

Once Only Technical System (OOTS)

The OOTS is currently being implemented as part of the "Digital Services Platform" project, which began in May 2023 and is set to be completed by April 2026. The system facilitates the "once only" principle for providing digital services to EU citizens, allowing secure cross-border data exchanges through the eDelivery network.

Single Digital Gateway Regulation (SDGR)

No grade included above, as sufficient data was not available to the country expert.

EU Digital Identity Wallet (EUDIW)

Lithuania is participating in the pilot project POTENTIAL for the development of a technical solution for testing digital driver's license. Lithuania is participating in the project together with, among others, Estonia, Germany, and France. The EUDIW are currently facing challenges related to difficulties in mapping the information on how and which institution will process the data, which attributes will be stored etc.

The European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL)

Grades for the implementation of EHDS and UDCL are not included, cf. paragraph 3.3.2 above.

6.3 Social Inclusion

In Lithuania, where a digital PoA is not attainable, individuals must visit a Registry Centre to obtain one in person, a situation that mainly affects the elderly. Despite official e-services like Epaslaugos.lt being only partially translated into English, the country adheres to EU regulations, including EN 301 549 and WCAG 2.1, to enhance accessibility for people with impairments. However, gaps remain, especially for those with visual disabilities due to insufficient implementation of these standards.

There are no existing technical solutions for guardians to manage PoAs for the vulnerable, and the process is tightly governed by legal frameworks. Nonetheless, modifications are possible when represented by associations calling for such changes.

Digital PoAs in Lithuania are limited mostly to business use at this time, lacking centralization and widespread educational support, unlike in neighbouring Latvia where PoAs can be managed either in paper form or digitally across various sectors. Latvia provides more robust language support and navigational assistance for its e-services through customer service centers, despite similar challenges with complete digital inclusivity.

Table 31. Status of efforts in ensuring digital inclusion

Social	Have not started	Planning implementation	Partly implemented	Fully implemented
Options for physical PoAs				✓
English language options available			✓	
Information Systems for people with impairments			✓	
Alternative access to digital ID				✓
Spokesperson/ representation of other people to obtain a PoA		✓		
Education, support-service and facilitators to obtain a digital PoA		✓		

6.3.1 Options for physical PoAs

In cases where a digital PoA cannot be obtained, the only alternative is to go to a physical office of the Registry Centre and demand to issue a digital PoA on-site. It is especially elderly people who are the target group for the physical procedure.

6.3.2 English language options available

The official administrative and public e-service portal, Epaslaugos.lt, is in Lithuanian and partly translated into English depending on the services of request.

6.3.3 Information Systems for people with impairments

Both EN 301 549 and WCAG 2.1 are implemented in Lithuania as part of the broader European Union regulations on accessibility. EN 301 549, which includes WCAG 2.1 standards, is the EU's accessibility framework for Information and Communication Technology (ICT). It sets requirements for public sector services and products to ensure they are accessible to individuals with disabilities.

IS solution is not adapted to people with visual impairments, which arise from several factors. Primarily, there may have been an oversight during the design and development stages, where accessibility standards like WCAG were not fully integrated or enforced. Furthermore, existing infrastructure and content might not have been audited or updated to meet these standards post-implementation, leading to gaps in accessibility. Lastly, the absence of a formal procedure to ensure continued adherence to accessibility guidelines can lead to such shortcomings not being systematically identified and addressed.

6.3.4 Alternative access to digital ID

I'm not sure if I understood the question's intent. But you can always access your digital services (including the ID itself) if you go directly to the local branch office of the respective institutions (Tax Inspection Authority or the Registry Centre). No external organisations/institutions participate in this process.

6.3.5 Spokesperson/ representation of other people to obtain a PoA

There are currently no technical solutions available for guardians to assist vulnerable individuals in establishing a PoA. However, PoA processes are developed according to legal acts and regulations. If associations representing specific interest groups submit requests for improvements, efforts are made to implement changes, provided they are both technically and legally feasible.

6.3.6 Education, support-service and facilitators to obtain a digital PoA

Digital PoAs are still a fairly niche service in Lithuania, mostly needed only by businesses. Since the issuance of digital PoAs is not centralized, there have been no notable efforts in making education, support-service and facilitators to obtain a digital PoA.

7. Norway

The analysis of Norway's digital PoA infrastructure reveals a system in transition, striving to weave together digital, legal, and cross-border elements to boost convenience and inclusiveness.

Norway's approach entails distinct digital platforms for handling PoAs across the sectors of healthcare, taxation, and business. These platforms are rooted in a solid eID framework that is broadly embraced by Norwegians, enhancing identification and verification processes essential for PoA functions.

The country, however, faces hurdles in achieving cross-border coherence, particularly in validating foreign nationals' identities and PoAs. Alignment with the EU's legal standards, including *eIDAS 2.0*, remains a work in progress. National efforts are discernible in initiatives like *eIDAS 2.0* adoption, reflecting a wider movement toward consolidating digital PoA structures and fostering better data interchange in accordance with European norms.

From a social perspective, Norway is proactive in making digital PoA services reachable to individuals with disabilities and has provided mechanisms for manual PoAs. These initiatives are complemented by multilingual support across digital platforms, aiding users who may not speak Norwegian and ensuring representation for those needing help with PoA engagements.

Norwegian PoA statutes are distinctly outlined within its sectors, influenced by laws like the Norwegian Agreement Act and specific legislations catering to taxation and healthcare. These regulations prescribe the extent of liabilities and enforce compliance with the country's legal tenets related to agency and contractual dealings.

As Norway progresses in optimizing its digital PoA landscape, it needs to balance technological advancement with social equity, ensuring the digital shift includes adequate support for all citizens, thereby fostering an inclusive, electronically enabled legal environment.

7.1 Digital and process

This section examines the maturity of technical standards and barriers across access, authentication, verification, and integration of digital PoAs in Norway.

7.1.1 Technical Standards and ID Infrastructure: Advantages and Disadvantages

The following describes the maturity for technical standards and barriers regarding access, authentication, verification, and integration, alongside cross-border interoperability to highlight advantages and disadvantages in Norway.

Table 32. Norway's maturity for technical standards and barriers

Digital	Basic	Intermediate	Advanced	Fully integrated
Access to handle PoAs		✓		
Verification			✓	
Authentication			✓	
Integration		✓		
Cross-border interoperability		✓		

Access to handle PoAs

In Norway, there are a few access points to handle PoAs that are generally sector specific. PoA matters are split up according to healthcare, taxation, banking and more. One portal, *Altinn*, connects citizens with public and private entities, and integrates some PoAs for the relevant sectors, such as taxation and business. This platform connects various digital services and allows for the creation of PoAs, notifications and more for some sectors.

For healthcare matters, citizens can log into the national healthcare portal, *HelseNorge*. In HelseNorge, citizens can access, view, and create PoAs digitally, as well as use any PoAs they have been assigned on behalf of their assignors.

Taxation matters can be conducted in the taxation authority's portal, *Skatteetaten*, with some also available in *Altinn*. Skatteetaten uses Altinn-APIs to delegate digital PoAs. On both platforms, PoAs can be viewed and assigned both in digital formats, as well as more traditional forms that can be filled out as PDFs and submitted with physical or electronic signature. In some cases, attorneys or lawyers need to handle

tax matters for a company, to which they need to fill out a form to request access to the tax files. The forms are available digitally at *Skatteetaten*, where there is currently one PoA options (view taxa. The Norwegian Tax Administration will then inform the assignor (company) that the assignee has applied for access. Further, a different form must be filled out for non-digital citizens to grant a PoA to a trusted private person to handle their tax matters. The forms are sent by e-mail to the Norwegian tax administration.

In the business sector, general PoA matters are handled in *Altinn* as well. However, the most frequently used PoAs identified in the business sector in Norway in this report involve mainly banking matters, which require a consent-based loan application, transferring PoA to bank or insurance, or for bank account affairs. Hence, the PoA is primarily handled directly with the bank/insurance company. Moreover, the business sector has established other platforms that are partly based on PoAs regarding Debt (norsgjeld.no) and Pension (norskpensjon.no).

PoAs are generally handled digitally in Norway through access to various PoA platforms and health, tax, and business matters in many cases works well with predefined PoAs. However, the country's general landscape does not appear entirely clear, which lands Norway on an intermediate level. *Altinn*, interestingly, is scheduled to be phased out and replaced by *Altinn 3.0*, a more developed version by 2026, which may strengthen the access and integrations, including for private matters.

Verification

Norway's PoA platforms utilizes a strong ID infrastructure setup to verify citizens and businesses through eIDs. The eID solutions include *BankID*, *Buypass*, *Commfides*, and *MinID*, which are all attached to personal identification number of Norwegian citizens. All eID solutions can be used as means to verify citizens' identity to access PoA platforms (e.g. *HelseNorge* or *Skatteetaten*). Moreover, the three solutions are at the highest level of security, which demonstrates a high level of verification maturity for digital PoAs.

Generally, BankID is issued by citizens' bank and is the most used eID mean in Norway and is also the necessary means for an assignor to grant PoAs related to banking matters, with *MinID* as an alternative.

Authentication

The Norwegian eID infrastructure leverages the robust authentication mechanisms of the various eIDs available, which all use a form of qualified electronic signature in combination with multi factor authentication. This uses either, physical key codes, authenticator apps, or physical authentication in combination with the personal identification number and a password.

BankID is the most widely used eID in Norway. *BankID* is a PKI solution where a private key is generated and stored, used to sign and authenticate, which is protected with respective pin codes. Citizens selects login via BankID and writes their personal identification number. Hereafter, they open the app, and enter a personal password.

Buypass has various ID and authentication methods, including PKI on a "smart card", mobile 2 factor authentication, PKI for mobile and biometric ID.

Commfides is mostly used by firms, e.g., pharmacy technicians, and involves a card-reader.

The solutions demonstrate a high level of authentication in Norway, with the use of an eID being necessary for all digital PoA steps.

Integration

In Norway, there is no central PoA administration platform solution integrating all PoAs (public or private). Instead, PoAs for healthcare, taxation and business matters are handled separately.

Furthermore, the health system is not fully integrated with other public health services in the sector. For instance, a PoA for HelseNorge services cannot be used to access services in Helfo (the Norwegian Health Economics Administration).

Several interviewees have voiced a need for a general archive of PoAs. PoAs can cover several sectors, e.g., bank and health, but if it is only possible to register within one sector, it will not be accessible to other third parties looking to validify a request from the person that had been given the PoA.

Altinn is the digital service providing integration for PoA matters, as Skatteetaten integrates fully with the platform. *Altinn* also provides digital services and PoAs for some business matters. However, it is not an overall repository of PoAs and does not integrate with healthcare or other sectors. The upcoming version 3.0 of *Altinn* may develop the level of integration in Norway.

Additionally, the *DSOP* collaboration, a collaboration between state and business actors for digitalization, provides a link between actors to send data for information such as banking, insurance, debt registrations, and more, when requested and if authorised. However, this is does not integrate with PoA solutions, from the data collected.

Overall, integration is fragmented across the Norwegian PoA landscape, with some developments being made. Maturity can be considered as intermediate. No further data was collected regarding authorization or integration standards.

Cross-border interoperability

Today, all Norwegian PoAs requires personal identification numbers, which are issued for national citizens and linked to the digital identities through eID mechanisms. For example, Altinn relies on the credentials of the personal identification number. Thus, foreign citizens and business cannot digitally request or grant a PoA.

The biggest challenge to this is around matching identities with foreign citizens and businesses. It is thereby suggested to enable the acceptance of other EU countries' national eID to provide access for foreigners.

Furthermore, the fact that the sectors are not even integrated nationally, as for the healthcare sector. Integrating with health services across borders may therefore be a complex exercise.

7.1.2 PoA Process

Access & verification

For healthcare matters, Norwegian citizens can login to *HelseNorge* to handle PoAs. For taxation matters citizens can login to *Skatteetaten* or *Altinn*. Other digital PoAs and business matters can be accessed through *Altinn* or banks/the specific service's websites.

Creating the PoA

For healthcare matters, PoAs can be created directly in *HelseNorge*. For taxation matters this can be done either on *Skatteetaten* or on *Altinn*, however, there is also the option to do it via PDF forms filled out and sent to the tax authorities.

For banking and other PoAs an assignor must fill out a form, either online via the individual platforms or by printing out a PDF.

PoAs are stored on government servers (*HelseNorge, Skatteetaten, Altinn*) or at Bank's or other third party servers.

There are no costs involved.

Some PoAs grants permission without acceptance by default (e.g., PoAs for parent/child or bank account affairs), while others require the assignee to fill out a form (e.g., Next of kin to people not capable of taking care of themselves). Moreover, this is the case if assigner is requesting the PoA.

For some taxation matters, the assignee is required to e-mail its signature on paper to the Norwegian tax administration. For companies, this is done between the company and the private person or the company they are representing.

For other taxation matters, the financial institution sends an SMS to the person applying for a loan, the loaner logs in with BankID, gives consent (PoA) for the institution to get the necessary information from the tax authority.

Use PoA

For all the citizen PoAs in question, the PoAs can be used directly when logging into the adequate platforms, e.g., *HelseNorge*, *Altinn*, or the assignor's bank account. Similarly, companies (e.g., banks) can access the assignor's data upon having created a PoA.

Third-party interactions also differ slightly. In some cases, an ID is sufficient (e.g., analogue PoA to handle dead persons estate). For healthcare PoAs involving physical presence, such as picking up prescribed medicine, the data suggests that assignee can show ID at the pharmacy.

Terminate PoA

A PoA can be valid for a limited period, indefinitely, or until withdrawn by the assignor or assignee (both can do so). PoAs that are still valid can be changed, e.g. by assignor for healthcare matters. When a PoA is changed, it will be deleted, and a new one is automatically created with the changes. Deleted and invalid PoAs will automatically be moved to the historical archive from where they, in most cases, are deleted after five years. Communication channels for notifications are for health received in HelseNorge or via DigiPost. Some authorities also use SMS, e.g. for tax authorities to notify assignor to provide consent through BankID.

In case of changes to regulations or the implementation of new digital services, the Tax Administration may change the scope of the permission regarding the bank account affairs. Consequently, rights may differ from the original mandate. Significant changes to the scope of PoAs will be notified at least four weeks in advance.

7.2 Legal Aspects

The following section will first present an overview of legal topics, followed by a review of EU initiatives.

In Norway powers of attorney (PoAs) are used across in the health, taxation and business sectors, e.g. granting parents' rights to act on behalf of their children (up to age 16), to handle the assignors' assets if the assignor dies or for loan applications for businesses. The legal basis in Norway is primarily, Lov om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer (avtaleloven), supplemented by other acts in specific matters. There is limited data on liability regarding PoAs in Norway, but it is assumed to be similar to the Nordic standard. Legal barriers exist for minors (under the age of 18) and for people with mental limitations, and in certain instances one must have a registered address in Norway.

7.2.1 Legal Topics

This section covers the legal topics also included in the main report: semantics, types of PoAs, legal basis, liability, and legal barriers.

Semantics

Table 33. Role descriptions of various sectors

	Health sector	Taxation sector	Business sector
Assignor	Parents or citizen with capabilities.	Private person or a person who is in charge of the tax affairs for a company. Could also be the local court.	Bank costumer or insurance costumer
Assignee	The persons with the official parental responsibility.	Either a private trusted person (e.g. a family member), or an accountant or lawyer.	Another private person, often a family member or person within a close circle of the bank costumer. Could also be a company through an authorized person, e.g., CEO.

A third party in Norway could be the tax authority, public authorities and financial institutions who are members of the DSOP-cooperation. Some financial institutions who are a part of the DSOP are; Brønnøysundregisteret, Bits AS and Finans Noreg. However, especially The Norwegian Tax Authority is frequently a third party since they are the ones providing information about tax and income. Moreover, it is often creditors who interact as third parties, typically electricity suppliers, healthcare providers, and others who have a claim against the customer.

Types of PoAs

The most commonly used PoA within the health sector is the general PoA grating parents rights to act on behalf of children up until 16 years of age. This PoA grants parents the right to represent their kids in contact with health service providers.

Within the taxation sector, a specific/limited PoAs to view, execute, granting decision power, access assignors' bank account and to handle assignors' assets such as real estate if the assignor dies is commonly used.

For businesses, a PoA regarding bank account affairs and loan application is commonly used.

Legal basis

In Norway, the legal basis for agreements and PoA is very similar to the Danish since the contract law in the Nordic countries are very similar. However, in Norway it is the Norwegian Agreement Act ("LOV-1918-05-31-4 Lov om avslutning av avtaler, om fuldmagt og om ugyldige viljeserklæringer (avtaleloven)") that includes sections on PoAs and when they are legally binding.

The data collected from Norway also show that regarding health PoAs the Act "LOV-1999-07-02-63 Lov om pasient- og brukerrettigheter" is applicable. If the PoA includes circumstances regarding death the Act "LOV-2019-06-14-21 Lov om arv og dødsboskifte" is applicable. Moreover, the Act "LOV-2022-12-16-90 Lov om regnskapsførere" is applicable for taxation matters.

Liability

In general, data regarding the liability in PoAs in Norway was not available to the country expert.

However, since the legal basis seem very similar in the Nordic countries, there is reason to assume that liability regulation is similar, as well. Thus, the paragraph liability regulation in Denmark may provide useful information on liability in Norway.

However, within the health sector, the PoA must be written by the patient, given to someone, and the guardian parent must consign if the PoA concerns cognitive disabilities.

A potential liability challenge shown by the data collection is that foster parents is not considered in the regulation, which may be troubling under the circumstances where the biological parents might still have PoA.

Legal barriers

In Norway, the age of 18 of the citizen is a barrier when granting or being granted a PoA. Furthermore, the mental health status of the citizen is also fundamental.

Within the taxation sector, the assignor/assignee must be an accountant or lawyer if representing a company.

Within the business sector, the mental health status is also important. Furthermore, the assignor/assignee must be in a position to represent the company. Additionally, one must have a registered address in Norway to apply for loans.

Furthermore, the collected data shows a specific challenge regarding loans. Apparently, taking out loans cross-border at this point is not possible since all loan applications is denied if the registered address is not in Norway.

7.2.2 Status of implementation of relevant EU initiatives

The table below summarises the implementation status for each regulative in the Norwegian context. The content is unfolded in the section below.

Table 34. The implementation status for each regulative in Norway

Legal	Have not started	Planning implementatio	Pilot phase or partly implemented	Fully implemented
Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)		✓		
Once Only Technical System (OOTS)			✓	
EU Single Digital Gateway Regulation (SDGR)		✓		
EU Digital Identity Wallet (EUDIW)			✓	
The European Health Data Space (EHDS)		✓		
Upgrading Digital Company Law (UDCL)			**N/A**	

Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)

The eIDAS 2.0 entered into force mid-2024, with an implementation deadline for national EUDIWs at late-2026 at the latest. Due to the insufficient data collected it hasn't been possible to provide further information about this regulation in Norway. Additionally, this means that the score given is indefinite due to the missing data.

Once Only Technical System (OOTS)

OOTS 2.0 Project started in spring 2024. Phase one will last until the first half of 2025 and concentrate on studies on Legal and Technical Aspects. After that the

project group consisting of national SDG and OOTS coordinators and experts will choose the proof-of-concept implementations that are carried out within the framework of the project. The project is planned to end at the end of 2026.

EU Single Digital Gateway Regulation (SDGR)

Applies to Norway as well but may have a different application deadline than the EU-members. According to supplementary data collected, the Norwegian Directorate of Digitalization, the regulation is not completely implemented in Norwegian legislation, but the Directorate is working on meeting the requirements set in the regulation.

EU Digital Identity Wallet (EUDIW)

According to the European Commission, Norway is participating in four large-scale pilot projects that are testing the EU Digital Identity Wallet and leading one of them. These projects were launched in May 202 and cover use cases such as digital driving licenses, payments, and educational and professional qualifications. The pilots are expected to continue until 2025.

The European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL)

The collected data shows the Norwegian Authority for E-health is following the development of the regulation and making assessments along the way to determine how to comply with the regulation, thus qualifying for the score 2.

However, grades for the implementation of EHDS and UDCL are not included, cf. paragraph 3.3.2 above.

7.3 Social Inclusion

In the table below, the progress of Norway's endeavours in facilitating digital inclusivity is depicted. The ensuing narrative details the various initiatives Norway has undertaken in this domain. The table categorizes the status of these measures, highlighting those that have been fully realized and others still under partial implementation. Overall, Norway demonstrates a significant adoption of these identified measures within its public sector, culminating in a high degree of digital accessibility and integration.

Table 35. Norway's endeavours in facilitating digital inclusivity

Social	Have not started	Planning implementation	Partly implemented	Fully implemented
Options for physical PoAs				✓
English language options available				✓
Information Systems for people with impairments				✓
Alternative access to digital ID			✓	
Spokesperson/ representation of other people to obtain a PoA				✓
Education, support-service and facilitators to obtain a digital PoA			✓	

7.3.1 Options for physical PoAs

Options for physical PoAs include downloading and filling out paper forms offered by various institutions, such as NAV, pharmacies, Kartverket, UDI, or Posten. These can be signed and delivered physically or uploaded for processing. Legal websites like Jurio or Justify also provide services to create PoAs, with options for digital or physical signing. It's generally more challenging to draft a handwritten PoA due to concerns over witnesses and validity.

7.3.2 English language options available

The two digital platforms for dialogue between businesses, private individuals and public agencies, altinn.no and helsenorge.no, are available in English, Nynorsk and Bokmål.

7.3.3 Information Systems for people with impairments

EN 301 549 has been implemented in Norway, although Norway is not a member of the EU. As part of the European Economic Area (EEA), which includes EU member states and the three EFTA (European Free Trade Association), Norway has implemented the EU Web Accessibility Directive (Directive (EU) 2016/2102), which references EN 301 549. Therefore, Norway is obligated to implement the same accessibility requirements for public sector websites and mobile applications as EU member states. In extension, the standard is implemented for both public and private sector websites designed or updated after 2014.[7]

7.3.4 Alternative access to digital ID

Various digital login methods exist for public services in Norway, typically requiring a personal identification number. An alternative without such a requirement is the Commfides USB pin. Options include MinID issued by the Digitalisation Agency, BankID provided by banks, Buypass ID in smart card or mobile form, and Commfides, a secure USB pin issued by Commfides Norge AS at a cost and requiring a physical ID card or passport.

7.3.5 Spokesperson/ representation of other people to obtain a PoA

Legal PoA is a statutory right that allows an individual to represent a family member who is unable to manage their own affairs as described in vergemålsloven §94 §85. This authority does not require a formal PoA from the family member in question, nor the appointment of a guardian. The law grants this right to a specific group of individuals—close relatives—enabling them to act on behalf of the person through legal PoA.

7.3.6 Education, support-service and facilitators to obtain a digital PoA

Entities like Digihjelpen from the Norwegian Association of Local and Regional Authorities (KS) offer guidance and support at community locations such as libraries or service centers for individuals needing assistance with digital services. Additionally, volunteer organizations like the Red Cross and public libraries provide similar support services.

---

7. Web Accessibility in Europe: The Full Compliance Guide (2024)

8. Sweden

The exploration of Sweden's digital PoA infrastructure reveals a complex environment characterized by both advancements and challenges.

Sweden's digital landscape for PoAs shows varying levels of integration, with advanced platforms in some sectors like healthcare, via *Läkemedelskollen*, but only partial digital solutions in areas such as business affairs. The recently launched *Mina ombud* PoA platform solution exemplifies Sweden's strive towards a holistic digital approach, seeking to unify PoA management across multiple domains.

Authentication and verification mechanisms are robust within national boundaries, anchored by eIDs that tie into a strong level of trust. Yet cross-border PoA recognition and validation present significant stumbling blocks, with *eIDAS* alignment and cross-border solutions still under development. Sweden anticipates amendments to its digital identity infrastructure following EU directives and ongoing national assessments.

Legal frameworks such as the Swedish Agreement Act, alongside sector-specific acts, govern the PoAs validity and administration. However, data on PoA liabilities remains limited, with Sweden often aligning with broader Nordic norms. Sweden is currently in the pilot phase or has already party implemented key EU initiatives, such as OOTS, EUDIW and SDGR, while being in the planning phase for eIDAS 2.0.

Inclusion efforts are evident, with strategies to address the needs of individuals with impairments and those lacking Swedish personal identifiers. Multilingual options and support systems are in place to expand digital inclusiveness; nonetheless, access to digital PoAs for non-Norwegian speakers and representation for individuals needing assistance in PoA activities are areas that need further enhancement.

Sweden's commitment to evolving its PoA frameworks, while aiming to align with European legal standards, reflects a wider ambition to facilitate a seamless digital transition. Moving forward, Sweden must navigate the complexities of integrating technology with legal requirements and inclusivity to provide a comprehensive and accessible digital PoA system.

8.1 Digital and process

This section examines the maturity of technical standards and barriers across access, authentication, verification, and integration of digital PoAs in Sweden.

8.1.1 Technical Standards and ID Infrastructure: Advantages and Disadvantages

The following describes the maturity for technical standards and barriers regarding access, authentication, verification, and integration, alongside cross-border interoperability to highlight advantages and disadvantages in Sweden.

Table 36. Sweden's maturity for technical standards and barriers

Digital	Basic	Intermediate	Advanced	Fully integrated
Access to handle PoAs			✓	
Verification			✓	
Authentication		✓		
Integration		✓		
Cross-border interoperability	✓			

Access to handle PoAs

Läkemedelskollen offers multiple options for establishing a PoA, either fully digitally through its website or in person at any pharmacy. Similarly, the Swedish Tax Agency allows for the creation, modification, or termination of a PoA entirely online. A common theme across all these examples is that specific PoAs can be established digitally. However, the degree of digitalization in other areas varies. For example, the Swedish Companies Registration Office's PoA solution is only partially digital. In their services, the assignor must scan a PDF and upload it to their e-service, which differs from the fully digital PoA processes offered by the Swedish Tax Agency and the Swedish eHealth Agency.

One of the more interesting initiatives that came across in the interviews is the development of *Mina ombud*, in English 'My representatives'. It is a platform that aims to standardize and fully digitalize PoAs across sectors in one single platform. The Platform was launched October 2024. It is a platform where it is possible to hand out PoAs, see if they are distributed and to get an overview of the current PoAs a person holds. Digital PoAs can be distributed and used through Mina ombud for PoAs by municipalities, authorities and other organisations that have joined 'mina ombud'.[8] (Nb. The platforms mentioned above has not joined Mina ombud yet).

A public entity can join Mina ombud, so that users can create a PoA with the entity. The public entity then creates a PoA template, where a template contains one or more permissions that can be assigned to a PoA assignee. The template forms the basis for what a PoA looks like. An affiliated party is responsible for creating PoA templates and their permissions. Mina ombud store the PoA templates and offer a service where the assignor can create them. An affiliated party owns the PoA templates that they create. When a company, an association or a private individual wants to distribute a PoA to an assignee, the service minaombud.se will present the PoA templates that are available from those who are connected to *Mina ombud*. The Assignor can then choose from the permissions available in a template and decide on the permissions to be assigned.

To use the functionality on *minaombud.se*, the user needs to identify themselves with an e-ID at trust level 3, such as *BankID*. Mina ombud is part of a larger project for Sweden's digital government where a number of authorities are responsible for the parts that are being developed right now. It is the Swedish Company Registration Office that is responsible for the development, administration and technical operation of Mina ombud. The work is funded by the European Union through NextGenerationEU.[9]

Almost all respondents referred to "Mina ombud" when asked questions about cross-border PoAs, with the expectation that it will address most of the challenges raised regarding cross-border PoAs.

Verification

Verification happens for health through official documents like passports, ID cards, or electronic identification methods as: BankID, Freja eID or Foreign eID, which has a Trustlevel 3 (a Swedish standard for e-identificaiton[10]). When pharmacy staff handle the registration of a PoA based on a physical form, the assignor's identification is always required if the assignor submits the form. If the assignee submits the form, both the assignor's and assignee's identification must be verified.

8. See the joined parties here: https://minaombud.se/info/anslutna-parter
9. https://minaombud.se/info/om-oss
10. https://www.digg.se/digitala-tjanster/e-legitimering/tillitsnivaer-for-e-legitimering

For taxation it happens through BankID, FrejaID plus or AB Svenska Pass with a Trust level 3 as mentioned above. A smaller proportion of the authorizations established at the Swedish Tax Agency (Skatteverket) are submitted on paper. For these, a manual identity check is carried out, which may include verification of attached documents, among other things. And lastly for business matters it happens through BankID, Freja eID plus, Telia or Foreign eID, with Trust level 3.

The eID are connected to following attributes: Family Name, First Name, Date of Birth, Person Identifier. For all sectors, the verification process supports the digital access to PoAs to a strong degree.

Authentication

Following authentication options are available for health, taxation, and business matters, but does not work across borders: BankID, Freja eID Plus, Foreign eID including authentication services e.g. authenticator app.

The process for verifying a PoA varies depending on the context. When a private individual accesses the services of the Swedish eHealth Agency (via Läkemedelskollen or a pharmacy's e-commerce platform) to register or utilize a PoA, they must log in using e-identification. The system verifies whether the logged-in individual's personal number is authorized to act.

Integration

For health, taxation, and business matters, there are APIs for Läkemedelskollen/ Skatteverket/ Bolagsverket PoA-handling, machine-to-machine-integration grows fast. However, all the above mentioned PoA platforms use different IT infrastructure.

It is uncertain when the OOTS is going to be implemented in Sweden. As of this moment, DIGG (Agency for Digital Government in Sweden) is waiting for a governmental investigation of the technical conditions. The aim is that the OOTS will become active in the second part of 2025.

Cross-border interoperability

Verification and authentication do not happen for cross-border identities. There are not any cross-border solutions for PoAs now but there are ongoing discussions regarding solutions.

For eIDAS within health, it is not possible at this moment. The system for taxation is prepared for eIDAS and Skatteverket is adding new applications to allow eIDAS for authorization using PoA. But so far there has not been a very big demand from other countries (if any). For business matters, if the PoA has been signed with an EU certified eID in another country and want to use it in Sweden, The National Courts Administration can validate the PoA manually.

The greatest challenges in connection to cross-border solutions now are in connection to individuals that do not have a social security number or individuals who has a secure identity, cannot use the services. Authorizing individuals that do not have a Swedish social security number, is a challenge at the moment, which The National Courts Administration do not think they have any authority over, as it needs to be solved at a higher level.

In June 2024, the Governmental investigation "A Secure and Accessible Digital Identity" presented several proposals for implementing the eIDAS regulation in its final report. This is the same government investigation that previously developed proposals for a national e-ID. The report suggests that Digg should be responsible for providing and managing digital identity wallets for both individuals and legal entities in Sweden. It also proposes that Digg handle personal data management for these wallets, while the Swedish Companies Registration Office (Bolagsverket) should manage data for legal entities.[11]

The report is now being reviewed by the Government Offices before a decision is made on how the digital identity wallet will function in Sweden and which authorities will oversee its implementation. The proposed regulations are expected to take effect on 1 October 2025.

8.1.2 PoA Process

Access & verification

Access to health PoAs happens through *Läkemedelskollen*, by logging in with either BankId, Freja EID Plus or Foreign eID. For taxation it is through *skatteverket* by logging in with either BankID, FrejaID plus or AB Svenska Pass. Lastly for business matters it happens via *Verksamt* or The National Courts Administration 's website by logging in with same verification types as mentioned for health (Through BankID, Freja eID plus or Foreign eID).

Create PoA

PoAs being created for health are done through *Läkemedelskollen* where an individual can change the duration of the PoA, and the pharmacy you will get registered. For a legal guardian the PoA is registered automatically through the population registration. E.g. A parent or guardian can automatically see the child's information and act on the child's behalf.

For taxation the PoAs are created by the assignor, who can create and customize the PoA inside of the platform skatteverket.

For creation of PoAs for business matters it depends on the specific PoA. Swedish Companies Registration Office has no authority over how the PoA is established, as

11. https://www.digg.se/om-oss/nyheter/digital-identitet/nyheter/2024-06-20-nyckelroll-for-digg-i-utvecklingen-av-nya-e-legitimeringstjanster

it is not fully digital. After a Business has signed a PoA physically, they can then upload it in the e-service where it gets stored by Bolagsverket.

For court cases it can be created fully digitally though their website (The National Courts Administration) or written by paper and scanned in.

Accepting health PoAs is done by either identifying yourself as the assignor at any pharmacy or registration of the PoA online. The assignee accepts by ether identifying yourself at any pharmacy or accepting the terms via the e-service. For a PoA registered digitally, the assignee awaits consent from the assignor for up to seven days. For legal guardians the acceptance is done automatically through the population registration. Notifications happens through governmental- or secure message platform.

For taxation, accepting a PoA happens by logging into the platform with the verified login method (Through BankID, FrejaID plus or AB Svenska Pass). Lastly for business matters it is by signing the PoA physically, and for court cases it is done by logging into the platform with the verified login method (Through BankID, Freja eID plus or Foreign eID), and notifications happens through governmental or secure message platform.

Use PoA

The PoAs for health are used mainly to collect pharmaceuticals on the assignee's behalf or for a child. The third-party interactions happen by having PoAs registered in their pharmacy systems and validating them through id card at the pharmacies. Same happens for taxation, as it concerns managing the assignors tax declaration, and where Skatteverket goes through each PoA and verifies its validity. And lastly for business matters it depends on the specific PoA or court case.

Terminate PoA

Changes is updated in Läkemedelkollen's systems as well as the pharmacy's systems. A child under the age of 18 can't terminate a PoA that is created by the guardian.

If changes happen to the PoA within Skatteverket's system, the assignor and assignee will be notified. Termination can be made through Skatteverket's system.

The assignor must notify the Swedish Companies Registration Office where they can terminate it or change the contents of the PoA digitally. Regarding changing a court case PoA, it is done by either setting up a new PoA or contacting the specific court, asking to make changes or to terminate it.

8.2 Legal Aspects

The following section will first present an overview of legal topics, followed by a review of EU initiatives.

In Sweden, Powers of Attorney (PoA) are used within health and taxation sectors, with typical ones including permissions to pick up medicine and handling tax returns. The Swedish Agreement Act governs the legality of PoAs, with specific acts for health and tax matters. Assigning a PoA can be done in person at a pharmacy or online for health-related matters, and through specific systems or agencies for taxation and business matters. There is limited data on PoA liability in Sweden, but it is assumed to be similar to the Nordic standard. Legal barriers exist for minors and obtaining a Swedish eID requires a social security number, registration at a Swedish address, and permission for those over 13. Sweden is currently in the pilot phase or has already party implemented key EU initiatives, such as OOTS, EUDIW and SDGR, while being in the planning phase for eIDAS 2.0.

8.2.1 Legal Topics

This section covers the legal topics also included in the main report: semantics, types of PoAs, legal basis, liability, and legal barriers.

Semantics

Table 37. Role descriptions for various sectors

	Health sector	Taxation sector	Business sector
Assignor	Individual person or a child	Individuals, sole proprietorships, companies, partnerships, limited partnerships, and economic associations can use the e-service "Ombud och behörigheter" (Agents and Authorizations). Companies where the firm is signed by multiple people jointly can also use it.	An individual or a company wanting to create a PoA.
Assignee	Individual persons, legal guardians, and employees at healthcare providers	Individual person & companies	An individual or company who has been given the right to be the assignee or anyone that the PoA is assigned to, e.g. family member, partner etc.

A third party in Sweden within the health and taxation sectors could be a Pharmacy, The Swedish eHealth Agency, Swedish Tax Agency. In the business sector, it could be anyone according to Swedish Companies Registration Office. It depends on the specific PoA and where it is being used.

Types of PoAs

In Sweden, the typical PoAs are PoAs to pick up medicine and parent guardian. Within the taxation sector the most frequently used PoAs are regarding tax return, and for businesses PoAs regarding company signatory.

Legal basis

In Sweden, the legal basis for agreements and PoA is very similar to the Danish since the contract law in the Nordic countries are very similar to each other. However, in Sweden it is the Swedish Agreement Act ("Lag 1915:218 om avtal och andra rättshandlingar på förmögenhetsrättens område") that includes sections on PoAs and when they are legally binding.

The data collected from Sweden also shows that regarding health PoAs the Act (2018:1212) on the National List of Medicinal Products is applicable, and regarding taxation matters, the Tax Procedure Act (2011:1244) ("Skatteförfarandelag") and Administrative Procedure Act (2017:900) ("Förvaltningslag") is applicable. For business matters there is no other relevant regulation stated in the data collection.

If an assignor wants to grant an assignee a PoA within the health sector, it can either be done by identifying yourself and the assignee at any pharmacy or register the PoA online. If the PoA is made online, the assignee has to accept the terms via the e-service. In case a child under the age of 18 wants to terminate a PoA which is created by its guardian, it is not possible to terminate the PoA at this point.

Within the taxation sector, it is possible to terminate, revoke or change a PoA by changing it manually through "Skatteverkets" systems.

Within the business sector, the assignor has to notify "Bolagsverket" if they want to terminate the PoA. This can be done by either logging in to the e-service or contacting the specific court.

Liability

In general, there is a lack of data available to our country expert regarding the liability in PoAs in Sweden. However, since the legal basis seem very similar in the Nordic countries, there is reason to assume that liability regulation is similar, as well. Thus, the paragraph on liability regulation in Denmark may provide useful information on liability in Sweden.

Furthermore, in Sweden, it is stated that regarding taxation PoAs, Skatteverket goes through each PoA and verifies its validity.

Legal barriers

In Sweden, it is only possible for adults (currently 18 years old) who can request/apply to have a representative registered for them. For example, for minors, it is the parents (guardians) who have the right to sign.

In order to receive an eID in Sweden, the data collected is insufficient, but you must have a Swedish social security number and must be registered in a Swedish address. Moreover, the citizen applying for a Swedish eID must be over the age of 18. If the citizen is over the age of 13 it is possible to have the eID if a guardian grants permission to this.

8.2.2 Status of implementation of relevant EU initiatives

The table below summarises the implementation status for each regulative in the Swedish context. The content is unfolded in the section below.

Table 38. The implementation status for each regulative in Sweden

Legal	Have not started	Planning implementatio	Pilot phase or partly implemented	Fully implemented
Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)		✓		
Once Only Technical System (OOTS)			✓	
EU Single Digital Gateway Regulation (SDGR)			✓	
EU Digital Identity Wallet (EUDIW)			✓	
The European Health Data Space (EHDS)	✓			
Upgrading Digital Company Law (UDCL)			**N/A**	

Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)

The revised version of eIDAS is being implemented towards 2026 according to Myndigheten för digital förvaltning. According to the data collected, most of the respondents are already affected by the eIDAS and will be even more in the implementation of the EU-wallet. There is a possibility that the platform "Mina ombud" will be affected the most because of the work that is being done at the moment, as described above.

Once Only Technical System (OOTS)

The once-only principle became operational in Sweden in December 2023. However, in the European Commission's "June 2024 version of the OOTS Acceleratormeter" it is currently in a production ready phase, where the configuration needs to be finalized and it needs to be connected to the Evidence Provider or Requester before making the first transactions.

EU Single Digital Gateway Regulation (SDGR)

Missing data regarding the implementation of this regulation, but according to Myndigheten för digital förvaltning, it will be implemented in H2 2025

EU Digital Identity Wallet (EUDIW)

Sweden is involved in two pilot projects regarding the EUDIW including the Digital Credentials for Europe (DC4EU) and EU Digital Identity Wallet Consortium (EWC). Sweden expects to have regulations regarding the EUDIW ready and taking effect on 1 October 2025.

The European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL)

Grades for the implementation of EHDS and UDCL are not included, cf. paragraph 3.3.2 above. However, according to the data collected, significant work is underway concerning the EHDS, including efforts related to enabling a national digital infrastructure for health data. In this regard, the Swedish eHealth Agency is closely monitoring these developments and maintains an ongoing dialogue with the investigation. The investigation is set to deliver its final report on 1 April 2026, and as of today, there is therefore no clear answer on how the eHealth Agency's authorization services will be affected by the EHDS.

8.3 Social inclusion

In the table below, the strategies employed by Sweden to improve digital inclusion are outlined. The narrative elucidates the options for individuals including those with impairments or without Swedish personal numbers, detailing both digital and physical alternatives for accessing PoA and participating in digital life. Notably, while the Swedish eHealth Agency's services are chiefly in Swedish, measures are in place to cater to those needing assistance, highlighting a blend of implementation levels across these provisions. Sweden's commitment to these inclusivity initiatives, as mandated by the EU Directive and national laws, reflects a concerted effort towards broad digital accessibility.

However, when asking about vulnerable groups in interviews, interviewees indicated that while the topic has been discussed, it is not actively addressed in the PoA process. Issues often arise with foreign identification, but there are no standardized solutions, and each case is handled individually. To strengthen Sweden's work with digital inclusion, the Swedish eHealth Agency regularly conducts usability tests, which have included elderly participants with varying levels of digital literacy. Also, tests with other vulnerable groups are performed.

Table 39. Sweden's strategy to improve digital inclusion

Social	Have not started	Planning implementation	Partly implemented	Fully implemented
Options for physical PoAs				✓
English language options available			✓	
Information Systems for people with impairments				✓
Alternative access to digital ID				✓
Spokesperson/ representation of other people to obtain a PoA				✓
Education, support-service and facilitators to obtain a digital PoA			✓	

8.3.1 Options for physical PoAs

In certain situations, using a digital PoA is either not feasible or inappropriate. For example, individuals with protected personal information cannot use digital PoAs due to concerns about traceability; instead, they must use paper forms, which must be presented each time the PoA is needed. The Swedish eHealth Agency is not involved in these cases, and if an individual receives protected personal data, any previously registered digital authorization is deleted. Digital PoAs are only available to individuals with a Swedish personal number and are not designed for those without one, including individuals with coordination numbers. Importantly, a digital PoA is not required for collecting medications from a pharmacy, as the Swedish eHealth Agency does not mandate that PoAs be registered in their PoA system.

8.3.2 English language options available

In general, PoA forms are translated into English, but no other languages are currently supported. The Swedish eHealth Agency's website is available in several languages; however, the services are available in Swedish only.

8.3.3 Information Systems for people with impairments

The European standard EN 301 549 is implemented in Sweden. It sets accessibility requirements for ICT products and services and is used to ensure compliance with the European Union's Web Accessibility Directive. This directive mandates that public sector websites and mobile applications be accessible to all users, including individuals with disabilities. In Sweden, the relevant legislation supporting this is the Act (2018:1937) on accessibility to digital public services, which integrates EN 301 549 into its framework. The Agency for Digital Government (DIGG) oversees compliance with these accessibility standards. The law applies to public sector bodies, and while private entities may adopt these guidelines voluntarily, public sector compliance is mandatory.[12]

8.3.4 Alternative access to digital ID

Individuals without e-identification can register a PoA by submitting the necessary form and presenting valid identification. If a person is unable to physically sign the PoA but understands its significance, they can still authorize it in the presence of two witnesses. In such cases, either the principal or the agent may for example visit a pharmacy to complete the registration of the PoA.

12. Sweden | Web Accessibility Initiative (WAI) | W3C

8.3.5 Spokesperson/ representation of other people to obtain a PoA

An assignee can register a PoA on behalf of the individual they represent, both with healthcare providers and private entities. This must be done using a physical form, which can be submitted, for example, at any pharmacy. The assignee must provide identification and a certificate proving their legal status as the principal's guardian. The certificate must specifically state that the assignment includes "caring for the person," thereby authorizing the guardian to issue a PoA for pharmacy-related matters on the principal's behalf.

8.3.6 Education, support-service and facilitators to obtain a digital PoA

There is no national standard for training people who are not familiar with digital services, even when it comes to e-identification. There are good examples of training programs for people who are not familiar with IT and digital services, but there is no national standard. For example, there are several examples of municipalities, counties and private companies offering IT training for the elderly. The courses are often free and held at regular intervals.

APPENDIX 2: PoAs IN EACH COUNTRY

Sector & Country	PoA title	Description of PoA
Health		
Denmark	Medical authority (The collected data did not specify the three most frequently used PoAs)	View health data on behalf of another person, pick up prescribed medicine from the pharmacy. Typically used for elderly or incapacitated individuals. Gives the assignee authority to make medical treatment decisions on behalf of the assignor, incl. surgeries etc.
Finland	Prescription	Allows picking up prescribed medicine on behalf of another person.
	Manage health info	View health data and access information and (re)schedule appointments
	Handle social care matters	View social care related data, search for social services, receive information of decisions related to social care, and declare and receive data related to social care.
Iceland	Prescription	Allows picking up prescribed medicine on behalf of another person.
	Representing children	Parents/Guardians have access to My pages on Heilsuvera.is for their children up to the age of 16
Norway	Representing children	This a power of attorney for people with parental responsibility (could be a parent or another guardian in general).
	Execution power, e.g. Pick up medicine	This a power of attorney for natural persons. It is used by guardians to access HelseNorge's services, which includes access to doctor appointments, communication with the doctor, receipts, test resultets, vaccine cards, patient travel, free pass ("frikort"), and more.
	Decision power, e.g. Choosing between medical treatments	It is used by guardians to access HelseNorge's services, which includes access to doctor appointments, communication with the doctor, receipts, test resultets, vaccine cards, patient travel, free pass ("frikort"), and more.

Sweden	Prescription	Allows picking up prescribed medicine on behalf of another person.
	Parent guardian	Legal guardians can act as representatives (assigner) for their child in contacts with the healthcare system via the 1177 Vårdguiden e-services. This means that they can carry out the child's tasks via their own login.
	PoA Pick up medicine (Employees at healthcare providers)	A specific PoA that grants authorization for employees at healthcare providers to pick up medicine for an individual.
Estonia	Prescription	Allows picking up prescribed medicine on behalf of another person, as well as ordering on e-pharmacies.
	Manage health info	Viewing a patient's health data in the health Portal.
Lithuania	Prescription	Allows picking up prescribed medicine on behalf of another person.
	Review patient referrals	Allows patients to authorise specific individuals to manage their health-related matters. This authority can include access to medical records, reviewing vaccination schedules, collecting prescriptions, and submitting requests on behalf of the patient.
Latvia	Prescription	Allows picking up prescribed medicine on behalf of another person.
	Decision and viewing power	Right to make treatment-related decisions for the patient, as well as to receive medical information
Taxation		
Denmark	Manage tax info	Grants accountants or other trusted persons access to view and manage tax info on behalf of another person, submit annual tax returns, handle tax-related tasks, etc.
Finland	Handle all taxation matters	PoA to handle all taxation matters including making tax declarations and viewing tax information
	Tax declaration	PoA to make tax declarations
	Handle real estate tax matters	PoA to handle all real estate tax matters

Iceland	Returning VAT	Allows company representative to submit VAT returns on behalf of a business.
	Pay	Grants authority to manage payroll tax obligations
	Tax returns	Provides access to the tax administration's web portal, enabling representatives to file tax returns, access tax information, and perform other related tasks
Norway	Viewing, execution and decision power, power granted to access assignors bank account	The purpose of the PoA is to grant access to an individual who is competent to handle tax matters on your behalf. Can be a family member, an accountant, or a lawyer.
	Limits to access information about salary and last year's tax-return papers for assignors loan application	Cooperation between the bank and several public agencies is necessary to gather information for a loan application.
	PoA to handle a dead person's estate.	PoA automatically given to the public administration to handle the estate. Can be transferred to private person, should they decide to execute a private shift of estate.
Sweden	Tax return	The Swedish tax agency offers a service where individuals and companies can give digital authorizations to another person or company, such as an accountant, to handle declarations, tax payments, and other tax matters.
Estonia	Manage tax info for legal or natural person	Manage tax info on behalf of another person or business, submit annual tax returns, handle tax-related tasks. Accountant access for legal persons includes rights to key applications necessary for fulfilling tax obligations.
	Performing actions on behalf of a legal entity	The legal entity's access rights manager (assignor) in the e-services environment of the Estonian Tax and Customs Board has granted the individual (assignee) rights to perform actions not as a package, but as individual permissions. (execution power)
	Access Rights of Management Board Members in the e-services environment	Access Rights (PoA) of Management Board Members in the e-services environment of the Estonian Tax and Customs Board. (decision power)

Lithuania	Access to look at taxation data, specific or all available taxation related forms within the system.	All PoAs can be customized not only by roles but also by exact forms that the person can have access to read, edit, send/receive on behalf of the legal person.
	Submit certain or all available taxation related forms within the system or edit them	All PoAs can be customized not only by roles but also by exact forms that the person can have access to read, edit, send/receive on behalf of the legal person.
	Possibility to add assignees	All PoAs can be customized not only by roles but also by exact forms that the person can have access to read, edit, send/receive on behalf of the legal person.
Latvia	Access to look in taxation data for natural persons	Grants accountants or other trusted persons access to view and manage tax info on behalf of another person, submit annual tax returns, handle tax-related tasks, etc.
	Access to look in taxation data for legal persons	Grants accountants or other trusted persons access to view and manage tax info on behalf of another person, submit annual tax returns, handle tax-related tasks, etc.
Business		
Denmark	Business authorization (Not specifically defined)	Allows an authorized person to execute business transactions, such as filing reports, applying for permits, or conducting administrative tasks, granting authorizations to other organizations and more.
Finland	Processing Salary Information	Allows for a representative to process and view salary information.
	Customs clearance	PoA that allows for management of customs clearance matters
	Application for company funding	With this authorisation, the assignee can handle business funding applications, their follow-up and payment requests on behalf of the delegate.
Iceland	Company Representation	Allows for CEO or other legal person to access company data, or act on behalf of the company.

Norway	Viewing, execution and decision power, power granted to access assignor's bank account	The purpose of the PoA is to grant another person access to one`s bank account, typically to assist with the payment of bills and similar tasks.
	Viewing power, e.g. gather information for assignor's loan application	Cooperation between the bank and several public agencies is necessary to gather information for a loan application.
	Viewing power, e.g. grants power to assignor's bank and insurance companies for easier transition between companies	Grants power of attorney to the bank/insurance company when you want to switch banks/insurance companies.
Sweden	Company Signatory	Business owners can use digital authorizations to grant other individuals, such as accountants or employees, access to the company's affairs with the Swedish Companies Registration Office (Bolagsverket), for example, to submit annual reports or make changes to company registrations.
	Court case PoA	The purpose of the PoA is to act on behalf of another individual or company in a court case.
Estonia	Performing actions in bank	A member of the company's management board can create a business client account in the bank's self-service environment and then add representatives authorized to act on behalf of the company to view or perform operations related to the company's data in the bank's self-service portal.
	Submitting statistical reports in the Statistics Office's self-service portal eSTAT.	A legal entity's authorized representative has the right to add data reporters, i.e., questionnaire responders, for their company.
	PoA for entering and submitting the annual report	The authorized representative may grant PoA for the report entry and submission, for example, to an accountant(s). The accountant can input the data, monitor the signing of the report, and track when the auditor signs the opinion.

Lithuania	Checking a company's data in register	In the PoA registry, the CEO of the company, or in case of some legal person forms, person equal to that is the only person able to access company's data (view, edit, apply for, etc)
	Completing and providing electronic sets of financial reports	In the PoA registry, the CEO of the company, or in case of some legal person forms, person equal to that is the only person able to access company's data (view, edit, apply for, etc)
	Establishing a subsidiary	In the PoA registry, the CEO of the company, or in case of some legal person forms, person equal to that is the only person able to access company's data (view, edit, apply for, etc)
Latvia	Viewing power, e.g. checking a company's data in register	On the service portal of the Enterprise Register a legal entity can grant a certain amount of rights to a natural person to work on the portal with a legal entity profile (delegation).
	Execution power, e.g. applying for a permit	A merchant can authorize a person to conclude transactions or perform commercial activities on behalf of the merchant.
	Decision power, e.g. establishing a subsidiary	A merchant can authorize a person to conclude transactions or perform commercial activities on behalf of the merchant.

APPENDIX 3: FREQUENTLY USED ABBREVIATIONS

In the following section, an overview of the frequently used abbreviations is described.

Electronic, Identification, Authentication and Trust Services (eIDAS 2.0)

The European Digital Identity Regulation (Regulation (EU) 2024/1183), also known as eIDAS 2.0entered into force on 20 May 2024. eIDAS 2.0. is an upgrade to the original eIDAS regulation from 2016 and aims to introduce new trust services and digital identity solutions. A key feature of eIDAS 2.0 is the EUDIW, providing a digital platform to control and share personal data, cf. below. Another key feature is the cross-border interoperability across EU member states, by enabling a uniform recognition of electronic identification, which facilitates easier access to services.

EU Digital Identity Wallet (EUDIW)

The EUDIW is a wallet app providing EU citizens with control over their personal data and the opportunity to decide when and with whom to share it with. EUDIW will be a secure and easy way for European citizens, residents, and businesses to prove who they are when accessing digital services. The wallet app will enable citizens to safely obtain, store and share important digital documents about yourself and electronically sign or seal documents, e.g. bank statements, university records or job applications. Each Member State will offer at least one version of the EUDIW, built to the same common specifications. Each member state shall provide at least one European Digital Identity Wallet before 21 November 2026, which is 24 months after the date of entry into force of the implementations acts (21 November 2024).

Nordic-Baltic eID (NOBID)

The Nordic-Baltic eID Project (NOBID) is a collaborative arena for innovations enabling access to national digital services to users from other countries. Countries involved are Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden. The project was a key component in the NCM Cross Border Digital Services-programme and is currently leading a consortium of Nordic and Baltic countries who, together with Italy and Germany, are developing a large-scale pilot for the payment use case in the EU Digital Wallet.

Once Only Technical System (OOTS)

The Once Only Technical System (OOTS) enables the sharing of information between public administrations across borders between EU countries. The system is cross-sectorial and can be expanded beyond the current scope of life events set out in the Single Digital Gateway Regulation. It puts into practice the Once-Only Principle, which states that citizens should not be forced to provide information to authorities if another authority already holds that information in electronic format. The legal deadline for implementing the Once Only Technical system was 12 December 2023.

EU Single Digital Gateway Regulation (SDGR)

The SDGR provides the legal framework for the creation of a trusted European data space for public administrations to share information, including administrative procedures and assistance services for residents and businesses in the EU. The multifaceted EU-wide initiative strives to create the digital infrastructure required to overcome these challenges and help citizens and businesses make best use of the Single Market. SDGR entered into force on 11 December 2018.

The European Health Data Space Regulation (EHDS)

The EHDS aims to create an ecosystem for health data sharing and utilization across EU member states. The initiative provides a single market for electronic health record systems, allowing individuals to take control over their health data and facilitate the exchange for healthcare delivery across the EU.

This also provides a trustworthy and efficient system for reusing health data for research, innovation, policy-making and other regulatory activities.

The status of EHDS is that the European Parliament approved the creation on 24 April 2024. The provisional agreement still needs to be formally approved by the Council. Once published in the Official Journal of the EU, it will enter into force 20 days later and then applied two years after (with certain exceptions).

Upgrading Digital Company Law (UDCL)

This EU company law initiative aims to improve transparency regarding EU companies, by making more data available across the EU member states.

Additionally, the UDCL allows for the cross-border use of trustworthy data and modernizing EU company law by digitalizing this.

The European Commission published a proposed directive in March 2023. The next steps regarding the UDCL involves negotiations between the Council and the European Parliament. If the directive is adopted each EU member state will have two years to transpose it into national legislation.

APPENDIX 4: REGULATIONS

eIDAS 2.0 2024/1183, Including EU Digital Identity Wallet

Regarding i) Digital Identity Wallet

A central element to the eIDAS 2.0 regulation is the European Digital Identity Wallet (EUDIW). The EUDIW will be rolled out, in the form of apps, and allow citizens, residents and businesses to digitally identify themselves. By 21 November 2026, each member state must provide at least one EUDIW to its citizens, cf. art. 5a, section 1.

The EUDIW adds enhanced measures regarding security and privacy, where users will be able to securely request, obtain, select, store, delete, share and present personal identification data and, when applicable, in combination with electronic attestations of attributes, authenticate relying parties both online and offline, to access public and private services, cf. art. 5a, section 4 (a). These data may, among other personal identification data, include PoA's.

In addition, this will also allow for the selective disclosure of data. The EUDIW will enforce the right to pseudonymity, where users can store pseudonyms, adding a layer of privacy.

Regarding ii) Electronic attestation of attributes

Another important element is the electronic attestation of attributes, especially when using PoAs. These are attestations in electronic form allowing the authentication of features, characteristics or qualities for natural and legal persons. According to the regulation member states shall ensure that these electronic attestations have the same legal effect as lawfully issued attestations in paper form, cf. art. 45b.

The following minimum list of attributes is included in eIDAS 2.0, cf. annex VI:

- Address
- Age
- Gender
- Civil status
- Family composition
- Nationality or citizenship

- Educational qualifications, titles, and licenses
- Professional qualifications, titles, and licenses
- Powers and mandates to represent natural or legal persons
- Public permits and licenses
- For legal persons, financial and company data

Regarding iii) Unequivocal identity matching

The regulation aims to improve cross-border electronic identification between Member States, which ensures interoperability and trust in digital interactions within the EU, e.g. in connection with cross border PoA use. Thus, when acting as a relying party for cross-border services, Member States shall ensure unequivocal identity matching for natural persons using notified electronic identification means or EUDIW, cf. art. 11a.

Single Digital Gateway Regulation 2017/1724, including Once Only Technical System

Regarding i) Your Europe Portal

According to the regulation the Commission and Member States are to establish the SDG. The SDG must consist of a common user interface managed by the Commission and be integrated into the "Your Europe" portal. The Your Europe portal shall give access to relevant Union and national webpages, cf. art. 2.

Regarding ii) Access to information

Member States are responsible for ensuring that users have easy, online access on their national webpages to specific information from a national level, while the Commission is responsible for ensuring that the Your Europe portal provides users with easy online access to specific information from a Union level, cf. art. 4.

The information includes e.g. rights, obligations and rules laid down in Union and national law that are applicable to users exercising or intending to exercise their rights derived from Union law in the field of the internal market in the areas listed in Annex I (e.g. travel, work and retirement within the Union or taking a vehicle to another Member State). It is reasonable to assume that Member States will include information on EU citizens' abilities to exercise their rights by the use of PoA's, including for cross-border actions.

For the Member State and the Commission to comply with Article 4, they must follow the quality requirements related to information, cf. art. 9–11.

Regarding iii) Once-Only Technical System

Operating within the SDG Regulation framework, the OOTS enables the sharing of information between public administrations cross-border between EU countries. The OOTS implements the "once-only" principle and is core infrastructure in the implementation of the SDG.

When natural and legal persons complete an online procedure in one Member State, the system will be able to make a request to automatically and securely retrieve official documents or structured data from a public authority's eGovernment portal in another Member State, cf. art. 14. As shown below in para. **Error! Reference source not found.**, OOTS may be utilized as a platform for cross border PoA use.

Considering the complex nature of the OOTS system, an initial manual process might be necessary to verify the accuracy of data retrieved via OOTS. Over time, these verifications could be automated, enhancing the efficiency of cross-border administrative tasks.

While exploring these possibilities, it's vital to approach the potential applications of the OOTS with a view toward understanding its capabilities, rather than prescribing specific recommendations. Continuing research and analysis will be essential to fully grasp how this technology can be best utilized for streamlined cross-border activities, particularly with respect to PoAs and assignments. The observations here aim to open discussions around the evolution of these systems and their role in facilitating easier, more effective cross-border transactions and administrative processes.

Proposals: European Health Data Space (EHDS) and Upgrading Digital Company Law (UDCL)

EHDS
Regarding i) Primary use of data

Natural persons will have a variety of rights regarding the primary use of their personal electronic health data. These rights include e.g. the access to their personal electronic health data processed in the context of primary use of electronic health data, or the right to receive an electronic copy, cf. (EU) COM/2022/197 art. 3. All these rights may be possible to invoke by the use of PoA's.

When health professionals are processing data in an electronic format, they shall e.g., have access to the electronic health data of natural persons under their treatment (regardless of the Member State of affiliation/treatment) and ensure

that the data of the person they treat are fully updated, cf. art. 4. The Commission shall, by implementing acts, set the technical specifications for the European electronic health record exchange format, cf. art. 6.

Regarding ii) Secondary use of data

The proposal lists a variety of minimum categories for the secondary use of electronic data, e.g. reusing health data for research, innovation or policy making and regulatory activities. Data holders shall make the electronic data available, such as, EHRs (electronic health record), data impacting on health, relevant pathogen genomic data, person generated electronic health data or electronic health data from clinical trials, cf. art. 33.

Additionally, the proposal lists a variety of purposes for which electronic health data can be processed. This includes, to produce national, multi-national and Union level official statistics related to the health/care sectors, for education or teaching activities in the health/care sector or scientific research related to the health/care sectors, cf. art. 34.

Prohibited secondary uses of electronic health data includes, for advertising or marketing activities towards health professionals, organizations in health or natural person, or to give access to health data to third parties not mentioned in the data permit, cf. art. 35.

UDCL

Regarding i) Information about companies

Member States must ensure compulsory disclosure of companies listed in Annex IIB (list of partnerships in the Member States) of at least documents and information, such as, the name of the partnership, legal form of the partnership and the registration number of the partnership, cf. (EU) COM (2003)177 art. 14a. These rules may aid with ensuring sufficient identification when using PoA's in corporate relations, e.g. agreements involving at least one company

The directive introduces an obligation for Member States to ensure the ultimate parent company governed by the law of a Member State discloses where it is registered and at least information, such as, name and legal form of each subsidiary, cf. art. 14b.

Information about companies that are listed in Annex II and IIB are to be stored in registers referred to in article 16 and kept up to date, cf. art. 15.

Regarding ii) Digital EU PoA

Member states must ensure that, when carrying out procedures in another Member State, companies listed in Annex II and IIB may use a standard model of the digital EU PoA, to authorize a person to represent the company, cf. art. 16c.

The digital EU PoA shall be drawn up and revoked in accordance with national legislation and other formal requirements. The requirements must at least include the verification of identity, legal capacity and authority to represent the company of the assignor.

Additionally, the digital EU PoA must be compatible with EUDIW.

ABOUT THIS PUBLICATION

Analysis on Power of Attorney in the Nordic Baltic region

TemaNord 2025:537

ISBN 978-92-893-8253-3 (PDF)
ISBN 978-92-893-8254-0 (ONLINE)
http://dx.doi.org/10.6027/temanord2025-537

Cover photo: Unsplash
Published: April 2025

Disclaimer

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

Rights and permissions

third-party content may include, but are not limited to, tables, figures or images.

Photo rights (further permission required for reuse):

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

Nordic co-operation

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

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

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

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

Read more Nordic publications on www.norden.org/publications