



ANALYSIS AND CONCLUSIONS ON EXISTING ELECTRONIC MANDATE SYSTEMS IN THE EUROPEAN UNION

STATE OF AFFAIRS OF EU EMANDATE SYSTEMS

31/10/2018

Document characteristics

Deliverable name	Analysis and conclusions on existing electronic mandate systems in the European Union
Owner	DIGIT
Version	V2.0
Status	Submitted for second review
Due date	September 2018
Authors	Danaë Desplanques danae.desplanques@everis.com Virginia Gomariz Gonzalez virginia.gomariz.gonzalez@everis.com Nicoletta Roselli nicoletta.roselli@everis.com Enric Staromiejski Torregrosa Enric.Staromiejski.Torregrosa@everis.com
Reviewed by	
Approved by	

Document history

Version	Description	Date
v 1.0	Document submitted for review	16.07.2018
V 1.1	Second revision after comments by the client	18.09.2018
V 2.0	Final version	31.10.2018

Disclaimer

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this document. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

TABLE OF CONTENTS

1. Executive summary	13
2. Introduction	14
2.1. ISA ² Programme Action 2016.12	14
2.2. Main deliverables and outputs	14
Shortlist of MS to be assessed	15
Shortlist of prioritised services for cross-border RPaM	15
Assessment of AS-IS situation	15
Conceptual models.....	15
Information requirements and feasible solutions	16
Recommendations and next steps.....	17
2.3. Document scope and objectives	17
2.4. Definitions	18
2.5. Methodology.....	20
Choice of case studies	20
Information researched	20
Methods	20
2.6. Structure of the report.....	21
3. State-of-affairs on eMandate systems in six MS.....	23
3.1. What eMandate system(s) exist in the analysed MS?	23
Austria	23
Belgium.....	24
Finland.....	25
The Netherlands.....	26
Portugal	27
Spain.....	27
Comparative analysis: commonalities and differences.....	28
3.2. For which sectors, public services applications, business cases and use cases are eMandates available?	29
Austria	29
Belgium.....	30
Finland.....	33
The Netherlands.....	33
Portugal	34

Spain	35
Comparative analysis: commonalities and differences.....	36
3.3. What types of representations are covered by the eMandate system?	37
Austria	38
Belgium.....	38
Finland.....	38
The Netherlands.....	39
Portugal	39
Spain	39
Comparative analysis: commonalities and differences.....	39
3.4. From which register is the identification and authentication information retrieved?40	
Austria	40
Belgium.....	41
Finland.....	42
The Netherlands.....	42
Portugal	42
Spain	43
Comparative analysis: commonalities and differences.....	43
3.5. Where are the eMandates stored and how are they digitally preserved?	44
Austria	44
Belgium.....	44
Finland.....	45
The Netherlands.....	46
Portugal	46
Spain	46
Comparative analysis: commonalities and differences.....	47
3.6. Who issues the eMandates and where can the end-user manage them?	47
Austria	47
Belgium.....	48
Finland.....	48
The Netherlands.....	49
Portugal	49
Spain	49
Comparative analysis: commonalities and differences.....	49

3.7.	Do the MS have national vocabularies and/or specifications for eMandates?	50
	Austria	50
	Belgium.....	51
	Finland.....	51
	The Netherlands.....	52
	Portugal.....	52
	Spain.....	52
	Comparative analysis: commonalities and differences.....	53
3.8.	What legal framework impacts the eMandate system?	54
	Austria	54
	Belgium.....	55
	Finland.....	57
	The Netherlands.....	59
	Portugal.....	60
	Spain.....	62
	Comparative analysis: commonalities and differences.....	65
4.	Conclusions of the desk research.....	67
5.	Annexes.....	68
5.1.	Annex I – Lists of public service applications	69
	Austria	69
	Belgium.....	70
	Finland.....	75
5.2.	Annex II – Lists of business cases	77
	Belgium.....	77
	Finland.....	85
5.3.	Annex III – Lists of use cases	90
	Belgium.....	90
	Spain.....	90
5.4.	Annex IV – Online questionnaire answers	92
	Austria	92
	Czech Republic	96
	Portugal.....	99
	Spain.....	102

LIST OF FIGURES

Figure 1: The Austrian web-service for electronic Mandates	23
Figure 2: Example of an NSSO e-procurement document.....	24
Figure 3: Suomi.fi e-Authorisations service	25
Figure 4: CSAM service offering (current and planned).....	31
Figure 5: Management of Access Managers	32
Figure 6: CRR, SourcePIN and ssPIN numbers.....	41
Figure 7: Architecture of the online Mandate service EGIZ	44
Figure 8: Number of active Mandates in SSM.....	45
Figure 9: Identification and authentication access (CSAM)	48
Figure 10: Website to download the Austrian Specifications of Electronic Mandates... 50	
Figure 11: Attributes provided for natural persons under the SCAP eID scheme	52

LIST OF TABLES

Table 1: Business cases and use cases matrix	15
Table 2: Comparative analysis of the eMandate system(s)	28
Table 3: Comparative analysis of eMandate system availability	37
Table 4: Comparative analysis of types of persons and types of representation.....	40
Table 5: National specification AS-IS detailed overview	50
Table 6: Legal framework AS-IS detailed overview.....	54
Table 7: Comparative analysis of legal framework impacting eMandate systems.....	65
Table 21: Examples of business cases in Finland	85

LIST OF ABBREVIATIONS

eID	Electronic Identity Document
EU	European Union
LP	Legal Person
LL	Legal Person representing a Legal Person
LN	Legal Person representing a Natural Person
MS	Member States
NL	Natural Person representing a Legal Person
NN	Natural Person representing a Natural Person
NP	Natural Person
RPaM	Representation Powers and Mandates

GLOSSARY

Administration to Administration	A public administration requesting a service from another public administration.
Administration to Business	A public administration requesting a service from a business.
Administration to Citizen	A public administration requesting a service from a citizen.
Archiver	Entity/authority storing the Mandate.
Bilateral Mandate	A Mandate that, along with requiring the approval of the Mandator, also necessitates the approval/acceptance of the Mandate by its recipient, i.e. the Mandatee.
Business to Administration	A business requesting a service from the public administration.
Business to Business	A business requesting a service from another business.
Business to Citizen	A business requesting a service from a citizen.
Citizen to Administration	A citizen requesting a service from the public administration.
Citizen to Business	A citizen requesting a service from a business.
Citizen to Citizen	A citizen requesting a service from another citizen.
Continuing Power of Representation	An eMandate appointing a natural person to represent another natural person in case of loss of the decision-making capacity of the Mandator (e.g. accident, Alzheimer, etc.). The Mandator appoints a Mandatee, who must agree to this authorisation, and define the scope.
Core vocabulary	Simplified, re-usable and extensible data models that capture the fundamental characteristics of a data entity in a context-neutral and syntax-neutral fashion.
Cross-border login	The ability of citizens from other European countries to log in to other European countries' e-services with their own national eID and vice versa.
Cross-border-by-default	Accessible for all citizens in the EU.
Cross-sector-by-default	Accessible for different organisational domains.

Data availability	Making data available at the moment when it is required, as well as ensuring that systems enabling data provision are running and accessible.
Data confidentiality	Keeping private data private, and allowing the data subject to decide when and on what terms its attributes may be revealed.
Data integrity	Assurance that the data available is correct, implying the application of the correct data format and the provision of the correct data value.
Digital-by-default	The processes of creating, updating and revoking cross-border electronic Mandates that are preferably completed entirely via digital channels.
eAuthentication	An electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.
eAuthorisation	An electronic process that enables a natural person to access and use a system. It occurs after previous identification and eAuthentication in that system.
eCODEX	e-Justice domain enabling citizens and businesses to have cross-border access to legal means in Europe.
eDocument	A set of interrelated information representing the facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual, that the capability exchanges with other capabilities to support the execution of value streams.
eIdentification	The process of using person identification data in electronic form to represent either a natural or legal person, or a natural person representing a legal person.
eMandate	An eDocument that proves that a Mandator has assigned his/her powers to one or more Mandatees.
eMandate process requirement	Requirement that an actor must meet to be legitimately involved in an eMandate and make the Mandate valid.
eMandate restriction	Restrictions applying to the eMandate, for example time restrictions and financial restrictions.

eMandate transfer	An eMandate can be transferred by a Mandatee to a sub-Mandatee, who will then have the power to execute activities on behalf of the Mandator. The Mandatee needs an authorisation by the Mandator to transfer the eMandate.
ePower	An eDocument that proves that a natural person has the legal capacity, the right or the privilege to access a Service Provider System. ePowers are evidences.. ePowers are evidences.
Entity	Legal or natural person.
eSignature	CEF building block to allow public administrations and businesses to accelerate the creation and verification of electronic signatures.
Excise	An excise or excise tax is any duty on manufactured goods which is levied at the moment of manufacture, rather than at sale.
General eMandate	An eMandate encompassing all affairs of the Mandator, i.e. it entails in principle a universal right to represent the Mandator.
Individual eMandate	An eMandate limiting the Mandate to one or more individual acts.
Information requirement	The information about the characteristics of the eMandate that is necessary to ensure interoperability and cross-border validity to the eMandate.
Legal interoperability	Ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together.
Legal person	Entity constituted under, or governed by, the law of an MS, irrespective of its legal form.
Mandate	Contract under which an entity (Mandatee) undertakes to perform one or more legal acts in the interest of another person (Mandator); the Mandate includes the acts for which it was awarded and those necessary for its completion.
Mandatee	Person who executes an activity in the name of the Mandator; user of the Mandate. Synonyms to this term can be: “proxy”, “assignee”, “agent”, “representative”.
Mandator	Person who needs an activity executed in his name; creator of the Mandate. Synonyms to this term can be: “principal”, “assignor”, “represented”.

Natural person	Entity that is an individual human being who has its own legal personality.
Open-by-default	Enabling reuse, participation/access and transparency.
Organisational interoperability	Ensuring that organisations align their business processes, responsibilities and expectations to achieve commonly agreed and mutually beneficial goals.
Person	A natural or legal person, or a natural person representing a legal person.
Personal Power	The legal capacity, right or privilege to act on behalf of oneself.
Power	The legal capacity, right or privilege to act.
Register	The authority responsible for the information that is registered.
Registry	The system where the information is kept.
Relying party	A Service Provider that requires information to a cross-border eMandates system in order to authorise a user that acts on behalf of another person to access its system.
Representation Power	The power to act on behalf of another person, either natural or legal.
Role	Bundle of one or more authorisations linked to a specific type of entity in a specific context, such as a doctor, lawyer, police officer, nurse, etc.
Semantic interoperability	Ensuring that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties.
Service Provider	An organisation, public or private, that provides an online service, e.g. a Public Administration's online service that requires the electronic identification of the user and, in the case of a person acting on behalf of another person, the information needed for the authorisation to access the service, based on an eMandate.
eMandate Provider System	An organisation, public or private, that allows the reception of requests or the search of Mandates and responds with the delivery of one or more eMandates.

Mandate	The evidence that a person (the Mandator) has given a power to another person (the Mandatee).
Special eMandate	An eMandate limiting the Mandatee's rights to a certain type(s) of act.
Sub-Mandatee	A person that receives by transfer a Mandate from the original Mandatee, and obtains the Power to act on behalf of the Mandator.
Technical interoperability	Covering the applications and infrastructures linking systems and services.
Unilateral Mandate	A Mandate that requires only the approval of the creator of the Mandate, i.e. Mandator.
User-centric-by-default	Principles such as starting with user needs, usability, multi-channel service delivery, provision of the information that is absolutely necessary once only, or having an identified governance and maintenance organisation with a clear single point of contact.
Witness	Person who validates the Mandate hence making it valid and in effect, and who can revoke it if necessary. A Mandate is only valid if it meets all applicable requirements. The witness must be a qualified notary, lawyer, or public officer.

1. EXECUTIVE SUMMARY

In order to instigate and facilitate the cross-border use of electronic Representation Powers and Mandates, the European Commission (**DIGIT, with the support of DG CNECT**), through the ISA² Programme Action 2016.12 “Semantic Interoperability for Representation Powers and Mandates”, seeks to create a **shared European data model for Representation Powers and Mandates**. Creating a **common semantic framework** will ultimately allow Powers and Mandates’ data originating from the information systems of one Member State (MS) to be processed automatically by the information systems in another MS.

Phase 1 of this Action assessed **Member States’ preparedness for cross-border interoperability** of electronic Representation Powers and Mandates. **A shortlist of five services** was identified as priority business cases for cross-border scenarios. Each Member State’s AS-IS situation was analysed and evaluated across the Interoperability Framework’s layers. **Information requirements** were identified, and **ten feasible solutions were listed and ranked** by feasibility criteria. Finally, a **set of twelve recommendations** were issued as next steps towards cross-border and cross-sector interoperability for eMandates.

The scope of the current document is the analysis of the electronic Mandate systems and data models of six selected pioneer Member States: **Austria, Belgium, Finland, The Netherlands, Spain and Portugal**. This desk research seeks to determine which types of Mandates are used; how the Mandates are defined, collected and used to grant access to the public service applications; what types of representations are supported; if there are commonalities and differences between MS regarding both the semantic and legal dimensions; and the needs of MS to facilitate the federation of their information sources, taking into account all the interoperability layers.

This desk research task was conducted through **initial online desk research, an online survey questionnaire sent to MS, and several phone interviews with experts from each MS**.

The conclusions of this report summarise the **commonalities and differences** between the eMandate systems analysed, as well as the **existence of common/harmonised** vocabularies.

2. INTRODUCTION

2.1. ISA² Programme Action 2016.12

In order to instigate and facilitate the cross-border use of electronic Representation Powers and Mandates, the European Commission (**DIGIT, with the support of DG CNECT**), through the ISA² Program Action 2016.12 “Semantic Interoperability for Representation Powers and Mandates”, seeks to create a **shared European data model for Representation Powers and Mandates**. Creating a **common semantic framework** will ultimately allow Powers and Mandates data originating from the information systems of one MS to be processed automatically by the information systems in another MS.

This ISA² Action builds upon and follows the results of the following previous and ongoing European initiatives¹:

- eGovernment Action Plan
- eIDAS
- ISA Action 1.18 “Federated Authorisation across European Public Administration”
- Services Directive
- CEF
- Digital Single Market
- E-SENS
- ISA2 Action 2016.07 “SEMIC”
- ISA2 Action 2016.28 “Access to base registries”
- STORK 2.0.

2.2. Main deliverables and outputs

The first phase of the ISA² 2016.12 Action produced the following deliverables:

- ISA2.D.01.1 “Study about cross-border interoperability of Powers and Mandates”²
- ISA2.D.2.1.a “List of common information requirements of the prioritized services/projects/domains”³
- ISA2.D.2.1.b and D.2.1.d “Ranked long list of solutions”⁴
- ISA2.D.2.1.c “Set of feasibility criteria for solutions which meet the information requirements described in D.2.1.a”⁵

The main outputs of this first phase are described below.

¹ ISA² Action 2016.12 coherence: <http://ec.europa.eu/isa2/dashboard/node/2852/coherence>

² ISA2.D.01.1 “Study about cross-border interoperability of Powers and Mandates”: <https://joinup.ec.europa.eu/document/study-about-cross-border-interoperability-Powers-and-Mandates>

³ ISA2.D.2.1.a “List of common information requirements of the prioritized services/projects/domains”: <https://joinup.ec.europa.eu/document/list-common-information-requirements-prioritized-servicesprojectsdomains>

⁴ ISA2.D.2.1.b and D.2.1.d “Ranked long list of solutions”: https://joinup.ec.europa.eu/sites/default/files/document/2017-11/ISA2-D.2.1.b%20and%20D.2.1.d%20Ranked%20long%20list%20of%20solutions_v1.0.pdf

⁵ ISA2.D.2.1.c “Set of feasibility criteria for solutions which meet the information requirements described in D.2.1.a”: https://joinup.ec.europa.eu/sites/default/files/document/2017-11/ISA2-D.2.1.c%20Set%20of%20feasibility%20criteria_v1.0_0.pdf

Shortlist of Member States to be assessed

First, a list of MS to be assessed was established, depending on their capacity to provide relevant information on electronic Representation Powers and Mandates (RPaM). The 18 shortlisted MS were: Austria, Belgium, Czech Republic, Estonia, Finland, France, Germany, Greece, Italy, Lithuania, Luxembourg, the Netherlands, Norway, Portugal, Slovakia, Slovenia, Spain and Sweden.

Shortlist of prioritised services for cross-border RPaM

Second, a shortlist of five prioritised services where cross-border Representation Powers and Mandates are most needed was established.

The following TO-BE business cases were identified:

- Registering/opening a business cross-border;
- Submitting a tender for public procurement cross-border;
- Managing a bank account cross-border;
- Declaring corporate tax cross-border;
- Accessing a patient summary cross-border.

Assessment of AS-IS situation

Thirdly, the AS-IS situation in each MS was analysed, with regards to the cross-border scenarios for eMandates.

The situation was evaluated using a tailor-made assessment framework inspired by the ISA Interoperability Maturity Model. It assessed the maturity of Member States across the four layers of the European Interoperability Framework (legal, organisational, semantic and technical).

The overall maturity of MS corresponds to the “applied level” (score 3), which is not very mature. Austria, The Netherlands, and Finland were the highest-scored, with respective scores of 4.3, 4.1 and 3.6.

Additional studies were carried out for those three pioneering MS, in order to produce a detailed overview of the eMandate types, uses and information requirements. Similarities between the systems were revealed.

Conceptual models

The five most appropriate services identified were embedded into five different TO-BE business cases. For each business case, a conceptual model of the creation and use of an electronic cross-border Mandate was defined, with corresponding use cases and activity diagrams.

We have summarised the business cases and use cases in the following matrix:

TABLE 1: BUSINESS CASES AND USE CASES MATRIX

	Opening a business	Submitting a tender for public procurement	Opening a bank account	Submitting a corporate tax declaration	Accessing patient summary

Mandate creation	Mandator authentication	x				
	Mandator identity verification	x				
	Mandate storage	x				
Mandate usage	Mandatee authentication	x	x	x	x	x
	Mandate attributes validation	x		x	x	
	Mandates' usage	x	x	x	x	
	Company's certificate retrieval		x			
	Patient attributes validation					x
	Patient summary usage					x

Types of relationships (LN, NN, NL, LL)	NL	NL	NN, NL	NL	NN
---	----	----	--------	----	----

text	Business cases
text	Use cases
text	Specific use case

Information requirements and feasible solutions

Finally, for each of the five prioritised business cases, the information requirements for cross-border service delivery, and the list of solutions that could meet these requirements were identified and ranked by a feasibility criteria.

The ten identified solutions comprised:

- Five European projects:
 - CEF Building Blocks;
 - STORK 2.0. pilot projects;
 - Business Register Interconnection System;

- Core Business Vocabulary;
- Core Person Vocabulary.
- Five MS existing eMandates systems:
 - Austria's Electronic Mandate Service;
 - Belgium's Self-Service Mandate;
 - The Netherlands' eHerkenning;
 - Spain's @Podera;
 - Finland's Katso interface.

Recommendations and next steps

Phase 1 of the ISA² 2016.12 Action also identified a **set of 12 recommendations** that could be considered as **next steps** towards achieving cross-border and cross-sector interoperability for Representation Powers and Mandates. These recommendations include, among others:

- Developing a common vocabulary for Representation of Powers and Mandates by following documented methodologies such as the Methodology for Developing Core Vocabularies;
- Considering existing solutions involving Powers and Mandates processes at national level as references for building cross-border solutions.

2.3. Document scope and objectives

The following report documents the analysis and conclusions on existing electronic Mandate systems in the European Union, within Task Number 01 for Specific Contract N°1993, under framework contract N° DI/07445.

This project is framed within **Action 2016.02 "Semantic Interoperability for Representation Powers and Mandates"** from the **Interoperability Solutions for Public Administrations ISA² Programme**.

This **desk research** aimed at analysing the eMandate systems in selected MS to find out what types of Mandates are used; how the Mandates are defined, collected and used to grant access to the public service applications; what types of representations are supported; if there are commonalities and differences between MS regarding both the semantic and legal dimensions; and the needs of MS to facilitate the federation of their information sources, taking into account all interoperability layers.

This document, presenting the state-of-affairs of eMandate systems in selected MS, is complemented by the document "**RPaM use cases and architecture**", which presents cross-border interoperability experiences and challenges, and provides some recommendations that can serve as inputs for Task 02

The expected work results from the two documents were:

- **Commonalities and differences** among the different Powers and Mandates systems for same legal purposes across borders and sectors;
- A **data model analysis and comparison** from MSS' systems, including a common working terminology;
- A **cartography of existing information sources** for Representation Powers and Mandates in the MS, including their needs for automated federation;

- **List of functional requirements** for the definition of a core vocabulary modelling of the authorisation interactions across borders and sectors.

2.4. Definitions

For the sake of a common understanding and a better comprehension of the content and goals of this project, it is necessary to establish a clear distinction between some of the concepts used or defined in the deliveries.

For definitions of other terms used along the development of the project, please refer to the project glossary deliverable.

Power

“The legal capacity, right or privilege to act on behalf of oneself”.

Example: the power to use services provided by a Public Administration or a private organisation.

(Source ISA², “Representation Powers and Mandates” glossary)

Representation Power

“The power to act on behalf of another Person, either Natural or Legal”.

Example: the power to represent a company when signing a contract.

(Source ISA², “Representation Powers and Mandates” glossary)

Mandate

“The **evidence** that a Person (the Mandator) has given a Power to another Person (the Mandatee)”.

Additional information: the Mandate also describes specificities about the assignment of that Power, e.g. the time limit of the Mandate, financial constraints and other specific restrictions on the empowerment itself.

Example: a hand-written document signed by a notary, the Mandator and one Mandatee where the assignment of the Power is described.

(Source ISA², “Representation Powers and Mandates” glossary)

eDocument

“A set of interrelated information representing the facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual forms that the capability exchanges with other capabilities to support the execution of value streams”.

Examples: an electronic certificate (eCertificate), an eOrder, an eInvoice, an ePower, an eMandate, a deed as a PDF document, an interview with a politician as a WAV file, etc.

(Source ISA², adapted from the definition of “eBusiness Document”).

ePower

“An eDocument that proves that a natural person has the legal capacity, the right or the privilege to access a Service Provider System. ePowers are evidences.. ePowers are evidences”.

Additional information:

- The eDocument contains structured data and references to additional sources of evidences.
- ePowers are machine-readable.
- ePowers aim mostly to allow access to an online service, but could be used for more generic purposes (the statement of a Power in human-to-human transactions or operations).

Example: an eCertificate kept in an eMandate Registry containing the necessary data for a Service Provider to allow a User access to one or more of its systems and use of one or more services.

(Source ISA², “Representation Powers and Mandates” glossary)

eMandate

“An eDocument that proves that a Mandator has assigned its Powers to one or more Mandatees”.

Additional information:

- Possible constraints and details about the Power(s) being assigned and about the Mandate in itself are defined therein.
- The eDocument contains structured data and may contain references to additional sources of evidences.
- eMandates are machine-readable.
- eMandates aim mostly to allow access to an online service, but could be used for more generic purposes (the statement of a Power in human-to-human transactions or operations).

Example: an eMandate kept in an eMandate Registry containing the assignment of Powers necessary for a Service Provider to allow a Mandatee access to one or more of its systems and use of one or more services.

(Source ISA², “Representation Powers and Mandates” glossary)

Register

“The authority responsible for the information that is registered.”

Example: the Directorate General of Registries in the Ministry of Public Administrations.

Registry

“The system where the information is kept.”

Example: the eMandate Registry @podera in Spain.

Additional Information:

The organisation responsible for the information kept in the Registry (the Register) may not be the same organisation as the one that manages the Registry.

2.5. Methodology

Choice of case studies

The scope of the current document is the **analysis of the electronic Mandate systems and data models of six selected MS:**

- Austria
- Belgium
- Finland
- The Netherlands
- Spain
- Portugal.

The choice of these MS was made according to the results of Phase 1 as well as the results of an online questionnaire that was sent to the MS.

In the first phase of the Action, the assessment **framework scored Austria, Finland and The Netherlands with the highest interoperability scores**, out of 14 MS. Those three MS and their eMandate systems were also part of the **final list of ten solutions proposed as feasible solutions that meet the information requirements for cross-border interoperability**. For this reason, Austria, Finland and The Netherlands are part of this desk research.

In addition, this list of feasible solutions contains the Belgian (SSM), Spanish (@Podera) and Portuguese (SCAP) systems. The **detailed answers to the online questionnaire** confirmed that Spain and Portugal could be interesting case studies.

It is worth noting that, while the feasible solution identified in Phase 1 for Finland was the Katso interface, our desk research revealed that Suomi.fi e-authorisation was a more complete and mature system.

Information researched

The deliverables from Phase 1 of this Action disclosed important findings that formed the basis for this desk research; for example, the description of the system and data model attributes for the three pioneer MS: Austria, The Netherlands and Finland.

The business cases and use cases developed in Phase 1 were conceptual models, developed within the framework of a theoretical situation of cross-border service and cross-border electronic Mandate.

This desk research complements Phase 1 by analysing in detail **the state-of-affairs of existing eMandate systems in the selected pioneer MS**, investigating its different components in order to identify commonalities and differences that could constitute opportunities or constraints for a cross-border exchange of information.

All the information found was checked against the deliverables of Phase 1, and more specifically against the **information requirements** identified.

Methods

The desk research task was conducted through:

- Initial online desk research;
- An online survey questionnaire sent to MS;
- Phone interviews with experts from each MS.

During the initial **online desk research**, a substantial number of documents was analysed. The first documents were the **deliverables from the first phase** of the ISA² Action project as well as the additional documents referenced there, including the **STORK 2.0 deliverables**. Other sources of information included European and national eGovernment documents and projects, as well as academic research.

In parallel to this online desk research, **an online survey** was sent to MS through the European Commission website. The goal of the questionnaire was to obtain relevant information as well as to identify relevant case studies that were not initially spotted. The questions were based on existing questionnaires used in Phase 1 of the Action and were enriched so that the detailed scope of the current task would be addressed. The survey was published on the **EU Survey website**. It was **launched on 16 May and remained open until 15 June**. Four MS answered the online survey: **Austria, Spain, Portugal and the Czech Republic**.

The scarcity of information found online and through the online questionnaire made further research necessary. In order to complement the information obtained, **six 90-minute phone interviews were arranged** with experts and groups of experts identified in each MS. The experts identified were, in most cases, directly in charge of the eMandate system in the MS, and some of them were participants of past or current European pilot projects such as STORK, eIDAS or TOOP. The phone interview aimed at validating first observations, acquire missing information, and above all, obtaining key documents and direct URL links; for example, to the data models or legal instruments.

2.6. Structure of the report

The information offered in this study is organised as follows:

Chapter 1 is the executive summary of this report.

Chapter 2 is the introduction to the report.

Chapter 3 is a state-of-affairs on electronic Mandate systems in the six MS.

- Section 3.1 describes in general terms the different eMandate systems in each MS;
- Section 3.2 analyses for which public services and business cases the eMandates are used in each MS;
- Section 3.3 analyses which type of representations are supported by each eMandate system in each MS;
- Section 3.4 describes who issues the eMandates and where the end-user can manage his/her Mandates in each MS;
- Section 3.5 is a cartography of the authentic source registries where the identity data is retrieved by the eMandate systems;
- Section 3.6 details where the eMandates are stored and how they are digitally preserved;
- Section 3.7 analyses whether a MS has developed national vocabularies or specifications for eMandates;
- Section 3.8 analyses what laws impact, directly or indirectly, the eMandate system in each MS.

The conclusion of the report gives an overview of the findings.

The Annexes display the lists of public services, business cases and uses cases where eMandates are available for each MS, as well as the complete answers from the four MS to the online survey that was sent at the beginning of this desk research.

3. STATE-OF-AFFAIRS ON EMANDATE SYSTEMS IN SIX MEMBER STATES

3.1. What eMandate system(s) exist in the analysed MS?

Austria

The Austrian Electronic Mandate Service (EMS) is a system hosted by the **Austrian Source PIN Register Authority**, which is hosted by the **Austrian Data Protection Authority**.



FIGURE 1: THE AUSTRIAN WEB-SERVICE FOR ELECTRONIC MANDATES⁶

This eMandate service is fully integrated into the Austrian eID system, which is technically realised through the **Austrian Citizen Card** (smartcard or mobile phone signature). The Citizen Card provides **electronic identification** with a unique identification and maximum privacy, as well as **qualified electronic signatures** aligned with the requirements of the Austrian Signature and Trust Services Law and the EU eIDAS Regulation.

Currently, the Austrian eID system is **not notified under the eIDAS**, but it is foreseen that the notification will be completed in 2019.

Thanks to the EMS, Austrian individuals can authorise a Mandatee to act on their behalf through **an electronic Mandate agreement that is saved in a Mandate register operated by the Source PIN Register Authority**.

EMS is available for both Natural Persons and Legal Persons.

“Statutory representation” (natural person acting as the legal representative of a company) is derived from authoritative sources (e.g. Register of Company Names, Register of Associations, Supplementary Register). It is also possible to authorise official representatives from the municipality or district authority to fill out electronic application forms on behalf of another person.

The electronic Mandates in Austria are **issued and signed by the SourcePIN Register Authority**.

⁶ <https://mms.stammzahlenregister.gv.at/mms/moaid.do>

Belgium

In Belgium, **two different eMandate** systems currently co-exist: one developed by the **Federal Public Service Finances (FPS Finances)**, and the other one by the **National Social Security Office (NSSO)**. A third system has been developed by the **Flemish Region**.

Self-Service Mandate (finances system)

The **Self-Service Mandate (SSM) system** originates from **FPS Finances**, the department of finances of the federal government. This system was initially made for **personal income tax declarations**, but is now extending its scope through the **CSAM platform (Common Secure Access Management)** towards healthcare services (eHealth). SSM is also being assessed by **Social Security services** and the **Flemish Region** to determine whether synergies exist.

In the SSM system, users can be identified and authenticated by using **different types of eID**: in most cases the national eID system, but also by identification based on a bank account and/or a token. Currently, the Belgian eID system is preparing for **eIDAS regulation and infrastructure**.

MAHIS (Social Security system)

The **MAHIS system** originates from the **National Social Security Office** of Belgium. This system is made for **employers (Mandator)** and their **payroll professionals (Mandate receiver)**. The system produces an **“e-procuration” as an electronic document in a PDF format** that must be signed by both parties. A validated Mandate allows a payroll professional to perform (social) administrative obligations on behalf of the employer.

PROCURATION

Données de l'employeur

Numero d'entreprise : 052.093.431 Numero ONSS : 1277926-67
Dénomination : MARTI GUTIERREZ, ALEXANDRA
Rue : KERKELARENGAARD 6 Numero : - Boite : -
Code postal : 7800 Commune : CDINGEN Pays : Belgique

Données du prestataire de services

N° d'agrément du SSA : 999
N° de la succursale où le dossier est tenu à jour : 999
N° d'affiliation de l'employeur auprès du SSA : -
N° d'entreprise : 052.093.431
Dénomination : TEST ESSA
Rue : AVENUE FONSNY Numero : 20 Boite : -
Code postal : 1060 Commune : ST-GILLES Pays : Belgique
Tél : 02787541 e-Mail : gregory.cassiers@ensml.be

A. Donne le mandat au prestataire de services ou secrétariat social agréé précité, qui l'accepte, d'exécuter en son nom et pour son compte les formalités en matière de sécurité sociale.

Le mandat porte spécifiquement sur le ou les group(es) suivant(s) (1) :

Sécurité sociale Reques sociales Autres

Droits - Dimens Droits-Chômage Sigets (D&P - Employeur)

Services Internationaux Droits Accidents du travail

Chômage temporaire

Trimestre d'affiliation : 3/2018 (TIAAAA)

B. Confirme également que le mandataire précédent (si d'application) a été révisé correctement.

C. Fait mention de domicile au siège du secrétariat social agréé pour la réception de la correspondance et des communications émanant de l'Office afin que ce dernier puisse adresser valablement tous les documents au secrétariat social.

D. Le mandat prend cours le 1er jour du trimestre d'affiliation susmentionné.

* informations au verso

REMARQUES IMPORTANTES :

(1) Le fait de cocher un ou plusieurs groupes d'applications implique que le prestataire de services est accès au réseau électronique de la sécurité sociale ainsi qu'à l'infrastructure de base et aux logiciels nécessaires pour pouvoir gérer ses obligations de l'employeur.

FIGURE 2: EXAMPLE OF AN NSSO E-PROCURATION DOCUMENT⁷

Both **SSM** and **MAHIS** are **“Mandate managing” systems** that are limited to the creation and modification of Mandates. For this reason, they are **closely linked to a number of other applications** that allow the management of identification and authentication processes, user access processes, and role administration processes (see section Belgium 01 for further details).

⁷ PDF shared during the Belgium MAHIS interview

Gulf of Finland as convenient as possible. Institutions expecting to begin exchanging data include health insurance funds, tax and custom boards, traffic registers and population registers.

The Netherlands

In the Netherlands, citizens and businesses can manage Mandates and Powers of Representation digitally. Citizens may do so by using the DigiD platform, while businesses and organisations can use the eRecognition platform. Once created, the Representation Powers can be used in all public administration online services.

DigiD stands for Digital identity. With a DigiD, residents and Dutch citizens living abroad can log into government and healthcare websites. In addition to this eID feature, DigiD facilitates the representation of citizens by other citizens through the DigiD Machtigen ('DigiD Authorise') online facility, where it is possible to authorise a third person to access online services provided by the government. Within the DigiD Authorise facility, the user can create and revoke Representation Powers, assign them to one or multiple Mandatees, and choose the particular type of Representation Power to be utilised. In 2017, there were more than 2.5 million active authorisations.

eHerkenning (eRecognition) is an electronic application functioning as an electronic identification and recognition 'gate', allowing users to access and use different services with just one single user eID and password. The basic features of eRecognition are as follows:

- Identifying and authenticating a company that is conducting business.
- Requesting and using an authentication token.
- Registering an authorisation and consulting it in an authorisation register (authorisation).
- Connecting to and purchasing a service.
- Requesting so-called self-declared attributes that the user provides. Data can only be given to the service provider whose web service has been logged into with the explicit consent of the involved party.

eRecognition is already used in business, government and consumer sectors. The main groups of users are:

- Users in the public sector: They are (employees of) government service providers who receive and process applications submitted by the representatives of businesses and other legal entities.
- Users in the business sector: They are legal (or appointed) representatives of a business. Their authorisation levels correspond to their positions and activities. These authorisation levels are registered.

For eRecognition, there are five companies ("brokers") delivering the eMandate scheme¹⁰. The government authority qualifying these companies is the Ministry of Economic Affairs and Climate Policy. These private companies authenticate a company and its representatives, creating an eRecognition account and storing the company's eMandates.

It is worth noting that in **the Netherlands**, the **Dutch Agriculture portal**¹¹ enables Belgian farmers (legal persons) to use hundreds of online services with the same rights and obligations

¹⁰ <https://www.eherkenning.nl/aansluiten-op-eherkenning/aansluiten/>

¹¹ www.DRIloket.nl (operated by the National Service for the Implementations of Regulations)

as Dutch entrepreneurs, including application for subsidies, export permits and registration of cows and other animals. However, in order to do so, Belgian farmers still need to register as LP by using the national Dutch eID system.

Portugal

On 30 May 2018, Portugal pre-notified three eID schemes to the European Commission:

- The national eID card (Cartão de Cidadão - CC)
- The mobile eID solution (Chave Móvel Digital - CMD)
- The **Professional Attributes Certification System (Sistema de Certificação de Atributos Profissionais - SCAP)**.

The SCAP system is one of the two Representation Powers systems available in Portugal, the other one being the **Procurações Online**¹² system.

The Cartão do Cidadão is a smartcard-based eID combining four identification numbers (i.e. fiscal, social, health and civil ID), replacing five other paper-based ID cards. It is compulsory for all Portuguese citizens from the age of 20 days.

A complementary authentication option was introduced with the mobile-ID solution Chave Móvel Digital (Digital Mobile Key). It is available to Portuguese and foreign nationals aged 16 years or older. Activation of the CMD consists of a security code received by SMS or by email, which is combined with a mobile phone number or email address and a PIN code. The system requires users to previously identify themselves at a government agency, with a valid ID.

The third scheme - SCAP - serves to authenticate the functions that **the owner (natural person) of a Portuguese national eID card (CC) or mobile eID (CMD) performs in society as a qualified professional, and/or the powers and capacities in the context of a public/private company.** The SCAP will allow the user, through the citizen's card or the digital mobile key, **to authenticate or sign electronically, allowing him/her to prove the position s/he holds in a particular commercial entity, without having to provide any other evidence.**

It is important to underline that SCAP is understood as an electronic identification scheme.

Spain

@Podera REA (*Registro Electronico de Apoderamientos*) is a system that was established by law and entered into operation in 2012 in Spain. It allows the creation and management of electronic Powers and Mandates, so that persons (citizens, businesses or public administration officers) can act on behalf of others in the state government's online services (*Administración General del Estado*) and other public administrations' online services at regional and local level. It is managed by the *Ministerio de Hacienda y Función Pública*.

REA is composed of two applications: the **REA for administrative Mandates** (those made to interact with public administrations) and the **REA-J for judicial Mandates** (those made for lawyers and prosecutors to act in the judicial domain). A third system was developed and is managed by the notaries, for **notarial Mandates**.

¹² <http://www.procuracoesonline.mj.pt/ProcuracoesOnline/>

For the administrative Mandates, other eMandate systems exist in addition to the central REA. The three systems (administrative, judicial and notarial) were developed respectively by **the Department of Traffic, Social Security and the Tax Agency**. If a citizen wants to create an eMandate for Social Security, s/he can either do it through the central REA or through the Social Security eMandate system.

The law does not require merging the different eMandate systems, but it does require that all systems be interoperable and interconnected. For example, the REA DGT system (Department of Traffic) can consult the central REA system, but this central system does not need to consult REA DGT, as it also encompasses eMandates related to traffic.

In addition, the law does not require any organisation other than the state government to use the central REA. **Any public administration at regional or local level can develop its own eMandate system, as long as it is interoperable and interconnected to the others.**

Comparative analysis: commonalities and differences

Some MS, such as Austria and Finland, have a unique and centralised eMandate system. Others have several eMandate systems that were historically developed by different actors, as it is the case for Belgium where FPS Finances, the National Social Security Office and the Flemish Region each developed their own system. In the case of Spain, the different systems developed are totally interoperable and interconnected by law, so that a natural or legal person can use any of the systems equally.

In most of the MS, the eMandate system was developed and is managed by the public sector. Nevertheless, some MS such as the Netherlands have developed eMandate systems that rely exclusively on private partners as “eMandate system managers”. In such cases, each private partner manages its own eMandate system, in competition with the other existing systems.

Most of the MS have integrated their eMandate system into the national eID system. This allows users to access the whole range of online public services through their eID and multiple supports/devices (eID card, mobile, digital certificates), and to use eMandate whenever they need it, for any eGovernment application.

In MS with several eMandate systems, the eMandate systems can be specific, either to a sector/service/application as in the case of Belgium, or to a type of person (natural or legal), as in the case of the Netherlands. In Portugal, the SCAP system is specifically designed for professional representation use cases (lawyers, attorneys, CEOs, public officers, etc.).

Most of the sector-specific eMandate systems are now looking at how to expand their scope towards other sectors/services/applications and how to find synergies and interconnection with other systems. The experts recognise that there is a need to federate the different systems amongst themselves and present one single interface to the user.

TABLE 2: COMPARATIVE ANALYSIS OF THE eMANDATE SYSTEM(S)

	AT	BE		FI	NL		SP	PT
	EMS	SSM	MAHIS	E SUOMI	DigiID	eHerkenn ing	@Podera	SCAP
Unique centralised system of eMandates	YES	NO	NO	YES	NO	NO	NO	YES
Same eMandate system for NP and LP	YES	NO	NO	YES	NO	NO	YES	YES

eMandate system integrated with the eID system								
	YES	YES	YES	YES	YES	YES	YES	YES
eMandate system available for all public services								
	YES	NO	NO	YES	YES	YES	YES	YES
eMandate system managed by the private sector								
	NO	NO	NO	NO	NO	YES	NO	NO

3.2. For which sectors, public service applications, business cases and use cases are eMandates available?

In some of the analysed MS, the number of public services and business cases related to the use of eMandates can be very large, specifically when the eMandate system is integrated with the eID system. In order to maintain the conciseness of the present report, the long lists of public services, business cases and/or use cases related to the eMandate systems that we were able to find are displayed in Annexes I, II and III. The sections below only present a general overview of where and when the eMandates can be used.

Austria

The electronic Mandates in Austria **can be used on every public service online application** which uses the Austrian eID solution. For this reason, it is very difficult to obtain an exhaustive list of service providers and service applications that support eMandates.

Nevertheless, a “**list of Mandate profiles**” published on the Austrian eMandate services describe the different generic and pre-defined types of Mandates¹³.

- The section "*Unterstützte Profilgruppen*" contains predefined sets of single Mandate profiles;
- Mandate profiles for natural or legal persons are listed in section "*Unterstützte Einzelprofile*":
 - The profile "GeneralvollmachtBilateral" is the generic Mandate profile for natural persons that allows a Mandatee to use any type of eGovernment service.
 - The profile "Einzelvertretungsbefugnis" is the generic Mandate profile that allows a single natural person who is a Mandatee to represent a legal person on any type of eGovernment service.
- Mandate profiles for public servants are listed in section "*Unterstützte Profile für Organwalter und berufsmäßige Parteienvertreter*" (for professional representation by notary, lawyers and certain types of civil engineers, or by officials authorised to represent citizens).

The sector-specific or service-specific pre-defined Mandates are:

- Access to e-Health Records;
- Applications for the Data Protection Authority;
- Services of the Chamber of Commerce.

¹³ <https://vollmachten.stammzahlenregister.gv.at/mis/>

Mandates can range from universal rights to arbitrary limitations. Some of the pre-defined Mandates have implicit constraints. For example, an e-Health Record Mandate can only be used on the e-Health application, or a statutory representative assumes universal rights unless specifically constrained. In addition, “bilateral Mandates” can be established with arbitrary content.

Currently, the use of eMandates is limited to public sector bodies. An amendment of the legal basis in 2017 extends the use to the private sector, and its implementation is ongoing – eMandates are now available for some **private service applications related to electronic delivery** - but this has not yet been completed.

Belgium

In Belgium, eMandates are **limited to the public sector, and are application-specific**. In other words, there are no general purpose eMandates which are open for use by any interested third party.

SSM (finances system)

SSM was initially developed by **FPS Finances** for tax declarations. Its use is theoretically open to all public services, but at this time it is principally used by FPS Finances and by the federal **e-Health Platform**. Other partners such as **the Flemish Government** and **FPS Pensions** are preparing to begin use of the system.

In the **finances** domain, SSM allows a Mandate holder, usually an accountant, to submit a tax declaration via the online taxation services¹⁴.

In the **eHealth** domain, the Mandate holder (individuals, enterprises, care institutions) can access an application that aims to provide healthcare support (invoicing third-party payment, global medical file, insurability, etc.). With a similar logic to that of a company representation, care institutions must designate a Chief Access Manager who can allocate roles within his/her organisation¹⁵. Citizens themselves (patients) can manage Mandates through the eHealth platform via the applications PatientConsent¹⁶ (providing or withdrawing consent for specific healthcare providers to access the healthcare record of the patient) and eHealthconsent¹⁷ (granting authorisation to any healthcare provider to access the healthcare record of the patient).

In terms of use cases, SSM is a Mandate managing system that is **limited to the creation and modification of Mandates**. For this reason, it is closely linked to a number of other applications related to **identification and authentication, user access management and role administration**. Those applications are developed at a higher level than SSM, for all government services, and constitute **the CSAM platform**.

¹⁴ <https://finances.belgium.be/fr/E-services/Mandats/FAQ#q7>

¹⁵ <https://www.ehealth.fgov.be/nl/egezondheid/hoekrijgtu-toegang-tot-het-portaal-egezondheid-gebruikers-en-toegangsbeheer>

¹⁶ <https://www.ehealth.fgov.be/nl/egezondheid/patienten/ehealthconsent>

¹⁷ <https://www.ehealth.fgov.be/nl/egezondheid/patienten/patientconsent>

CSAM¹⁸ is the central system for identification and authentication processes in the public sector. It is managed by a group formed by the principal federal services that rely on it (Social Security, Finances, Crossroad Bank of Social Security, Economy, Internal Affairs, and Policy/Support). Login for CSAM relies on the **FAS (Federal Authentication Service)¹⁹**.

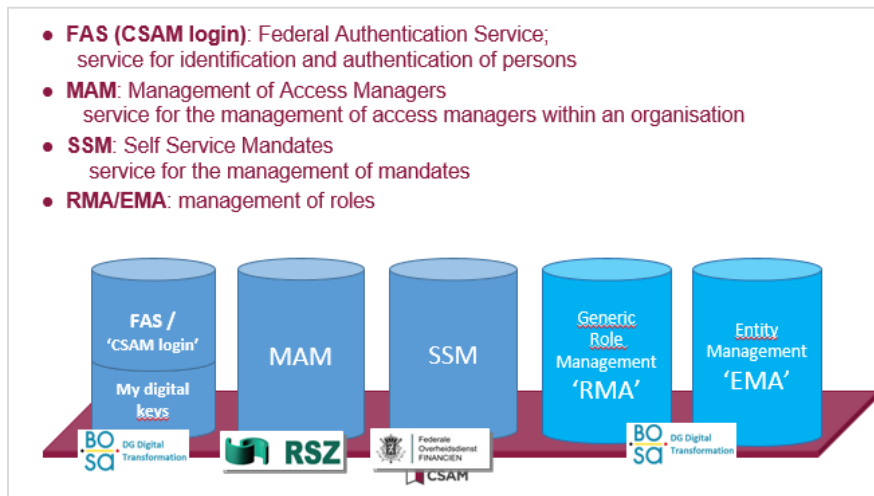


FIGURE 4: CSAM SERVICE OFFERING (CURRENT AND PLANNED)²⁰

The application **MAM (Management of Access Managers)²¹** was established in order to manage the characteristics of the users, including their profiles and authorisations. MAM relies on Policy Information Points (PIPs), i.e. an **authentic source database** that contains information on a person’s authorisations. One of the main PIPs is PI User Management Enterprises, which is located with the Crossroad Bank of Social Security, and **allows companies to designate a Chief Access Manager, who can thereby designate additional roles in a company** as needed for the purposes of social security applications. This mechanism therefore allows for the designation of representatives of legal entities at an application-specific level.

¹⁸ <https://www.csam.be/en/index.html>

¹⁹ https://dt.bosa.be/en/identificatie_beveiliging/federal_authentication_service

²⁰ Power Point shared during the Belgium SSM interview

²¹ <https://www.csam.be/en/management-access-managers.html>

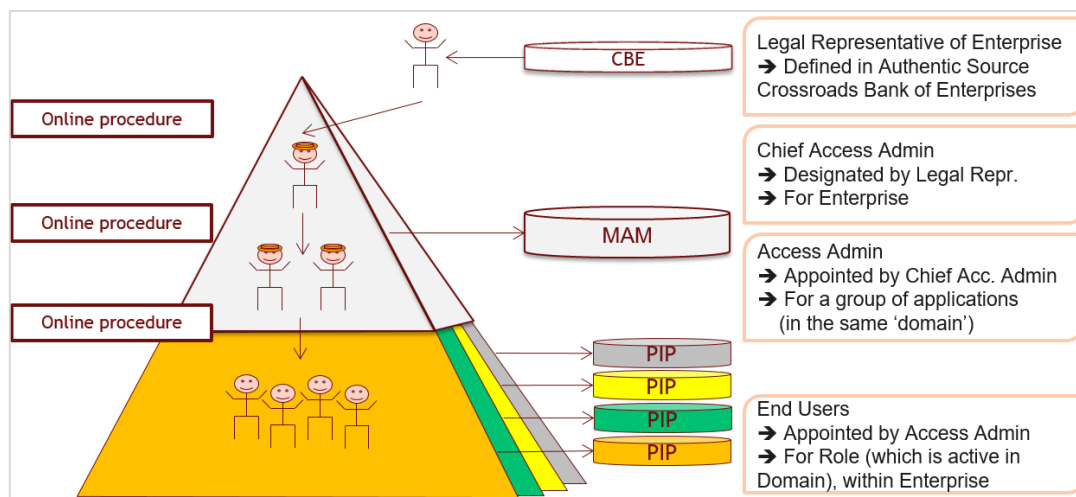


FIGURE 5: MANAGEMENT OF ACCESS MANAGERS²²

Finally, roles can be defined in this system via the application “My eGov Role Management”²³, operated by the federal public service Policy/Support (BOSA). This **separate role management system** allows businesses, public officials, and self-employed persons to allocate and manage roles that provide access to online government applications. This service is used by the eMandate application SSM as well as many other public or private e-services, in order to ensure correct role assignment as a part of the access management process.

The SSM eMandate system is closely linked to all the different applications mentioned above.

MAHIS (social security system)

MAHIS was initially created by the federal Social Security service and was meant to be exclusively used by its services. Through MAHIS, **employers can give an “e-procurement Mandate” to a service provider** to manage social security administration²⁴. It is only available for LP and only covers LL representations.

With MAHIS, a company can give a payroll professional (service provider) the permission (Mandate) to perform specific types of social security administration procedures on his/her behalf. Some examples include registering a company as an employer with the NSSO, or sending in declarations containing employer-employee relations, the salaries of employees and other data on the basis of which social contributions are calculated. When properly mandated, a service provider can also send in declarations that contain information regarding “social risks” that may give the right to benefits for an employee (unemployment, workplace accidents, etc.).

In MAHIS, Mandates are always created for a cluster of applications. A company can – to a certain extent – give permissions to different service providers for different sets of digital social security services. Each cluster can only be mandated to one service provider.

²² Power Point shared during the Belgium SSM interview.

²³ <https://iamapps.belgium.be/rma/generalinfo?redirectUrl=%2Frma>

²⁴ https://www.socialsecurity.be/site_fr/employer/applics/mahis/index.htm

Although MAHIS was specifically designed for social security needs, its usage was – in the spirit of reuse of existing applications/solutions – recently extended to other public sectors. One example is the Mandate for sending information concerning the mobility (commuting, etc.) of its employees to the federal institution of mobility. In the near future, MAHIS will also be opened up for specific regional²⁵ Mandates, by which a service provider can apply for (regional) employment incentives for and on behalf of the company/employer.

Finland

The Suomi.fi e-Authorisations can be used for both public service applications and private applications. Within the public domain, the Suomi.fi e-Authorisations can be used in all government domains and an eMandate can be created, managed and revoked entirely online.

At the moment, all Mandates apply to a **theme** instead of an organisation, a category or a specific, single transaction instance.

A list of business cases is available in Annex II.

Two examples of business cases are:

- **Preparation, planning and development of business activities:** With this Mandate, the Mandatee can manage the information needed in the preparation, planning and development of business activities on behalf of the Mandator.
- **Managing matters related to healthcare:** This Mandate gives the Mandatee the authority to act on behalf of the Mandator in healthcare services. The Mandatee may:
 - View information regarding the Mandator's state of health;
 - Make and change healthcare appointments;
 - Submit and receive information on the Mandator's state of health.

The Suomi.fi e-Authorisations can be used also in the private domain; for example, in the cases of the private companies United Medix Laboratories²⁶ and SuoraTyö²⁷ (a company focusing on recruiting, salary payment etc.).

The Netherlands

The electronic Mandates can be used for every public service online application. For this reason, it is very difficult to obtain a full list of service providers and service applications which support eMandates.

With DigiD, Natural Persons can interact with any Public Administration. 20 municipalities use DigiD, and five large agencies delivering public services are completely based on DigiD as an eID.

With eRecognition, Legal Persons can interact with the government – but they cannot open a bank account, for instance. Nearly all municipalities are connected to eRecognition, as well as the largest agencies such as Tax, Social Security, Netherlands Enterprise Agency, Water Boards (Dutch regional government bodies), etc.

²⁵ Currently the Flemish regional government.

²⁶ http://www.yml.fi/index.php?set_lang=en

²⁷ <https://www.suoratyo.fi/>

The general Mandate provided by both DigiD and eRecognition is partly service-based, and partly “portal-based” (a portal being the equivalent of a group of services).

For example, since eRecognition is provided by private companies, both public administrations (service providers) and users have to pay for creating Mandates. This is why the Netherlands Enterprise Agency Agricultural Portal, which delivers 120 services, decided to define just one Mandate that works for the whole portal and all of its 120 services.

But the Netherlands Enterprise Agency Agricultural Portal is also managing an alternative Mandate system that is highly advanced. Unlike eRecognition, which works for the entire portal, this Mandate system can be used for each service individually, and it can also be used for a specific process step of a specific service. There is a high degree of granularity in this Mandate system. To date, between 20,000 and 30,000 Legal Person to Legal Person Mandate instances are stored in this specific system.

The use cases in DigiD Authorise are:

- Mandator authentication;
- Mandate revocation;
- The Mandator receives an authorisation code in the Mandate creation process. The authorisation code together with the civil service number (BSN) must be handed over to the Mandatee. Using his/her own DigiD, together with the authorisation code received, the Mandatee is able to log on to the account of the Mandator and handle the specific service;
- The authorisation code has to be activated (in fact accepted) by the Mandatee by logging on to the DigiD Authorise portal.

Portugal

Becoming a member in the SCAP system can be done with the Citizen Card or the Digital Mobile Key. The system has two modalities.

First, the SCAP system is used for **professional attributes**. The system allows the citizen **to authenticate** with the portals and websites of different public entities and **to sign documents in the quality of a professional**. **Public officials** can become members of SCAP²⁸, and the certification of public attributes remains valid as long as the public bond or position held is maintained.

Second, the SCAP system is used for **business attributes**. The system allows **certification of qualities and powers of a citizen as the representative of a company**; for example, as administrator, manager, director, attorney or public prosecutor.

- **For administrators, managers or directors** as representatives of a company: this certification lasts for two years; the first certification request is free and the following ones have a cost of 40 euros.
- **For attorneys and public prosecutors** as representatives of a company: this certification must be done with an electronic power of attorney, which must be registered in the other eMandate system (**Procurações Online**) and costs 40 euros.

²⁸ In accordance with the provisions of the legislation (article 10 of Decree-Law no. 83/2016)

The system can be used by administrators, managers and directors of corporations, limited liability companies or cooperatives for signatures; namely:

- Contract work;
- Procedures associated with the formation and execution of public contracts;
- Current management contracts, namely contracts with suppliers of electricity, water, gas and telecommunications services;
- Contracts with other suppliers.

Once the signature has probative value, it is possible to sign contracts at a distance without the need for travel by the corporate bodies of the companies, or their representatives, thereby avoiding the costs and time spent on these steps.

The administrators, managers, directors and attorneys of the companies and cooperatives may join the SCAP system with the Citizen Card and / or Digital Mobile Key for later authentication and signature, as representatives of the company.

The signature may be used in the following acts:

- Contracts with entities providing electricity, water, gas and telecommunications services;
- Contracts with other suppliers, with the limit to be set by the corporate bodies;
- Employment contracts;
- Training and execution of public contracts in the context of public procurement;
- Presentation and execution of applications for financing with the limit to be set by the governing bodies;
- Submission and execution of applications for national or community funds;
- Opening and moving of bank accounts;
- Minutes and resolutions of the corporate bodies;
- Reception and collection of postal correspondence.

Spain

Spain classifies its Mandates in three types:

- **Administrative eMandates:** for any interaction with public administrations at all three levels (national, regional and local), regulated by Law 39/2015 (article 6)²⁹, Royal Decree 668/2015 (art.15)³⁰, Ministerial order HAP/1637/2012³¹;
- **Judicial eMandates:** for any act of lawyers and prosecutors in judicial procedures, regulated by Law 18/2011 (article 32bis)³²;
- **Notarial eMandates:** for acts of notaries, including interactions with public administrations, regulated by the Civil Code³³.

The **Administrative eMandates** can themselves be classified into three sub-types, defined in the Law:

²⁹ <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a6>

³⁰ <https://www.boe.es/buscar/doc.php?id=BOE-A-2015-8048>

³¹ <https://boe.es/buscar/act.php?id=BOE-A-2017-7719>

³² <http://www.boe.es/buscar/act.php?id=BOE-A-2011-11605&p=20151006&tn=1#a32bis>

³³ <https://boe.es/buscar/act.php?id=BOE-A-1889-4763&p=20170629&tn=1#tix-2>

- **Type A: General Power** for the Mandatee to act on behalf of the Mandator in any administrative act (“procedimiento”) and before any of the public administrations at all three levels;
- **Type B: Power** for the Mandatee to act on behalf of the Mandator for any administrative act in one specific public administration or organisation;
- **Type C: Power** for the Mandatee to act on behalf of the Mandator for one or several specific procedures specified in the eMandate, before one specific public administration.

The public administrations are classified in the following way:

- “Administración General del Estado” (state government)
- “Comunidades Autónomas” (regional government)
- “Entidades Locales” (local government)
- Public bodies
- Other institutions.

Although there is no exhaustive list of public service applications and business cases for eMandates, **each public administration is codified in the DIR3 list, and each procedure is also codified in the SIA list.** Those inventories give a good overview of the possibilities provided by the eMandates that are valid for any of the public administrations and procedures listed. The Mandates also provide for cases in those inventories where procedures are not yet listed.

There is no case of REA Mandates being used by/for the private sector.

The **process is fully digital** for natural and legal persons. In the case of legal persons, the Mandatee encloses the statutes of the Mandator and makes a responsible declaration.

The citizen can either create the Mandate him/herself online, or go to a public servant who will do it for him/her.

Comparative analysis: commonalities and differences

The diversity of the public service applications making use of the eMandate system varies a lot from one MS to another. In some MS, such as Austria or Finland, the eMandates can be used for every eGovernment application. For other MS, such as Belgium, the eMandate system is very specific to one public service application, although efforts are being made to extend the scope to other sectors.

Most MS have extended the scope of eMandate systems to the regional and local governments, as is the case in Finland, Spain and the Netherlands.

Although all eMandate systems were initially developed by and for the public sector, some of them are now extending to private services, as with Austria for electronic delivery services. Finland also offers this option.

Some of the systems were initially developed at central level with the long-term objective to expand their scope to all public services, and others were created according to needs in a very specific sector; for example, the MAHIS social security system in Belgium. In Spain, although systems existed at the sector level, the law created a central system and requires all existing and future systems to be interoperable and interconnected.

Each system supports a number of use case that varies widely from one MS to another. Most of the processes are fully digital. In most MS, one online platform allows management of all steps of a process, from identification to creation and use of the Mandate. In Belgium, on the contrary,

at least four different applications are necessary for identification and authentication, access management, role management, Mandate creation and use.

TABLE 3: COMPARATIVE ANALYSIS OF eMANDATES AVAILABILITY

	AT	BE		FI	NL		ES	PT
	EMS	SSM	MAHIS	E SUOMI	DigiD	eHerkennin g	@Podera	SCAP
	System developed and managed by the public sector							
	YES	YES	YES	YES	YES	NO	YES	YES
	System developed to cover all public services applications							
	YES	NO	NO	YES	YES	YES	YES	YES
	System used at national, regional and local level							
		NO	NO	YES	YES	YES	YES	YES
	System gradually extended to private services							
	YES	NO	NO	YES	NO	YES	NO	NO
	Online system covers the complete life-cycle of the eMandate							
	YES	NO	NO	YES	YES	YES ³⁴	YES	NO

3.3. What types of representations are covered by the eMandate system?

Note: The annotation “NL” means a Natural Person that represents a Legal Person (and not that an NP gives a Mandate to an LP).

The four possible types of representations for a “**contractual representation**” are:

- **Natural Person representing a Natural Person (NN):** for example, when a citizen acts on behalf of their senior parent to manage matters related to healthcare.
- **Natural Person representing a Legal Person (NL):** for example, a high-ranking employee that signs public contracts in representation of his/her company.
- **Legal Person representing a Natural Person (LN):** for example, a wealth management company mandated by a citizen to manage its tax and property affairs.
- **Legal Person representing a Legal Person (LL):** for example, a Human Resources company contracted to seek employees on behalf of another company.

In addition to these types of representation, some MS further categorise the following specificities:

- **“Legislative representation”:** when the law automatically grants a person the Power of Representation for another person; for example, parents for their underage children.
- **“Statutory representation”:** when a person in reason of his/her profession is automatically able to represent another person. For example, lawyers for their clients, or doctors for their patients. The case of statutory representation of a legal person by its CEO is a mixed situation, since the Mandate is partially statutory, and partially defined by corporate law, or the company’s own statutes.
- **“Delegation of Power” or “chained Mandates”:** for example, when the legal representative of a company delegates his/her Power of Representation to his/her own employees, who themselves can sub-delegate the Power so that another staff member

³⁴ The legal representative of the company must send a copy of the company certificate to the eRecognition service provider to prove his/her Power of Representation.

can perform the final act. This delegation or transfer can be done internally within the company, but can also be done with another Legal Person such as a law firm or accounting firm.

Austria

In Austria, eMandates can be used by both NP and LP. The system supports NN and LN relationships.

An example of an NN relationship is the Electronic Health Record “ELGA” that allows mandating other NP, such as relatives, to access the service.

Examples of NL relationships are the statutory representation of a company as a CEO, or the company delegating access to the electronic delivery service to a staff member.

According to Austrian law, an NP must be behind an LP. Therefore, an LL relationship is possible only where an NP represents an LP. Still, the LP represented by the NP can delegate rights to another LP.

Belgium

SSM (finances system)

SSM was initially made for LP, but it is now available for both NP and LP.

All four types of representations are supported, although LL and LN are the most commonly used. LL representations are possible in the eHealth domain, for example. NN representations are rarely used within the SSM application.

MAHIS (social security system)

MAHIS is specifically made **for employers to delegate a Power to payroll professionals** (employed by another company specialised in payroll management) so that they can manage tasks within the Social Security administration, such as declaring a new employee to Social Security. This is the reason why in MAHIS, **only LP are represented and only LL representations are covered**.

Strictly speaking, an NP such as an independent accountant can also receive a Mandate via MAHIS, but only if they are registered within the Crossroad Bank of Enterprises (CBE) register. In the context of this research, we would consider them to be an LP.

The NL type also exists for the social security sector/applications. A legal representative of a company can also give a natural person (an employee) the permission to perform social security administrative tasks for the company. This is realised with the CSAM – MAM application, not via MAHIS.

Finland

In Suomi.fi e-Authorisations, one can act as a **person** (citizen) or as an **enterprise** (someone who is authorised to act in the company/ organisation’s name). Different scenarios include:

- Person to person Mandates
- Person to company/organisation Mandates
- Company/organisation to person Mandates
- Company/organisation to company/organisation Mandates.

In the case of Finland, an LP is always an NP who is authorised to act on behalf of the LP.

The Netherlands

Through DigiD, a Natural Person can grant a Mandate to a Natural Person, while through eRecognition, a Legal Person can grant a Mandate to a Natural Person (specifically, to an employee or a legal representative of the Legal Person). With DigiD, in a few cases, a Natural Person can grant a Mandate to a Legal Person; for example to labour unions so that they can manage their members' income tax procedures ("HUBA's" / Hulp bij Aangifte = Help With Declaration). The law "Digital Government" currently discussed in the Council of Ministers will improve DigiD Mandates so that this possibility can be extended to support most of the NN, NL and LN figures.

With eRecognition, it is possible for a Legal Person to grant a Mandate to another Legal Person, but on a limited scale, because both legal persons should use the same (private) Mandate system. eRecognition is delivered by five private companies that manage Mandate registers. If the two Legal Persons are using different private partners to manage the Mandates they grant to their employees, they cannot grant Mandates between one another. This is why they should have a contract with the same Mandate management company.

Portugal

The SCAP eID is automatically activated for owners of a valid Portuguese CC eID card or CMD eID, aged 16 years or older.

The SCAP eID usage starts after the owner of a valid Portuguese CC eID card or CMD eID requests and links professional, business or public attributes to their CC eID and / or CMD eID.

The SCAP system is very specific as it is meant **for professional representatives**. For this reason, it covers NL relationships, meaning natural persons representing legal persons.

Spain

The REA system covers all possible interactions established by law. It includes natural persons acting on behalf of legal persons and legal persons acting on behalf of legal persons.

Comparative analysis: commonalities and differences

Most of the systems cover all types of users and representations. It is worth noting that in all MS, an NP is always needed as the legal representative of an LP.

Some of the systems analysed are only made for one type of person, as in the case for eHerkenning in the Netherlands or MAHIS in Belgium (legal persons).

Some types of representations are more commonly used than others, as visible in the table below.

TABLE 4: COMPARATIVE ANALYSIS OF TYPES OF PERSONS AND TYPES OF REPRESENTATION

	AT	BE		FI	NL		ES	PT
	EMS	SSM	MAHIS	E SUOMI	@Podera	eHerkennin g	@Podera	SCAP
	TYPES OF PERSONS							
NP	YES	YES	NO	YES	YES	YES	YES	YES
LP	YES	YES	YES	YES	NO	YES	YES	NO
	TYPES OF REPRESENTATION							
NN	YES	YES	NO	YES	YES	NO	YES	NO
NL	YES	YES	NO	YES	YES ³⁵	NO	NO	YES
LN	YES	YES	NO	YES	NO	YES	YES	NO
LL	YES	YES	YES	YES	NO	YES	YES	NO

3.4. From which register is identification and authentication information retrieved?

Austria

For **Natural Persons**, identity information is retrieved from the **Central Register of Residents (CRR)** and from the **Supplementary Register for Natural Persons**.

Austrian citizens (natural persons) register in the Central Register of Residents (CRR) where a unique identifier (CRR number) is assigned. This CRR number is encrypted, to create a **Source Personal Identification Number (sourcePIN)**. This process is under the control of the sourcePIN Register Authority (SPA), which is governed by the Austrian Data Protection Commissioner.

Since a sourcePIN cannot be used directly within the different eGovernment applications due to privacy reasons, a **Sector-Specific Personal Identification Number (ssPIN)** is created for each application sector (taxes and duties, social security, etc.).

³⁵ Limited to a few business cases.

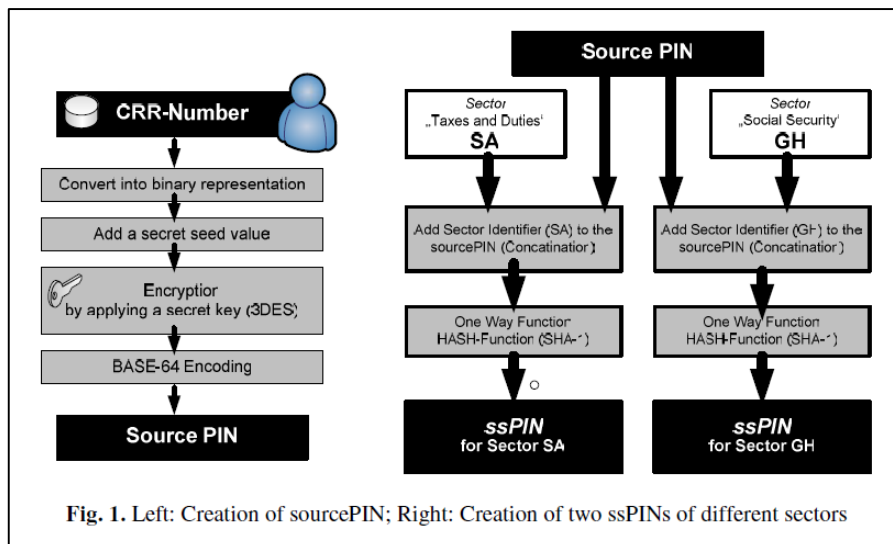


Fig. 1. Left: Creation of sourcePIN; Right: Creation of two ssPINs of different sectors

FIGURE 6: CRR, SOURCEPIN AND SSPIN NUMBERS³⁶

The next step is the **Person Authentication**, where the Citizen Card introduces the so-called **Identity-Link**, an XML structure combining the person's unique identification number (sourcePIN) with his/her public keys required to verify his/her qualified signatures. Identity-Link is electronically signed by the issuing sourcePIN Register Authority. Identity-Link is the only place where a person's sourcePIN is allowed to be stored. The Citizen Card is the only place where the Identity-Link is stored.

The sourcePIN Register Authority, in spite of its name, does not maintain a register of sourcePINs: it is only able to create sourcePINs on demand. Technically, the sourcePIN register is a virtual register, generating sourcePINs when required, and deleting them afterwards.

For Legal Persons, the identity information is retrieved from the following registers:

- For companies: Companies Register
- For associations: Zentrales Vereinsregister (ZVR) = Central Association Register
- For other legal entities: Ergänzungsregister für sonstige Betroffene (ERsB) = Supplementary Register for Other Parties Affected.

Belgium

SSM (finances system)

CSAM searches for its information in the following authentic source databases:

- For Natural Persons: **Rijksregister** (the national register for natural persons)³⁷

The Belgian National Register contains citizens' identity information as well as their unique personal identifier (national number). It is administered by the FPS Interior (Home Affairs), but the information is provided by the public administration of the municipalities and embassies

³⁶ [Empowerment through Electronic Mandates – Best Practice Austria, Thomas Rössler, A-SIT](#)

³⁷ <http://www.ibz.rn.fgov.be/nl/rijksregister/>

abroad. Access to the National Register is strictly controlled by the Commission for the Protection of Privacy.

- For Legal Persons: the **Crossroad Bank of Enterprises (CBE)**³⁸

The CBE contains comprehensive identification data related to businesses and their “establishment units” (i.e. business location). It covers all enterprises and contains their unique identifier (the Enterprise Number). It includes data from the national register of legal entities and the trade register.

MAHIS (social security system)

MAHIS uses the same authentic source databases as SSM:

- For the identification/authentication phase of NP: it is completed via eID, using the CSAM platform that is connected to the FAS (Federal Authentication Service), which retrieves information from the national register for natural persons.
- For the identification of companies and authorisation of the legal representative of the company: the Crossroad Bank of Enterprises.

Finland

The basic registers are the Population Information System, the Business Information System and the Trade Register.

The **Finnish Population Information System** is a computerised national register that contains basic information about Finnish citizens and foreign citizens residing permanently in Finland. This is one of the base registers that are used when producing e-Authorisations.

The Netherlands

The information sources are the following base registries:

- Base Registry of Persons (BRP)
- Business Registry (HR / Handelsregister).

The BRP is used to Mandate natural persons and HR to verify the authorisation of legal representatives to Mandate the so-called “Mandate administrators” and the Mandatees.

Additionally, other base registries are relevant (i.e. registry of notaries, lawyers and professionals working in the healthcare sector) with regards to “Statutory representation”, which, however, is not yet implemented.

Portugal

After successful authentication of the SCAP eID holder, the SCAP eID electronic identification authority (AMA₆ - Agência para a Modernização Administrativa, I.P.) communicates with the authoritative sources of professional, business or public attributes required to prove the functions that the SCAP eID holder performs in society as qualified professional and/or his/her powers and capacities in the context of a public/private company.

The authoritative sources of professional, business and public attributes are the authorities that are accountable for:

³⁸ https://e-justice.europa.eu/content_business_registers_in_member_states-106-be-en.do?member=1

- Managing the attributes;
- Linking the attributes to the CC eID and / or CMD eID of its rightful owner;
- Digitally signing the answer to the eID IdP (namely the eID IdP SCAP eID authentication mechanism component), when the eID IdP requests professional, business or public attributes of a citizen.

Professional, business or public attributes may be linked to the CC eID and / or CMD eID according to national legislation:

- Business attributes are linked to the CC eID and / or CMD eID by:
 - The registration services of IRN³⁹;
 - Lawyers, solicitors and notaries based on legal documents that are the authoritative source of business attributes.
- Public or professional attributes are linked to the CC eID and / or CMD eID by the entities that are the authoritative sources of the attributes concerned.
- Attributes with powers and capacities in the context of public companies are linked to the CC eID and / or CMD eID after being verified in the Official Gazette of the Portuguese Republic.
- Attributes with power of attorney are linked to the CC eID and / or CMD eID of the attorney, after being verified at the “Online power of attorney” web service⁴⁰ managed by the Ministry of Justice.

Spain

In Spain, the system is fully integrated with the eID system. Natural persons can use several methods for identification:

- The electronic ID, which is connected to the police database
- The electronic certificate
- The mobile application Cl@ve.

For natural persons, the identity data is retrieved from the **Registry of Persons**. For legal persons, the data comes from the **certification authorities**, which certify the validity of a Power given by a legal person and provide digital certificates.

The eMandates are stored in the **national Mandate registers**. The end-user manages his/her Mandates on the interface of each system/registry. Both the Mandator and the Mandatee can consult, modify and revoke Mandates there.

Comparative analysis: commonalities and differences

All the analysed MS retrieve the identity data information from citizens’ and businesses’ authentic source base registries. The information is always centralised.

Legal persons characterisation may differ from one MS to another. For example, in Austria a legal person can be registered in three different business registers, depending on their status.

³⁹ Instituto dos Registos e Notariado (Institute of Registries and Notaries)

⁴⁰ <https://www.procuracoesonline.mj.pt>

3.5. Where are the eMandates stored and how are they digitally preserved?

Austria

The online Mandate service only collects Mandate information from base registries. It is a **Mandate aggregation proxy** that does not store the eMandates.

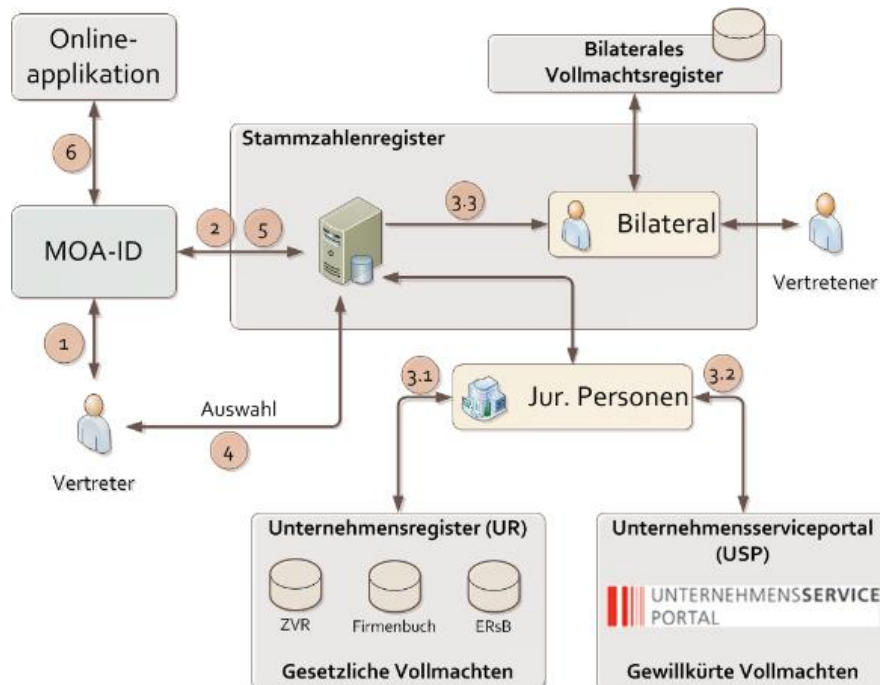


FIGURE 7: ARCHITECTURE OF THE ONLINE MANDATE SERVICE, EGIZ⁴¹

Natural Persons Mandates are stored in a service of the Source PIN Register Authority, which is a duty assigned to the Austrian Data Protection Authority. The Mandate register stores what Austria calls “bilateral Mandates” between natural persons. Through this web service, the eMandate can be created and retrieved whenever needed.

Legal Persons Mandates are stored in the different **business registers**:

- Commercial register
- Zentrales Vereinsregister (ZVR) = Central Association Register
- Ergänzungsregister für sonstige Betroffene (ERsB) = Supplementary Register for Other Parties Affected.

In addition to the business registers, **the USP portal (Unternehmens Service Portal)** is a web-based application that can be used for a lot of daily business operations. It facilitates the set-up, management and storing of what Austria calls **Delegated (or ad-hoc) Mandates (“Gewillkurte”)**.

Belgium

SSM (finances system)

⁴¹ <https://www.egiz.gv.at/en/e-government/6-Online-Vollmachten#sub-mis-mms>

The eMandate issued is stored in the FPS Finances **local database**. All eMandates are automatically preserved and remain accessible online. There is no specific regulation saying that once the Mandate expires it must remain visible or be archived. At the present time, the eMandates are not archived, but in the future there could be a need to archive the older ones.

- **Tax-on-web** (income tax private persons): 4 025 838
- **Intervat** (VAT declarations and reports): 347 529
- **Biztax** (income tax companies): 229 009
- **Mymifin** (individual digital tax file private persons and companies): 406 742
- **Work flow** (digital follow up of fiscal complaints): 7 061
- **Finprof** (salary related taxes): 382 278
- **E-health** (ministry of healthcare): 30 769

FIGURE 8: NUMBER OF ACTIVE MANDATES IN SSM⁴²

MAHIS (social security system)

In MAHIS, the Mandate issued is stored in an Oracle database and in a second database (dataguard) of the National Social Security Office. There is synchronisation in real time between the two databases in case of problems with the main one. The Mandates are stored for an unlimited period in the database.

Finland

Digital authorisations are saved in the national Mandate register, where the verification of the authorisations is done. A citizen or a company can create and save authorisations in digital form directly in the national Mandate register. Later, the stored eMandates are transferred to the long-term register.

Currently, eMandates can be accessed by services that are integrated into e-Authorisations. This means that these services are able to answer whether the Mandatee has a necessary Mandate or not, but the services don't have access to the content of the eMandate itself.

A Mandate itself can be valid up to 25 years. These are registered in the authorisations registry. Any changes in the authorisations registry are logged as well as the use of e-Authorisations. The use of e-Authorisations in this case means the inquiry service between the PRC and the user organisation enabling the inquiries via the national data exchange layer or interface inquiry/service and checking whether or not the person has a right to act on behalf of another person or organisation based on the data in the base registries or in the authorisations registry.

The logs are stored for five years. The logging data can be released for the person him/herself based on the KaPA-act (§ 13 Retention of data processed in service production and § 14 Disclosure of the information handled within service production) as well as in cases of malfunction or errors to user organisations (in general). Also, the handling of logs is logged and this log is stored for five years as well.

⁴² PowerPoint shared during the Belgium SSM interview

The registry data or logs are not public data and not publicly available. The person can check the eMandates via the national portal Suomi.fi where the s/he is identified via e-identification.

The Netherlands

For DigiD Authorisations, the eMandates are stored in a database.

As already explained, for eRecognition, there are five companies that deliver the eMandate scheme with several roles, including that of managing the Mandate register. The eMandates and their use history are stored by these private companies: they archive the trails and make it possible to audit the life-cycle of the Mandates.

Portugal

When a Mandate is created in front of an attorney for example, it can be registered electronically through the Procuracoes Online system.

The SCAP system does not allow for the creation or storage of eMandates. It simply acts as a bridge at the moment when the user authenticates on a system as a professional, discovering and providing the professional certification and/or eMandate that validates the powers of this citizen to act in front of the administration. SCAP supports interactions among different systems.

Spain

The eMandates in Spain are stored in many different registries:

- General Mandates are stored in the state, regional and local government registries;
- Specific Mandates are stored in the Tax Agency, Social Security and Traffic Department registries;
- Judicial Mandates are stored in one specific judicial registry;
- Notarial Mandates are stored in one specific notarial registry.

All the different registries must by law be interoperable and interconnected.

For administrative Mandates, **interoperability is mandatory by law 39/2015 (article 6)**⁴³: “The general and particular electronic registries of Powers belonging to each and every one of the Administrations must be fully interoperable with each other, so as to guarantee their interconnection, computer compatibility, as well as the electronic transmission of the requests, writings and communications.”

There is a **web service to query any kind of Powers registered** in the central information system. Query of other registries are not necessary, as the Powers within these registries only have effects in the administrations in charge of the specific registry.

Interoperability with notarial eMandates is mandatory by law 39/2015 (article 6): “The general and specific eMandate registries will make it possible to prove validly the representation of those who act before the Public Administrations on behalf of a third party, by consulting other similar administrative registries, the mercantile registry, the property registry, and the notarial registry. The mercantile registry, property registry, and notarial registry will be interoperable with general and specific eMandates registries”.

⁴³ <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a6>

There is a web service to query any kind of Powers registered in the notarial information system for eMandates.

For **judicial eMandates**, there is only one registry and it is accessed by all the Courts. No other Public Administration is entitled to access this registry.

The law says that **the Mandates are valid for a maximum of five years**. In terms of storage in Spain, there is a **document management policy**, but it is not specific to electronic Mandates' digital preservation.

Comparative analysis: commonalities and differences

For some MS, there are specific registers for Mandates. These specific Mandate registers can be public, as in Austria where it is hosted by the Data Protection Authority, or private, as in the Netherlands where different private companies manage and store the Mandates in their own system.

For other MS, the Mandates are directly stored in the base registries where natural and legal persons' identity data is initially retrieved, or in the registries of the public administrations, as in Spain.

For all MS except Finland, there is no retention and disposition policy that would be specific to eMandates. All of the MS preserve the Attributes of the Mandates: the log metadata of the transactions are preserved, and the information is permanently available. With the exception of Finland, this information is not transferred to an archive or to a more permanent system.

3.6. Who issues the eMandates and where can the end-user manage them?

Austria

In Austria, eMandates can only be issued by **the SourcePIN Register Authority**, an entity governed by the **Austrian Data Protection Authority**.

The eMandate system, which is integrated with the Austrian eID scheme, collects information from the authentic source registers and aggregates this information.

Once the eMandate is generated, **it has to be electronically signed by the SourcePIN Register Authority** before it is valid. The SourcePIN Register Authority signs the Mandate dataset.

The representation data is queried from authoritative sources and the eMandate is created and signed by the SourcePIN Register Authority at the moment when the Mandatee accesses the service. This ensures fresh Mandates, so that revoked Mandates or ceased representations can no longer be used.

Concerning the management of the eMandates by the end-user, there is no one-stop-shop in Austria.

NP can set up, view, manage and revoke their Mandates based on their profiles through the web service of the SourcePIN Register Authority, which is specific for NP / NN representation⁴⁴.

⁴⁴ eMandate management application for natural persons: <https://mms.stammzahlenregister.gv.at/mms/moaid.do>

Statutory eMandates for LP are managed by the authoritative sources (business registers) which have specific functionalities made for this purpose. **Delegated Mandates for LP** can be managed on the **USP portal (Unternehmens Service Portal)**, a web-based application used by companies for daily business operations⁴⁵. However, in some very specific use-cases, Mandates for LP can be also managed in the application for NP (e.g. for one-man companies).

Belgium

SSM and MAHIS are both user interfaces where users can change information on their Mandate.

In Belgium, the process of creating a Mandate with SSM makes use of several applications that are related to CSAM⁴⁶. SSM is one of those applications, but it is limited to the creation and use of eMandates. The other CSAM-related applications focus on identification and authentication, user access management, and role administration.

The social security related eMandates are created and managed in MAHIS. The Mandates are issued by the NSSO. The login/identification/authentication process is only partially managed by the NSSO, as it is linked to the CSAM collaborative project between federal institutions.

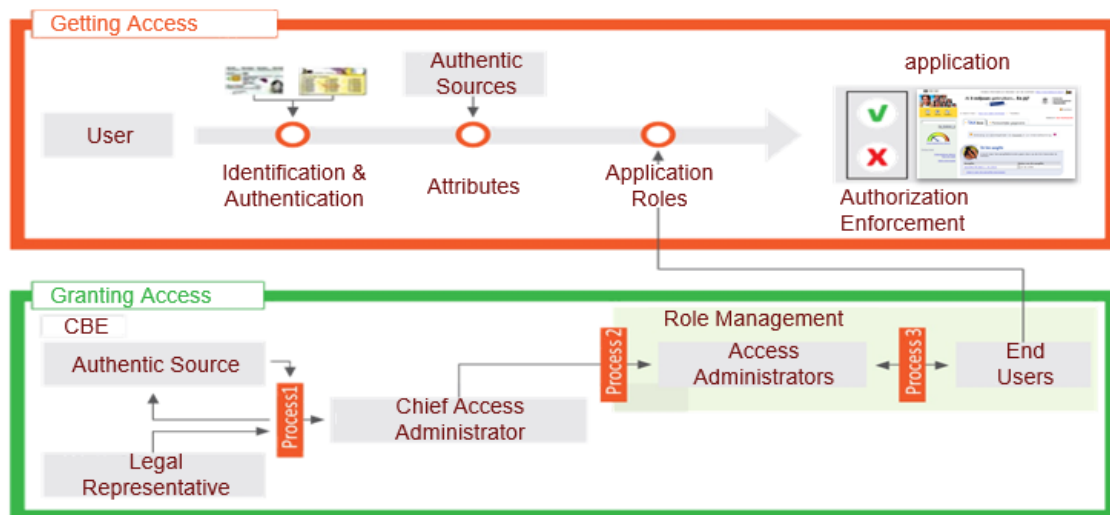


FIGURE 9: IDENTIFICATION & AUTHENTICATION ACCESS (CSAM)⁴⁷

Finland

In Finland, the Mandates are issued within the Suomi.fi e-Authorisations platform, which is a web application that citizens can access with their preferred eID and issue Mandates.

This user interface allows the Mandator to modify the Mandate scope or duration, and to revoke it if necessary.

⁴⁵Unternehmens Service Portal: <https://www.usp.gv.at/Portal.Node/usp/public>

⁴⁶ See CSAM demo videos on the identification, creation and acceptance of an eMandate: https://finances.belgium.be/fr/E-services/Mandats/demos_Mandaten

⁴⁷ PowerPoint transmitted by the Belgian interviewees

The Suomi.fi e-Authorisations platform allows for the electronic handling of Representation Powers between natural and legal persons, as well as between legal persons. In the user interface, users can access the usage history of all their Representation Powers.

The Netherlands

In the Netherlands, the eMandates of the type NN are issued within the DigiD Authorise platform, where there is a user interface allowing the Mandator to modify the Mandate scope or duration.

In both DigiD Authorise and eRecognition, there is a user interface allowing the Mandator to modify the Mandate scope or duration.

Portugal

SCAP is not a platform where eMandates can be created, stored or managed. The users of SCAP need to become “members” in order to use the service that will allow them to authenticate and sign documents with their professional certification.

The use of SCAP requires explicit acceptance of the respective conditions of use, which are defined by the **Agency for Administrative Modernization (AMA)** and are published on its website.

As a rule, the SCAP user is responsible for updating the data contained therein and cannot use the authentication and signature for certification of professional, business or public attributes when he or she no longer holds them.

Spain

The end-user can manage his/her Mandates on the different web applications hosted by the different systems.

Comparative analysis: commonalities and differences

In most MS, the Mandate Issuing System is managed by the same authority that provides the user interface for Mandate management.

In the Netherlands, there is one user interface for LP, eHerkenning, although the different eMandates and eMandate systems are managed by different private companies.

3.7. Do the MS have national vocabularies and/or specifications for eMandates?

In the deliverables of the first phase of the ISA² Action 2016.12, the following table was presented. The table has been updated according to the interviews performed.

TABLE 5: NATIONAL SPECIFICATION AS-IS DETAILED OVERVIEW⁴⁸

	AT	BE	FI	NL	ES
Defined reference data / core vocabulary / code list	Green	Red	Red	Red	Green
Defined semantic differentiation and identification of Mandates	Green	Yellow	Green	Green	Green
Defined technical requirements for creation, usage, handling and revocation of electronic Mandates	Green	White	Green	Green	Green

- Green: the MS is fully compliant with the statement specified
- Yellow: the MS is partially compliant with the statement specified
- Red: the MS is not compliant with the statement specified and there are no plans to work on this
- White: no information found

Austria

In Austria, national interoperability is supported by agreeing to the specifications through the Austrian eGovernment cooperation platform, called **Digital Austria**.

Austria has published **Austrian Specifications of Electronic Mandates**⁴⁹. This has allowed Austria to create its own Attributes for eMandates, in its own jurisdiction.



FIGURE 10: WEBSITE TO DOWNLOAD THE AUSTRIAN SPECIFICATIONS OF ELECTRONIC MANDATES⁵⁰

⁴⁸ Phase 1 Deliverable “List of common information requirements of the prioritized services/projects/domains” (page 12-13)

⁴⁹ https://www.ref.gv.at/fileadmin/_migrated/content_uploads/elvm-spez_1-0-0_20060530.pdf

⁵⁰ https://www.ref.gv.at/Q-BK_Elektronische_Vollmachten.961.0.html

Austria defined the transactional messages (Request and Response) in on XSD schema. XML instances of this schema “envelope” in a file “mandate” any possible format of eMandate coded as Base 64 binary content. The migration of the eMandate content to Attributes of the SAML assertion is planned but has not yet been implemented. Frequent Mandate types are indicated by an Object Identifier (OID)⁵¹. The XML specification contains the main constraints needed by application, such as the transaction limits or validity periods. In addition to pre-defined types and constraints, arbitrary limitations can be included in free text areas. Such arbitrary constraints, if included, usually need manual inspection.

In a nutshell, frequently used data is modelled in the XML scheme, and standard Mandate types are indicated by specific OIDs. To remain flexible, further OIDs can be introduced, and the free-text areas allow for specific cases.

Belgium

In Belgium, there is no eMandate national vocabulary or specifications. The systems have grown organically, and the experts have recognised that there is a need to now create a legal framework and to work on synergies.

SSM (finances system)

The harmonisation is done on a case-by-case basis, through agreements between the different systems/applications. For example:

- The application for Access Management has created domain definitions (healthcare, finance, etc.). The SSM system has to respect those domains, but they did not develop the definitions themselves.
- With the application used for Role Administration, some Service Level Agreements with SSM ensure that the names of the roles used to delegate representation within a company are the same in both systems.

For SSM, the existing business rules are very outdated and the current ones are not yet clearly defined.

MAHIS (social security system)

An IT partner has developed and is maintaining this system. Data models and business rules are described in the “Guidelines” document⁵² as well as on the website⁵³.

Finland

There is no general vocabulary for eMandates (“e-authorisations”). However, the terms and concepts used in the names and descriptions of the Mandate codes come from the ontologies of the National Library’s ontology service⁵⁴. The application and controlled use of these terms and concepts for the eMandate system was done in consultation with The Finnish Terminology Center (TSK). So even if there is no Finnish eMandate vocabulary per se, Finnish eMandates

⁵¹ <https://vollmachten.stammzahlenregister.gv.at/mis/>

⁵² https://www.socialsecurity.be/site_fr/employer/applics/mahis/documents/pdf/guidelines_mahis_F.pdf

⁵³ https://www.socialsecurity.be/site_fr/general/helpcentre/legend_xml/legend_xml_1.htm

⁵⁴ <http://finto.fi/en/>

adhere to the semantic framework and interoperability principles recommended for all public sector authorities in Finland.

The Netherlands

There are, for both DigiD Mandates and eRecognition terms and definitions, business rules and data models.

The legal basis is found in the Law Electronic Message Exchange (further analysed in the following chapter) and in the Ministerial regulation⁵⁵ containing rules concerning the operation, security and reliability of the facilities for electronic messaging and information provision, as well as facilities for electronic authentication and electronic registration of authorisations.

Portugal

There is no national vocabulary. However, SCAP has developed a set of attributes to be used by authentic sources.

5.1 Attributes provided for natural persons under the SCAP eID scheme

In the context of authentication of a natural person, the attributes provided by the Portuguese SCAP eID scheme (if requested by a relying party and authorized by the citizen) and their correspondence with the eIDAS Minimum Data Set in accordance with [eIDAS Attribute], are:

	eIDAS Minimum Data Set		Provided by the SCAP eID scheme
	Mandatory	Optional	
FamilyName - Current Family Name	X		Yes
FirstName - Current First Names	X		Yes
DateOfBirth - Date of Birth	X		Yes
PersonIdentifier - Unique Identifier	X		Yes
BirthName - First Names at Birth		X	No
BirthName - Family Name at Birth		X	No
PlaceOfBirth - Place of Birth		X	No
CurrentAddress - Current Address		X	Yes
Gender - Gender		X	Yes

FIGURE 11: ATTRIBUTES PROVIDED FOR NATURAL PERSONS UNDER THE SCAP EID SCHEME

Spain

All eMandate systems of the public administration, excluding the central notaries' one, use a common semantic interface/vocabulary (two XSD-based imported/included in the web-service WSDL, one for the request and one for the response) for the instantiation and exchange of the eMandate (as payload). This applies only when the exchange of eMandates is needed (in accordance with the law), therefore all remote systems use this semantic interface to consult the Mandates type A of @Podera.

⁵⁵ <https://zoek.officielebekendmakingen.nl/stcrt-2015-37158.html>

Comparative analysis: commonalities and differences

Spain has developed national specifications for eMandates, publicly available online. Finland has based its model on a general vocabulary, also available online. See Chapter **¡Error! No se encuentra el origen de la referencia.** “**¡Error! No se encuentra el origen de la referencia.**” for more details.

In some of the MS, such as Belgium, there are application-specific guidelines and business rules. In addition, some sector-specific laws define the minimum requirements for the Mandates, as is the case for eHealth in Belgium, for example.

3.8. What legal framework impacts the eMandate system?

In the deliverables of the first phase of the ISA² Action 2016.12, the following table was presented. The table was updated according to the interviews performed.

TABLE 6: LEGAL FRAMEWORK AS-IS DETAILED OVERVIEW⁵⁶

	AT	BE	FI	NL	ES
Concept of electronic Mandate defined by the legislation	Green	Red	Green	Green	Green
Validity of electronic Mandates legally equated to material/paper format	Green	White	Yellow	Green	Green
Management and requirements for handling electronic Mandates defined by law	Green	Red	Red	Green	Green

- Green: the MS is fully compliant with the statement specified
- Yellow: the MS is partially compliant with the statement specified
- Red: the MS is not compliant with the statement specified and there are no plans to work on this
- White: no information found

Austria

The central legislation in Austria for eGovernment⁵⁷ is **the eGovernment Act⁵⁸**, which also contains **a section on representations** for natural persons, representations for legal persons, and a specific type of representation for people working and acting in representation of natural or legal persons as a matter of law or as a part of their service (ex. lawyer).

The principal requirement in relation to (electronic) Mandates from the eGovernment act is that individuals may authorise another person to submit applications on their behalf. Specifically, §5 of the eGovernment Act states that in case of representation of natural or non-natural persons, a reference to the permissibility of the representation must be entered in the identity link of the representative. This occurs where the sourcePIN Register Authority, having been presented with proof of an existing authority to represent or in cases of statutory representation, enters into the citizen card of the representative, upon application by the representative, the sourcePIN of the data subject and a reference to the existence of an authority to represent, including any relevant material or temporal limitations.

Therefore, when a Mandate is given, the sourcePIN Register Authority stores the Mandate, including any limitations it may contain, as well as the sourcePIN of the person being represented. The Mandate is thereafter available for any public authorities with a legal Mandate to access and use it, if the citizen gives prior consent.

Mandates can also be used by **professional representatives**; this is governed by a separate section of the eGovernment Act which notes that: “In cases of professional representation

⁵⁶ Phase 1 Deliverable “List of common information requirements of the prioritized services/projects/domains” (page 12-13)

⁵⁷ See <http://archiv.digitales.oesterreich.gv.at/site/6514/default.aspx> for a general overview

⁵⁸ <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230>

(*berufsmäßiger Parteienvertretung*) no particular proof of authority as in subparagraph 1 to represent is required if the general authority to represent is evident from the notice of professional entitlement according to the professional regulations in the signature certificate. In this case, the sourcePIN Register Authority shall, upon application of the professional representative, provide the sourcePIN of the data subject”.

Whatever the form, the central legal requirements imposed by the eGovernment Act are the use of the sourcePIN, and the registration of the Mandates with the sourcePIN Register Authority. The sourcePIN is therefore an infrastructural component which also takes a prominent legal role. §5.4 of the eGovernment Act states explicitly that any Mandate must be included in the citizen link, and electronically signed or sealed by the sourcePIN Register Authority.

The sourcePIN Register Authority is governed by **the sourcePIN Register Act, which does not directly impact the eMandate system**: there is a requirement on eMandates and information that is required concerning, for example, a Mandate’s constraints and limitations on time or scope, but the information there is very generic.

Specifically, in relation to health care, further legal requirements for eMandates are included in the **Federal Act on Data Security Measures when using Personal Electronic Health Data** (Health Telematics Act 2012) (*Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verwendung elektronischer Gesundheitsdaten –(Gesundheitstelematikgesetz 2012 – GTelG 2012)*⁵⁹. Article 18 of the Health Telematics Act charges the *Hauptverband der Österreichs Sozialversicherungsträger* with the establishment and operation of a Patient Index. This serves two purposes:

- a) The verification of the identity (sect. 2 no. 2 E-Government Act) of natural persons in the context of EHR or other e-health applications; and
- b) The localisation of Registries, in which references to the EHR health data of these individuals can be found.

Data to be included in this Index are specified in the law. Powers of Representation for EHR participants must be registered in accordance with the eGovernment Act (i.e. stored with the Register Authority), with the important difference that the Personal Identification Number of the EHR participant must be used instead of the sourcePIN and that the permission to access the EHR must be registered separately. The Mandate may have a maximum duration of 365 days. The Mandate of healthcare providers themselves (i.e. the right to obtain EHR data at all) must be kept in a separate database, the Healthcare Provider Index, established and operated by the Minister of Health. Their data must be obtained from either (i) appropriate identification cards of the e-card system, a citizen card, or by using electronic signatures, which must be traceable to qualified certificates.

Belgium

Globally, eMandates in Belgian government systems are based on a centrally controlled infrastructure which leverages Belgium’s eID systems as far as possible, and which only allow these Mandates to be used for the purposes of Belgian eGovernment services.

⁵⁹https://www.ris.bka.gv.at/Dokumente/ErV/ERV_2012_1_111/ERV_2012_1_111.pdf

For MAHIS, **there is a sector-specific law for Social Security** that regulates Mandates, but it is not focused on eMandates in particular. The legal basis is primarily the Law of 29 June 1981. This law determines the conditions a payroll professional/service provider must meet to be able to receive a Mandate from a company/employer. The law also stipulates that the NSSO must be informed in advance of the Mandate by means of a procuration document (e-procuration)⁶⁰.

There is also a **sector-specific law for Mandates in the e-Health sector**. The legal basis for these Mandates can be found in the Law of 21 August 2008 establishing the eHealth Platform⁶¹ and in the authorisations of the sectorial committee on healthcare of the data protection authority.

There is **legislation in relation to the National Register**⁶² (containing information on Belgian citizens and permanent residents), **the Crossroads Bank of Enterprises**⁶³ (containing information on companies established in Belgium and branches of foreign companies in Belgium), the Belgian **eID card**⁶⁴, and **electronic identification**⁶⁵. However, these laws all relate to the resources used for the identification of natural persons and legal entities, and not to their representation as such (although the Crossroads Bank of Enterprises contains information on the designated managers of legal representatives of companies, so it is indirectly relevant to this topic).

Separate from this public sector context, eMandates can be created on a purely contractual basis, according to Art. 1984 of **the Civil Code** and following. Mandates are consensual contracts, and can be concluded even orally, in the absence of any written document, although the acceptance of the Mandate by the Mandatee is required. There is no signature requirement. Therefore, the conclusion of a Mandate can be done electronically without any requirements on the form.

As a final point in relation to electronic Mandates, it is worth noting that, when implementing the eIDAS Regulation into Belgian law via the Law of 21 July 2016 on electronic identification, a specific provision was added in relation to the use of **qualified electronic seals**. Specifically, Belgian law requires that, when an entity uses a qualified electronic seal on a legal act between Belgian entities, this seal is considered the legal equivalent of a hand-written signature of a natural person mandated to authorise that legal entity. In other words, under Belgian law, a qualified electronic seal belonging to a company is legal proof of the Mandate of the natural person controlling the seal to represent that company.

⁶⁰http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1981062902&table_name=wet

⁶¹http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2008082153

⁶² Law of 8 August 1983 on the National register of natural persons, as repeatedly modified; see http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=1983080836

⁶³ Law of 17 July 2013, introducing Book III into the Code of Economic law (integrating the prior Law establishing the Crossroads Bank of Enterprises into the Code of Economic law); see http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2013071732

⁶⁴ Law of 19 July 1991 on the population registers, Identity card, foreigner cards and residence documents; see http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=1991071931

⁶⁵ Law of 21 July 2016 on electronic identification; see http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2016072140&table_name=wet

Finland

The main legal framework regarding the Suomi.fi-e-Authorisations is the **Act on common administrative e-service support services (KaPA-Act)** (Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista⁶⁶), which entered into force on 15 July 2016. As the name suggests, this legal framework applies to eGovernment support services in general, known as Suomi.fi-services, and not only to electronic Mandates.

The Suomi.fi-services covered by the KaPA-Act most notably include:

- National data exchange layer (“X-road Finland”) – Suomi.fi Data Exchange Layer
- e-identification – Suomi.fi e-Identification
- e-authorisations – Suomi.fi Digital Authorisations
- Finnish service catalogue – Suomi.fi Finnish Service Catalogue
- National portal Suomi.fi – Suomi.fi Service Views
- e-messaging – Suomi.fi Messaging
- Payments – Suomi.fi Payments
- Maps – Suomi.fi Maps

For the purposes of this report, principally the Suomi.fi Digital Authorisations are relevant. The Act stipulates (among other topics) rules on the use of Digital Authorisations, conditions for bringing data/information to Service Views, the identification of a person, and communication of messages to a citizen or to an organisation represented by a citizen. Use of these support services is mandatory for government authorities, agencies, institutions and enterprises; the municipal authorities when performing their tasks as provided for by law; and courts and other jurisdictions (see §5 of the KaPA-Act). Private communities, foundations and businesses may also use the services under specific conditions (see §8). The e-Authorisations service is thus a shared solution which can be used free of charge, including by the private sector.

The main provision dealing with electronic Mandates can be found in §10, which states that the Population Register Center (PRC) “provides for a register of natural persons and authorisations and other expressions of willingness to act on behalf of the Communities. The Population Register Center may also provide information on other authorisations and other voluntary information stored by other authorities if the authority that deposited this data has given the Population Register Center permission to transmit the information and does not compromise the reliability of the information provided in the NSA”. Summarily, the PRC is mandated to keep a database of authorisations that have been created for the benefit of public services.

The conditions for the creation of eMandates are similarly established in §10, which notes that the PRC must register the expression of the will of a user based on a reliable identification process, using a method that is secure and provable. In addition, the registration of a Mandate is subject to the requirement that the PRC is able to ensure the person's competence, including by consulting specific authoritative registers listed in the law (notably the Population Information System, the Guardianship Register, the Association Register, the Business Register, the Corporate Information System and the Foundation Register). Supported identification methods must be approved by the PRC after consultation with the Ministry of Finance and FICORA.

⁶⁶ <https://www.finlex.fi/fi/laki/alkup/2016/20160571> (Finnish and Swedish)

The KaPA-Act allows the PRC, when offering an identification service to a natural person, to disclose information about an individual's personal identity, personal identity number and e-business identity (i.e. including its registered eMandates), or the necessary information to establish the existence of a limitation of competence or Power to a user organisation that maintains a service if the user organisation is legally entitled to handle such information. The use of the authorisation is thus tied to the use of the support services in general.

It is worth underlining that, under §15 of the Act, the user organisation must retrieve information using the citizen's personal identification number or other unique identifier, and must thereafter immediately discard the personal identity number or other unique identifier if it is not entitled to handle that information. This is a safeguard for data protection reasons.

From a technical and functional perspective, the KaPA-Act also defines specific standards for support services and the use of such services (Chapter 4), which include high-level requirements such as the obligation to ensure the quality and cost-effectiveness of the support service, and that the service must be "universally applicable, performance-efficient, reliable and user-friendly and unobtrusive. In the implementation of the support service, a service provider must comply with the overall architecture and interoperability descriptions and definitions of public administration". Furthermore, service providers have a breach notification obligation, and the PRC is required to keep log files for a duration of two years, in case of incidents.

Beyond the KaPA-Act, data protection law must be adhered to, including the GDPR and the upcoming national Personal Data Act. Furthermore, the data sources used to validate eMandates are subject to specific law, including the Population Information Act⁶⁷ and Population Information Decree⁶⁸. These govern the Finnish Population Information System, a computerised national register that contains basic information about Finnish citizens and foreign citizens residing permanently in Finland, as well as the certified online e-services of the PRC in support of social functions and information maintenance. This is one of the base registers which are used when producing e-Authorisations. In accordance with the law, all persons included in this register are allocated a national identification number, which is central to the use of authorisations as described above.

In addition, there is a separate law on strong electronic identification and electronic trust services (*Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista*)⁶⁹. This contains the core provisions on electronic identification and identification services, including requirements for strong identification and for identification service providers. However, authorisations and eMandates as such are not governed by this law.

eMandates in the context of the e-Authorisations support service are thus fairly clearly regulated and focus exclusively on the use of eMandates, which are retained by the public sector, although private sector companies can be permitted to rely on them as well. Beyond that context, electronic Mandates can also be granted under general contractual law, specifically under the terms of the Contracts Act (228/1929)⁷⁰. However, these provisions are generic (covering e.g. the scope of Mandates, the right to represent persons as a result of employment, the

⁶⁷ <https://www.finlex.fi/fi/laki/ajantasa/2009/20090661> (in Finnish)

⁶⁸ <https://www.finlex.fi/fi/laki/ajantasa/2010/20100128> (in Finnish)

⁶⁹ <https://www.finlex.fi/fi/laki/ajantasa/2009/20090617> (in Finnish)

⁷⁰ <https://www.finlex.fi/en/laki/kaannokset/1929/19290228>

consequences of exceeding one's Mandate, termination conditions, etc.), and don't contain specific provisions on electronic Mandates. They do, however, establish that Mandates are form free, and can be provided through simple communication. It follows that electronic Mandates are similarly possible.

Finally, there can be relevant context or sector specific legislation concerning the Mandate to represent a person or an organisation. This kind of regulation can be related to a specific organisational type, such as limited liability companies, or specified situations on how the Mandate should be given. The context and content of these regulations are taken into account in the e-Authorisations support service.

The Netherlands

Several sets of legislation are in place to support Mandates in the Netherlands. For the public sector, the central current piece of legislation is the "Law on Electronic Message Exchange Tax Services" (Wet elektronisch berichtenverkeer Belastingdienst⁷¹). Article X of this law stipulates that the Minister of the Interior and Kingdom Relations is responsible for the infrastructure for electronic messaging, for electronic authentication, and for the electronic registration of Mandates. Section 3 of this article references the need to integrate the citizen service number (CSN, burgerservicenummer, which is the Dutch general identification number for citizens), insofar as this is necessary to execute this task. In practice, the use of the CSN is indeed central in taxation Mandates.

It is on this legal basis that Logius⁷², the IT division of the Ministry of the Interior and Kingdom Relations was mandated to establish and maintain the Authorisations Register (*Machtigingenregister*)⁷³, using the DigiD identification system for natural persons (a service called *DigiD Machtigen* – Authorising DigiD), or the eHerkenning system for legal persons. Thus, the legal framework currently supports Mandates created through the national identification system, identifying citizens through the CSN, and registered with Logius in the Authorisations Register. Logius is responsible for verifying that the scope of the Mandate as registered is in accordance with the description provided in the registrations request. Entities that wish to use the Mandates – which is only possible for public sector bodies – must request this with Logius, under the contractual terms specified by Logius⁷⁴.

Mandates have a maximum duration of five years, and for legal persons, the Mandates in eHerkenning must be requested on the basis of the authorisations indicated in the commercial registers of the Chambers of Commerce⁷⁵.

More detailed provisions are established on the basis of the Decree on the Governance of Electronic Access Services (*Instellingsbesluit besturing elektronische toegangsdiensten*)⁷⁶, which

⁷¹ <http://wetten.overheid.nl/BWBR0037120/2015-11-01>

⁷² <https://www.logius.nl/over-logius/>

⁷³ <https://afsprakenstelsel.etoegang.nl/display/as/Vertegenwoordiging%2C+volmacht+en+machtiging>

⁷⁴ See <https://www.logius.nl/ondersteuning/digid-machtigen/#c10394>

⁷⁵ <https://www.eherkenning.nl/inloggen-met-eherkenning/machtigen/> and <https://eherkenning.kpn.com/machtiging/>

⁷⁶ <http://wetten.overheid.nl/BWBR0036524/2015-04-17>

establishes the institutional framework for electronic identification and authorisation in general. These have resulted in the Agreement System (*Afsprakenstelsel*)⁷⁷, which contains operational rules and common definitions.

While this legislation was originally written for the taxation context, the system is now used more broadly. Currently, the law is being revised to account for a broader context. The new draft Digital Government Law⁷⁸ (*Wet digitale overheid*) is currently being discussed in the Council of Ministers. It will cover all the legal issues concerning eID, DigiD, eHerkenning, as well as the alternative eID scheme for natural persons. This law will, on a national level, lay the foundation for Mandate creation and management, for both natural and legal persons. The law is expected to be in place in early 2019.

The Digital Government Law would create an authorisation service (*machtigingsdienst*), as the central entity storing Mandates. Comparable to the Law on Electronic Message Exchange Tax Services, the Minister is authorised to provide detailed rules for the operation of this service. However, it is worth noting that the draft Digital Government Law foresees “recognised authorisation services” (*erkende machtigingsdiensten*), implying that there would be multiple sources of Mandate information (rather than the current single Mandate Register). These too would be authorised to use the CSN where necessary.

There are no further specific laws for Mandate management in an administrative context, and existing laws will be replaced by the Digital Government Law. In fact, because of the law *Modernization Electronic Administrative Services*, the General Administrative Law (*Algemene Wet Bestuursrecht*)⁷⁹ is amended and it is regulated that citizens and businesses are entitled to do business electronically with the government.

Outside of the administrative/governmental context however, Mandates are governed by the Civil Code, notably article 3.60 and following⁸⁰. The Civil Code contains no requirements on form, and electronic Mandates are therefore permissible. However, the person to whom a Mandate is presented may request written proof of the Mandate (which may be in electronic form), or confirmation from the Mandator. This same principle (i.e. the right to demand proof) also exists for public services, as provided in article 2.1 of the General Administrative Law⁸¹. Thus, in practical terms, in order to be effective a Mandate must be in written form, since the counterparty may require this form to be presented. This is not a validity requirement for Mandates, but rather a requirement to ensure the legal effectiveness of the Mandate.

Portugal

The Professional Attributes Certification System (Sistema de Certificação de Atributos Profissionais - SCAP) is regulated through the specific Ordinance No. 73/2018⁸². This Ordinance

⁷⁷ <https://afsprakenstelsel.etoegang.nl/display/as/Juridisch+kader>

⁷⁸ <https://www.digitaleoverheid.nl/voorzieningen/identificatie-en-authenticatie/eid/wet-gdi/>

⁷⁹ <http://wetten.overheid.nl/BWBR0005537/2018-06-13>

⁸⁰ <http://wetten.overheid.nl/BWBR0005291/2017-09-01>

⁸¹ http://wetten.overheid.nl/BWBR0005537/2018-06-13#Hoofdstuk2_Afdeling2.1

⁸² Available at <https://dre.pt/web/guest/home/-/dre/114848693/details/maximized>

provides general terms and conditions of use for the SCAP system, including for the certification of professional, business and public attributes through the Citizen Card (regulated separately via the Law 7/2007, as amended⁸³) and the Digital Mobile Key. The Ordinance stipulates that identification in SCAP can be done via the Citizen Card, the Digital Mobile Key, or any other means of electronic identification which has been recognised in the EU MS, in particular as a result of the notification system established through the eIDAS Regulation (EU) No 910/2014. In this way, cross-border interoperability is supported with respect to the identification component of SCAP.

The Ordinance also allocates responsibility for the maintenance of attribute information in the SCAP system: for business attributes, this must be done by the registration services of the Institute of Registries and Notaries, IP (IRN), and by lawyers, solicitors and notaries (which may be freely chosen by the SCAP user). However, they are not the sole responsible parties, since end-users are responsible for ensuring that attribute information relating to them remains accurate in SCAP under Article 5 of the Ordinance; misrepresentation using SCAP is labelled as a criminal offense.

Professional public associations may join SCAP, thus allowing their members to certify their professional qualifications through the system. This requires the association to conclude a protocol agreement with the Agency for Administrative Modernization (AMA), which is in charge of SCAP and defines the terms and conditions for using it.

It is worth noting that the Ordinance also regulates certain SCAP use cases. Specifically, when SCAP is used to demonstrate the capacity of the administrator, manager or director of a company (article 8 of the Ordinance), or to demonstrate a power of attorney (article 9), the qualified electronic signature of that person may be used in combination with SCAP attribute information in the following cases:

- a) Contracts with entities providing electricity, water, gas and telecommunications services;
- b) Contracts with other suppliers, with the limit to be set by the corporate bodies;
- c) Work contracts;
- d) Training and execution of public contracts, in the context of public procurement;
- e) Presentation and execution of financing applications, with the limit to be set by the governing bodies;
- f) Presentation and execution of applications to national or community funds;
- g) Opening and movement of bank accounts;
- h) Minutes and deliberations of the corporate bodies;
- i) The receipt and collection of postal correspondence.

The adhesion to the qualified electronic signature of the capacity of administrator, manager and director, or the power of attorney, has a maximum validity of two years under the Ordinance.

⁸³ Available at https://dre.pt/web/guest/legislacao-consolidada/-/lc/69738113/201704110630/exportPdf/normal/1/cacheLevelPage?LegislacaoConsolidada_WAR_drefrontofficeportlet_rp=indic

Such a power of attorney can be directly created in electronic form via the website www.procuracoesonline.mj.pt; no paper process is required for this point.

With respect to public attributes – i.e. the capacities of civil servants and of managers with a public mandate, available via the official register of the Diário da República⁸⁴ – these can be certified within SCAP so that they are retrievable and validated via the Citizen Card or the Digital Mobile Key of the civil servant. This functionality has also been integrated as Article 546 of the Code of Commercial Companies, established via Decree-Law no. 262/86 (as amended)⁸⁵.

The Ordinance also defines applicable fees for the use of SCAP, which amount to 40 euros for the certification of the quality and powers of administrator, manager and director; and for the certification of the quality and powers of attorney. However, the first use of the certification service is free of charge.

Spain

Several legislative frameworks in Spain can apply, depending on the type of eMandate. Examining first the legal Mandates which are stored and managed by the government, these fall into three broad categories:

- a) **Administrative** eMandates, regulated by Law 39/2015⁸⁶ on common administrative procedures for government services, executed by Royal Decree 668/2015 (art.15)⁸⁷, and Ministerial order HAP/1637/2012⁸⁸ regulating the @Podera Electronic Registry of Authorisations. These Mandates can authorise a natural or legal person to act on behalf of another person towards public administration.
- b) **Judicial** eMandates, regulated by Law 18/2011⁸⁹. These Mandates allow the determination of competences in court administrations. There is only one registry for these Mandates.
- c) **Mandates** granted before **notaries**, regulated by the Civil Code⁹⁰. There is only one registry for these Mandates.

With respect to **administrative eMandates**, these Mandates are stored in two types of registries:

- a) General e-Mandate registries: State government, regional governments and local governments.
- b) Specific e-Mandate registries (which are explicitly permitted by the law): Tax Agency, Social Security, Department of Traffic.

⁸⁴ Regulated by Decree-Law No. 83/2016, see <https://dre.pt/web/guest/pesquisa/-/search/105371771/details/normal?!=1>

⁸⁵ Available at:

https://dre.pt/web/guest/legislacao-consolidada/-/lc/116042191/201810092123/73600517/diploma/indice?p_p_state=maximized

⁸⁶ <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a6>

⁸⁷ <https://www.boe.es/buscar/doc.php?id=BOE-A-2015-8048>

⁸⁸ <https://boe.es/buscar/act.php?id=BOE-A-2017-7719>

⁸⁹ <http://www.boe.es/buscar/act.php?id=BOE-A-2011-11605&p=20151006&tn=1#a32bis>

⁹⁰ <https://boe.es/buscar/act.php?id=BOE-A-1889-4763&p=20170629&tn=1#tix-2>

The @Podera Electronic Registry of Authorisations is the central register, governed by the aforementioned Ministerial Order HAP/1637/2012. Under this Order, it is managed by the Ministry of Territorial Policy and Public Function, through the Secretariat of State for Public Function, with the General Secretariat of Digital Administration.

Under Ministerial Order HAP/1637/2012, Mandates in the @Podera register are added through one of the following procedures:

- a) Through the Internet, through the use of the identification and authentication systems supported by Law 11/2007. In this case, the inscription of the Mandate must be made by means of standardised forms in Annex I of the Order, except when using a notarial legitimated signature.
- b) By personal appearance of the principal in Spanish citizen service offices, again using standardised forms and including the signatures of the Mandator and the proxy. The request will be recorded in the Common Electronic Registry and registered in the electronic Registry of Powers of Attorney by the official. The Mandate will take effect as of this registration.
- c) A Mandate by means of a public document or private document with a notarial authenticated signature, presented in an office attached to the Registry.

Under Article 6.3 of the Act, any eMandate entries made in the general and specific electronic records must contain, at least, the following information:

- a) Name and surnames or the name or business name, national identity document, tax identification number or equivalent document of the principal.
- b) Name and surname or the name or business name, national identity document, tax identification number or equivalent document of the proxy.
- c) Date of registration.
- d) Period of time for which the Power is granted.
- e) Type of Power according to the Powers granted.

On the latter point (“Type of Power”), the Law specifies that three different types of Powers are recognised:

- a) A general Mandate allowing the Mandatee to act on behalf of the Mandator **in any administrative action and before any administration.**
- b) A Mandate for the Mandatee to act on behalf of the Mandator in any administrative action **before a specific administration or organisation.**
- c) A Mandate for the Mandatee to act on behalf of the Mandator **only in specific procedures** specified in the Power of Attorney.

Limitations can thus be defined in terms of body or in terms of procedure. The form of these Mandates (including a typology of limitations of Powers) is set out in the Ministerial Order HAP/633/2017⁹¹.

The mandatory provisions under the law are thus relatively generic, with the exception of the reference to Spain’s national identification numbers. Interoperability is also mandatory by law 39/2015 (article 6)⁹²: “The general and specific electronic registries of Powers belonging to each

⁹¹ <https://www.boe.es/buscar/doc.php?id=BOE-A-2017-7719>

⁹² <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565>

and every one of the Administrations must be fully interoperable with each other, so as to guarantee their interconnection, computer compatibility, as well as the electronic transmission of the requests, writings and communications”. There is a web service to query any kind of Powers registered in the central information system.

The Powers within specific registries only have legal effects in the administrations in charge of the specific registry. As specified in Article 15.3 of Royal Decree 1671/2009⁹³, the registry of Mandates allows “Ministries and public bodies linked or dependent on the General Administration of the State that subscribe to it, to verify the representation held by those who act electronically before them on behalf of third parties”.

The Powers registered in the registries have a maximum validity of five years from the date of registration. At any time before the end of that period, the principal may revoke or extend the Mandate, with extensions having again a maximum validity of five years from the date of their registration.

With respect to **judicial eMandates**, there is only one registry which is accessed by all the Courts, although the law permits specific courts to set up separate registries. No other public administration is entitled to access this registry. As with the general administrative eMandates, there is a legal obligation of interoperability, as well as a statement of mandatory contents of eMandates and types of Power, and a maximum duration. These are identical to those of the administrative eMandates described above (with the exception of the duration of time, which is not mandatory for judicial eMandates). In addition, with respect to creation of the eMandates, the law notes that the Mandate is “granted by electronic appearance in the corresponding electronic judicial court, making use of the electronic signature systems provided for in this Act, or by personal appearance before the court clerk of any judicial office”. Thus, creation via electronic means requires an electronic signature supported by the Law. Under article 14 of the Law, this allows the following types: (a) electronic signatures created via the National Identity Document, for individuals; (b) advanced electronic signature systems, including those based on recognised electronic certificates, admitted by public administrations; and (c) other electronic signature systems admitted under the terms and conditions determined in each case by the competent administration.

Finally, with respect to **notarial eMandates**, these are regular contractual Mandates which have been witnessed by a public notary. Contractual Mandates are generally governed by articles 1709 and following of the Civil Code⁹⁴. The Civil Code is flexible, allowing Mandates to be express or tacit, written or oral. Acceptance of a Mandate is required, but this too may be express or tacit, including by deduction from the acts of the proxy. It follows that Mandates can also be concluded electronically, without specific requirements of form; although electronically signed Mandates and Mandates concluded before public notaries (an “escritura pública” - public deed) are of course easier to prove. Such notarial eMandates are stored in a central register. For these too, interoperability is mandatory by Law 39/2015, and there is a web service to query any kind of Powers registered in the notarial information system for eMandates.

⁹³ <https://www.boe.es/buscar/doc.php?id=BOE-A-2009-18358>

⁹⁴ <https://boe.es/buscar/act.php?id=BOE-A-1889-4763&p=20170629&tn=1#tix-2>

Comparative analysis: commonalities and differences

When examining the legal frameworks in each of the six examined MS (Austria, Belgium, Finland, the Netherlands, Portugal and Spain) in relation to eMandates, several common trends can be observed.

As the most obvious common element, in each of these MS one or more specific laws have been created **to establish official and authentic databases of Powers of Representation** for one or more of the use cases under examination in this study. These databases are **the only legally recognised sources of Mandate information on which the targeted public administrations may base themselves**.

To state this more pragmatically: Powers of Representation are only legally recognised as permissible in use cases where they originate from these databases. **Mandates from other MS would not be acceptable for the simple reason that they do not originate from the legally recognised databases**. This implies that, unless the legal frameworks are substantially revised, the only viable approach to support cross-border Mandates in these specific use cases would be **to facilitate the porting of Mandate information from foreign information sources into the local databases**.

The main drivers behind this choice seem to be the need **to ensure the reliable identification of Mandate holders and Mandate givers**, for which exclusively **national means of identification** (national identification numbers) are used; and the need to ensure that the Mandate information is reliably stored, for which **trusted administrations** are designated.

The databases in question are generally only accessible to and intended for the targeted public sector administrations, with the notable exceptions of Finland, which has a more open system in place; and Portugal, which allows the use of electronic means of identification from other Member States which have been notified in accordance with the eIDAS Regulation. With respect to the genesis of these databases, it is interesting to observe that one of two situations generally occurs: **either a generic Mandate system is set up which is gradually broadened** to more and more use cases (which is the situation in Austria, Finland and Portugal); **or an application specific system is set up which is then applied in other contexts after it has proven its merits** (which is the case in Belgium and the Netherlands, whose systems respectively originate in social security and taxation administration). The Spanish case is somewhat atypical, since it has both generic legislation for Mandates towards public administrations, and sector-specific Mandates for the justice sector.

However, it should not be overlooked that, in addition to these more specific laws, each MS also reports the existence of a **general contract law** that allows Mandate contracts to be concluded. On this point, none of the MS report barriers to the creation or use of electronic Mandates: **there are no requirements in relation to form, procedures (e.g. no requirement for the mandatory use of specific types of electronic signatures), or storage in any particular database**. However, while such eMandates are usable between private entities, Mandates towards public administrations would generally need to adhere to the more specific legislation described above.

TABLE 7: COMPARATIVE ANALYSIS OF LEGAL FRAMEWORK IMPACTING eMANDATE SYSTEMS

	AT	BE		FI	NL		ES	PT
	EMS	SSM	MAHIS	E SUOMI	DigiD	eHerkenn ing	@Podera	SCAP

National law?								
	YES	NO	NO	YES	NO	NO	YES	YES
Sector-specific law?								
	NO	NO	YES	NO	YES	YES	YES	NO
New law to come?								
	NO	NO	NO	NO	YES	YES	NO	NO

4. CONCLUSIONS OF THE DESK RESEARCH

Commonalities

- All analysed MS have developed operational eMandate systems.
- Most MS have developed or are willing to develop a **centralised system** that would be connected to the **national eID scheme** and that would be **available for all public service applications**. The level of centralisation and the scope of available business cases vary between the analysed MS.
- All types of persons and representations are covered by these systems.
- The identification data comes from the citizens and business **registries** (national identification systems).
- The process is always **fully digital**.
- Finland has a law for digital preservation that would be specific for eMandates. The rest of the MS keep permanently available logs on eMandate transactions.

Differences

- MS differ on **the information sources where the eMandates are stored and can be retrieved from**. Some MS set up a generic eMandate register, while other MS use the existing base registries for citizens and companies, and others use the eMandate system managers' or the public service applications' local databases. In any case, those Mandate sources are defined by law.

Cross-border scenarios

- **Practically none of the MS have tackled the cross-border usage of eMandates**, because of the inherent complexities (except pilot projects between Finland and Estonia, and the Netherlands and Belgium).
- No common/harmonised cross-border vocabulary or data model is currently used between MS, except UMM&DS.
- Very few common/harmonised vocabularies exist at the national level, for one sector or cross-sector interoperability scenarios (Spain, Finland).

5. ANNEXES

ANNEX I – LIST OF PUBLIC SERVICES APPLICATIONS

ANNEX II – LIST OF BUSINESS CASES

ANNEX III – LIST OF USE CASES

ANNEX IV – ONLINE QUESTIONNAIRE ANSWERS

5.1. Annex I – Lists of public services applications

This annex displays the list of public service applications that are connected to the different eMandate systems in the six MS analysed. These lists are the ones transmitted by the experts interviewed and are not necessarily exhaustive lists.

For MS where the eMandate system is fully integrated to the eID system, eMandates are available for all eGovernment services, which makes it difficult to provide with an exhaustive list of public services applications.

Austria

The electronic Mandates in Austria **can be used on every public service online application** that uses the Austrian eID solution. For this reason, it is very difficult to obtain an exhaustive list of service providers and service applications which support eMandates.

Nevertheless, a **“list of Mandate profiles”** published on the Austrian eMandate services describes the different generic and pre-defined types of Mandates⁹⁵:

- The section "Unterstützte Profilgruppen" contains predefined sets of single Mandate profiles
- Mandate profiles for natural or legal persons are listed in section "Unterstützte Einzelprofile"
 - The profile "GeneralvollmachtBilateral" is the generic Mandate profile for natural persons that allows a representative to use any type of eGovernment services.
 - The profile "Einzelvertretungsbefugnis" is the generic Mandate profile that allows a single natural person to represent a legal person for any type of eGovernment services.
- Mandate profiles for public servants are listed in section "Unterstützte Profile für Organwalter und berufsmäßige Parteienvertreter" (for professional representation by notary, lawyers and certain types of civil engineers, or by official authorised to represent citizens).

The sector-specific or service-specific pre-defined Mandates are:

- Access to the e-Health Records
- Applications of the Data Protection Authority
- Services of the Chamber of Commerce.

In addition, “bilateral Mandates” can be established with arbitrary content.

Mandates can range from universal rights to arbitrary limitations. Some of the pre-defined Mandates have implicit constraints. For example, an e-Health Record Mandate can only be used on the e-Health application, or a statutory representative assumes universal rights unless specifically constrained.

Currently, the use of eMandates is limited to public sector bodies. An amendment of the legal basis in 2017 extends the use to the private sector, and its implementation is ongoing –

⁹⁵ <https://vollmachten.stammzahlenregister.gv.at/mis/>

eMandates are now available for some **private service applications related to electronic delivery**, but this extension has not yet been completed.

Belgium

List of public service applications for SSM

Proxy Type	E-service (FPS Finances)	What ?	Giver – Taker authorised couples
Tax-on-web PB	Tax-on-web	Tax Declaration National civilians	civilian - enterprise
Tax-on-web BNI	Tax-on-web	Tax Declaration Foreign civilians	civilian - enterprise
Biztax	Biztax	Tax Declaration (National and Foreign) Enterprises,	enterprise - enterprise enterprise - civilian
Btw/VAT	Intervat	VAT-Declaration	enterprise - enterprise enterprise - civilian
Myminf	MyMinfin	Civilians Personal dossier for FPS Finances	civilian - enterprise
Finprof	Finprof	Payroll Tax Declaration	enterprise - enterprise
Geschillen	Workflow Geschillen	Filing Complaints / Appeals	civilian – enterprise enterprise - enterprise
Geschillen Advocaat	Workflow Geschillen	Acces to Complaints dossier	civilian – enterprise (advocaat) enterprise - enterprise (advocaat)

MAHIS – Groupe d’applications (IN FRENCH)

Groupes d'applications (V1.0, 2015)

Applications du groupe DmfA - DIMONA

Identifiant	Nom	Description
ARTICLE17	ARTICLE17 - Déclaration d'exonération de cotisations sociales.	Déclaration électronique pour l'exonération de cotisations sociales dans les secteurs public et socioculturel ainsi que dans le cadre de manifestations sportives (Article 17)
CAPELO	CAPELO - Compléments au Dossier de Carrière du personnel fédéral.	Ce service en ligne permet d'introduire ou modifier les données de complément au dossier de carrière ou les données historiques

CAPELODHG	CAPELO - Données Historiques	Formulaire de déclaration des données historiques de carrière pour les agents du secteur public.
COVA	COVA - Consultation du fichier "Vacances"	Consulter les données de vacances des travailleurs qui reçoivent leur pécule de vacances de l'ONVA. (pécule de vacances, durée, etc.)
DIMONA	DIMONA - La déclaration immédiate de l'emploi	Ce service permet à l'employeur de communiquer toute les entrées et les sorties de service d'un travailleur à l'ONSS ou à l'ORPSS.
PFREQ	PFREQ - Consultation fichier du personnel - batch	Ce service permet de consulter en batch, le fichier du personnel
DMFA	DMFA - Déclaration multifonctionnelle	Par cette déclaration, l'employeur transmet électroniquement les données de salaire et de temps de travail relatives à ses travailleurs.
DMFAUPD	DMFAUPD - Déclaration de modification Dmfa	Modifications d'une déclaration DMFA.
DMFAREQ	DMFAREQ - Consultation DMFA batch	Ce service permet de consulter les déclarations DMFA en Batch par un expéditeur habilité.
ECARO	ECARO - Consulter des données de l'Onem liées aux réductions de cotisations	Ce service en ligne permet aux employeurs et leurs Mandataires de consulter des données de l'Onem liées aux réductions de cotisations
ELOPLUS	Dossier interruption de carrière et crédit-temps	Ce service en ligne permet aux employeurs et aux travailleurs du secteur privé et des administrations publiques fédérales d'introduire une demande d'interruption de carrière ou de crédit-temps.
FOT2DELEGATE	FOT2DELEGATE - Mesures pour l'emploi	Ce service permet de vérifier si une entreprise peut recevoir des avantages ou des primes suite à l'engagement d'un nouveau travailleur.
MEP	LIMOSA - Déclaration obligatoire	Ce service permet de faire une déclaration Limosa, elle doit être remplie dans le cas où vous chargez un employeur ou un indépendant étranger d'une mission temporaire.
MOB-SURVEY	MOB-SURVEY - Enquête de mobilité	Les enquêtes de mobilité permettent de récolter les données sur : les lieux de résidence de vos travailleurs, leurs déplacements domicile-travail et leurs déplacements professionnels
PAYIT	PAYIT - Consultation factures employeurs	Ce service en ligne permet aux secrétariats sociaux agréés de rechercher et de consulter les factures que l'ONSS a délivrées pour un employeur affilié.
REDCORQ	DMFA - Demande de consultation des déductions	Demande de consultation de la dernière situation des déductions d'une déclaration multifonctionnelle
TRILLIUM	Trillium - Aperçu annuel des mesures en faveur de l'emploi	Consulter l'aperçu annuel des mesures en faveur de l'emploi (auparavant repris dans le Bilan social)

WIDE	WIDE - Identification, modification ou suppression de la qualité d'un employeur	L'application WIDE permet à une entreprise ou à son Mandataire de identifier un employeur auprès de l'ONSS, d'adapter ses données signalétiques ou de supprimer la qualité de cet employeur.
------	---	--

Applications et scénarios du groupe DRS Chômage

Identifiant	Nom	Description
CTW	CTW - Chômage temporaire	Ce service en ligne permet à l'employeur d'introduire une demande de chômage temporaire pour un ou plusieurs employé(s) et de consulter ensuite la décision prise par l'ONEM.
VBLV001	VBLV001 - Livre de validation	Dans le livre de validation électronique, l'employeur peut inscrire le numéro du formulaire de contrôle C 3.2 A en cas de chômage temporaire pour causes économiques et intempéries.
Scénario 1	WECH001 - Déclaration de fin du contrat de travail ou de chômage avec complément d'entreprise / Preuve de travail	Via cette déclaration, l'employeur transmet les données pour fixer le droit aux allocations de chômage complet ou de chômage avec complément d'entreprise. Cette déclaration contient une rubrique "mini-DmfA(PPL)" via laquelle l'employeur communique les données de temps de travail pour les déclarations trimestrielles ONSS ou ORPSS non encore acceptées ou introduites.
Scénario 2	WECH002 - Déclaration constat du droit au chômage temporaire ou à la suspension employés	Via cette déclaration, l'employeur transmet les données pour fixer le droit aux allocations ainsi que le montant journalier.
Scénario 3	WECH003 - Déclaration de début de travail à temps partiel.	Via cette déclaration l'employeur transmet, à la demande du travailleur, les données nécessaires pour déterminer si le travailleur peut bénéficier du statut de travailleur à temps partiel avec maintien des droits et/ou s'il peut bénéficier de l'allocation de garantie de revenus.
Scénario 5	WECH005 - Déclaration mensuelle d'heures de chômage temporaire ou de suspension employés	Via cette déclaration l'employeur communique notamment le nombre d'heures pendant lesquelles le travailleur a été en chômage au cours du mois.
Scénario 6	WECH006 - Déclaration mensuelle de travail à temps partiel pour le calcul de l'allocation de garantie de revenus.	Via cette déclaration l'employeur transmet les données nécessaires pour calculer l'allocation de garantie de revenus (AGR) et la payer au travailleur qui remplit les conditions réglementaires.
Scénario 7	WECH007 - Déclaration mensuelle de travail en tant que travailleur occupé dans un atelier protégé	Via cette déclaration l'employeur transmet mensuellement au secteur chômage les données requises pour calculer le montant de l'allocation

		du travailleur moins-valide occupé dans un atelier protégé.
Scénario 8	WECH008 - Déclaration mensuelle de travail dans le cadre d'un programme d'activation	Via cette déclaration l'employeur transmet les données requises pour le calcul et le paiement de l'allocation d'activation.
Scénario 9	WECH009 - Déclaration pour l'octroi du droit aux vacances jeunes ou seniors	Via cette déclaration l'employeur transmet les données requises pour vérifier si le jeune ou le travailleur âgé a droit à, respectivement, des vacances jeunes ou des vacances seniors, et pour déterminer le montant journalier de l'allocation.
Scénario 10	WECH010 - Déclaration mensuelle d'heures de vacances jeunes ou seniors	Via cette déclaration l'employeur communique le nombre d'heures de vacances par mois. Sur cette base, le secteur chômage calcule et paie l'allocation.

Scénarios du groupe DRS Indemnités

Identifiant	Nom	Description
Scénario 1	ZIMA001 - Feuille de renseignements	Déclaration en cas d'incapacité de travail, de repos de maternité, d'écartement complet ou partiel du travail en cas de protection de maternité, de congé de paternité et de congé d'adoption. - Scénario avec mini-dmfa
Scénario 2	ZIMA002 - Déclaration mensuelle en cas de reprise d'un travail adapté	Déclaration mensuelle en cas de reprise d'un travail adapté dans le courant d'une période d'incapacité de travail, d'exercice d'un travail adapté dans le cadre d'une mesure de protection de la maternité et de poursuite d'une activité chez un des deux employeurs....
Scénario 3	ZIMA003 - Attestation en vue de l'indemnisation des pauses d'allaitement	L'employeur communique les données permettant de déterminer le montant des indemnités à allouer pour les heures de pauses d'allaitement prises au cours du mois écoulé.
Scénario 5	ZIMA005 - Déclaration annuelle de vacances	L'employeur communique les données qui permettent d'appliquer la règle de refus des indemnités pour les jours couverts par un pécule de vacances ou une rémunération.
Scénario 6	ZIMA006 - Déclaration de reprise du travail	Via ce scénario l'employeur est invité à communiquer la date à laquelle le travailleur a repris le travail après la fin du risque social.
Scénario 7	AADD001 - Formulaire de demande	Ce formulaire électronique contient une demande de déclaration de risque social ; vous y trouvez entre autres, le type de déclaration demandée

		ainsi que l'identification de l'assuré social concerné.
--	--	---

Scénarios du groupe DRS Accidents du travail

Identifiant	Nom	Description
Scénario 1	AOAT001 - Déclaration d'un accident du travail	Via cette déclaration l'employeur a la possibilité de communiquer électroniquement à son assureur toutes les informations de la déclaration d'accident du travail.
Scénario 2	AOAT002 - Rapport mensuel	Via cette déclaration l'employeur peut introduire ses débours (salaire garanti, pertes salariales) auprès de son assureur en vue d'obtenir leur remboursement.
Scénario 3	AOAT003 - Déclaration de la reprise de travail	Cette déclaration est seulement possible lorsqu'une déclaration électronique d'accident de travail (Scénario 1) a été envoyée auparavant. Elle doit être faite lorsque la victime reprend le travail
Scénario 4	AOAT004 - Déclaration d'un accident grave de travail à l'inspection du travail	Via cette déclaration l'employeur peut effectuer la déclaration immédiate d'un accident grave aux services chargés de la surveillance du Bien-être au travail du SPF Emploi, travail et concertation sociale via le portail de la sécurité sociale.

Groupe attribué d'office à chaque Mandataire

Identifiant	Nom	Description
DESTHA	DESTHA - Gestion des règles d'expédition (DRS-Indemnités)	Permet aux employeurs et aux Mandataires sociaux de modifier les règles d'expédition définies initialement pour l'envoi des informations depuis l'extranet vers les destinataires.
FOLLOWIT	FOLLOWIT - Consultation suivi déclarations DRS	Grâce à Followit, vous pouvez effectuer une recherche sur vos déclarations DRS des 6 derniers mois, qu'elles aient été introduites via web ou par batch.
MAHIS	MAHIS - Historique des Mandats	Gestion et consultation des Mandats que vous avez délivrés en rapport avec la sécurité sociale.
RIP	RIP - Fichier du Personnel	Consultation du fichier du personnel

WREP	WREP - Consultation du répertoire des employeurs	La consultation du répertoire des employeurs met à votre disposition les informations que l'employeur a communiquées à l'ONSS ou à l'ORPSS.
------	--	---

Finland

- a) Registry-based verification for underage children (parents representing their children)
- OmaKanta (Patient Data Repository) <http://www.kanta.fi/>
 - Regional health services, seven regions <https://www.hyvis.fi/>
 - United Medix Laboratories http://www.yml.fi/index.php?set_lang=en (private company)
 - Pilot projects regarding the regional and health and social services reform in Finland (cities of Jyväskylä and Tampere)
 - Parastapalvelua (<https://parastapalvelua.fi>), online service for selecting public services provided by municipalities, includes 16 cities
 - Virttu.fi (<http://www.sosiaalikallega.fi/virttu.fi/>), regional (Lapland) virtual social and healthcare centre
 - <https://omasote.kainuu.fi/>, health services of Kainuu region
- b) Registry-based verification for the right to act on behalf of a company
- Business Finland online <https://www.businessfinland.fi/en/for-finnish-customers/online-services/>
 - Ilmoitin.fi (<https://www.ilmoitin.fi/webtamo/sivut/Esittelysivu?kieli=en>) Tax services for companies in Finland
 - Finnish Transportation Safety Agency <https://asiointi.trafi.fi/en/web/asiointi/organisaatiot> , digital services for companies
 - Suomi.fi (national portal), companies' register information and upcoming Messages service for companies
 - Palkka.fi (<https://www.palkka.fi/>), online salary payments etc.
 - SuoraTyö <https://www.suoratyo.fi/>, recruiting, salary payment etc. Private company
 - National services for companies in all regions <https://sahkoinenasiointi.ahtp.fi/fi/palvelut>
 - e-services for companies (<https://oma.yrityssuomi.fi/>), linked to Suomi.fi), tools for business planning
 - <https://hakupalvelu.tyomarkkinatori.fi/en> National Job Board
- c) Digital authorisation based on e-authorisations registry (person-person, company-person, company-company, person-company)
- <https://enterfinland.fi/eServices> for employers to handle immigration issues online
 - National Archive, e-services
 - Regional health services of Etelä-Savo: <https://www.essote.fi/ota-yhteyttasahkoisesti/>
 - NettiRassi <https://www.nettirassi.fi/> Social and healthcare services in Raahen area
 - Healthcare services for Oulu region <https://www.oulunomahoito.fi/>
 - <https://www.metsaan.fi/>, e-services for forest owners, national service

5.2. Annex II – Lists of business cases

Belgium

List of SSM business cases

NAME	DOMAIN	BUSINESS CASE
Tax-on-web PB	Finance	Submit a private (citizen) tax declaration
Tax-on-web BNI/NP	Finance	Submit a private (citizen) tax declaration as a non-resident
VTA	Finance	Submit VTA-declarations
BIZTAX	Finance	Submit a corporate tax declaration
MYMINFIN	Finance	Get access to a citizen personal tax file (consult personal documents, introduce demands, ...)
CONTENTIOUS MATTERS	Finance	Citizens / companies introduce an appeal concerning fiscal matters
FINPROF	Finance	Submit declarations of payroll taxes
INSURABILITY	E-Health	Healthcare providers mass consultation insurability status of patients / citizens with the public health insurance services
THIRD PARTY INVOICING	E-Health	Healthcare providers submit certificate of medical care with the public health insurance services to obtain reimbursement
MEDATTEST	E-Health	Healthcare providers submit E-attest with the public health insurance services
MEDADMIN	E-Health	Submit medical administration documents with the public health insurance services

UPCOMING

TRANSFERMYDBP2	Social Security	Empowers a private company (bank or insurance) (Mandatee) to access and upload data from a social security database holding data concerning legal and supplementary pension insurance, for its clients (Mandators)
E705	Customs	Declare an imported vehicle to obtain an electronic signal 705 with customs
KIS-SIC	Customs	Introduce a customs authorisation request for general import
BEPS13	Finance	Submit transfer pricing documents
RV	Finance	Submit declarations withholding taxes
CONTENTIOUS MATTERS LAWYER ONLY		Empowers the lawyer (Mandatee) defending a pursuant to access an entire file concerning a specific appeal /lawsuit

List of business cases for MAHIS

Main use case

A company (legal responsible) can give a social secretariat or payroll professional a Mandate for performing formalities (for that company) concerning the social security sector.

Sub use cases

Via the MAHIS application, the company can give a social secretariat or payroll professional a Mandate to use specific applications (within the social security sector):

- Registering a company as an employer with the NSSO (application WIDE);
- Sending the following declarations (social security sector) to:
 - Applications/databases managed by NSSO: Dimona, DmfA, Limosa, etc. These databases register employer-employee relations (Dimona-Limosa), the work performed, and salaries of employees (DmfA).
 - Databases managed by other institutions in the social security sector
- ASR (declaration of social risks that may give rights to benefits)
 - (Temporary) unemployment of an employee
 - Workplace accidents
 - ...
- Consulting these databases

Recent/future non-social security sector use cases (MAHIS)

- A company (legal responsible) can give a social secretariat or payroll professional a Mandate for sending information concerning mobility to the federal institution of mobility (Belgium) (already in production)⁹⁶
- A company (legal responsible) can give a social secretariat or payroll professional a Mandate for applying (for the company) for regional (Flanders) employment subsidies/incentives (future implementation)⁹⁷

Identifiant	Nom FR	Description FR
AOAT-LIGHT	AOAT-LIGHT - DRS Accidents du travail (Hirundo)	Application utilisée dans le cadre du contrôle d'accès Hirundo pour les DRS Accidents du travail
AOAT001	AOAT001 - Déclaration d'un accident du travail	Pour les accidents ayant entraîné une incapacité temporaire d'une durée inférieure à quatre jours, il est possible de faire une déclaration d'accident du travail simplifiée. Toute déclaration d'accident de travail doit être déclarée dans le délais de 8 jours à compter du jour de l'accident.
AOAT002	AOAT002 - Rapport mensuel	Cette déclaration doit être faite lorsqu'il y a eu au moins une déclaration électronique d'accident de travail pendant le mois de référence (Scénario 1). Elle doit être faite au début du mois qui suit celui auquel les informations se rapportent
AOAT003	AOAT003 - Déclaration de la reprise de travail	Cette déclaration est seulement possible lorsqu'une déclaration électronique d'accident de travail (Scénario 1) a été envoyée auparavant. Elle doit être faite lorsque la victime reprend le travail
AOAT004	AOAT004 - Déclaration d'un accident grave de travail à l'inspection du travail	Déclaration d'un accident grave de travail à l'inspection du travail. Elle doit être faite dans le délai de huit jours à compter du jour de l'accident.
AWI	AWI - Incitation au recrutement pour les demandeurs d'emploi à long terme	Avec les incitations au recrutement des demandeurs d'emploi de longue durée, le gouvernement flamand souhaite rendre le recrutement et l'emploi durable pour les demandeurs d'emploi de longue durée plus attratifs financièrement pour les employeurs et promouvoir aussi les possibilités d'emploi pour les demandeurs depuis plus de deux ans.
CAPELO	CAPELO - Compléments au Dossier de Carrière	L'application Capelo permet d'introduire ou modifier les données de complément au dossier de carrière ou les données historiques
CAPELODHG	CAPELO - Données Historiques	Formulaire de déclaration des données historiques de carrière pour les agents du secteur public.
COTRQ	COTRQ - Demande de chômage économique secteur non-construction	Application permettant aux employeurs et à leurs Mandataires de connaître le nombre de jour de chômage économique non-construction pris en compte dans le calcul de la cotisation « chômage économique »

⁹⁶ https://dt.bosa.be/en/over_fedict/realisaties/Mobiliteitsenquete

⁹⁷ <https://www.werk.be/online-diensten/aanwervingsincentive-voor-langdurig-werkzoekenden>

COVA	COVA - Fichier vacances	Consulter les données de vacances des travailleurs (pécule de vacances, durée, etc.)
CTW	CTW - Chômage temporaire	Introduction période de chômage temporaire des travailleurs.
DB2P	DB2P - Déclaration base de données pensions complémentaires	Consultation d'une partie des données déclarées par l'assureur et déclaration/consultation du plan de pension interne propre à l'entreprise
DIMONA	DIMONA - La déclaration immédiate de l'emploi	Message électronique par lequel l'employeur communique les entrées et les sorties de service de son personnel.
DMFA	DMFA - Déclaration multifonctionnelle	Par cette déclaration, l'employeur transmet électroniquement les données de salaire et de temps de travail relatives à ses travailleurs.
DMFANOTI	DMFANOTI - Notifications DMFA	Notifications DMFA
DMFAREQ	DMFAREQ - Demande de consultation DMFA	Demande de consultation de la dernière situation d'une déclaration multifonctionnelle
DMFAUPD	DMFAUPD - Déclaration de modification Dmfa	Modifications d'une déclaration DMFA.
ECARO	ECARO - Consulter des données de l'Onem liées aux réductions de cotisations	Consulter des données de l'Onem liées aux réductions de cotisations
ECARORQ	ECARORQ - Ecaro request	Demande de consultation données ONEM concernant les déductions d'un travailleur
ELOPLUS	ELOPLUS - Interruption de carrière et crédit-temps	Introduction de la demande interruption de carrière par le citoyen/travailleur et par l'employeur
FOT2DELEGATE	FOT2DELEGATE - Mesure pour l'emploi	Vérifier s'il existe des avantages ou des primes auxquels un employeur peut prétendre lors de l'engagement d'un nouveau travailleur
GOTOT	Travailler à l'étranger	Applications concernant le travail à l'étranger
MEP	MEP - Déclaration obligatoire (Limosa)	Enregistrer une mission temporaire d'un étranger en Belgique (Limosa)
MINIDMFA	Mini-Dmfa	Mini DMFA dans le cadre de la demande DRS Indemnité
MINIDMFA-LIGHT	MINIDMFA-LIGHT - Mini-dmfa	Application utilisée dans le cadre du contrôle d'accès Hirundo pour les DRS Indemnités avec mini-dmfa Application utilisée dans le cadre du contrôle d'accès Hirundo pour les DRS Indemnités avec mini-dmfa
MOB-SURVEY	MOB-SURVEY - Enquête de mobilité	Les enquêtes de mobilité permettent de récolter les données sur : les lieux de résidence de vos travailleurs, leurs déplacements domicile-travail et leurs déplacements professionnels

PAYIT	PAYIT - Consultation factures employeurs	Ce service en ligne permet aux Mandataires de rechercher et de consulter les factures que l'ONSS a délivrées pour un employeur affilié.
PFREQ	PFREQ - Demande de consultation du fichier du personnel	Demande de consultation de masse du fichier du personnel
PROACTIVITY	Proactivité - Retours des Mandataires vers l'ONSS	Ce service en ligne permet au Mandataire de donner du feedback en ce qui concerne les actions prises vis à vis des employeurs affiliés dans le cadre de la proactivité.
PUBLIATO	PUBLIATO - Accident du travail dans le secteur public	Déclaration des accidents du travail survenus dans le secteur public et réglés dans le cadre de la loi sur les accidents du travail du 3 juillet 1967.
REDCORQ	DMFA - Demande de consultation des déductions	Demande de consultation de la dernière situation des déductions d'une déclaration multifonctionnelle
RIP	RIP - Fichier du Personnel	Consultation du fichier du personnel
TRILLIUM		Trillium - Aperçu annuel des mesures en faveur de l'emploi
VBLV001	VBLV001 - Livre de validation	Dans le livre de validation électronique, l'employeur peut inscrire le numéro du formulaire de contrôle C 3.2 A en cas de chômage temporaire pour causes économiques et intempéries.
VOP	VOP - Prime de soutien flamande	Prime pour un employeur qui recrute ou a recruté une personne handicapée professionnelle dans le but de favoriser l'intégration des personnes handicapées dans la vie active.
WECH-LIGHT	WECH-LIGHT - DRS Chômage (Hirundo)	Application utilisée dans le cadre du contrôle d'accès Hirundo pour les DRS Chômage
WECH001	WECH001 - Déclaration de fin de contrat de travail ou prépension à temps plein / Preuve de travail	Cette déclaration doit être effectuée immédiatement, au plus tard le dernier jour de travail. Il s'agit d'une déclaration ponctuelle (fin de contrat de travail suite à un licenciement ou démission ou bien à une prépension). - avec mini-DMFA
WECH002	WECH002 - Déclaration constat du droit au chômage temporaire ou à la suspension de crise employés	Déclaration ponctuelle traitée pour une même occupation avec l'employeur. Les causes du chômage temporaire constituent les sous risque de la déclaration.
WECH003	WECH003 - Déclaration de début de travail à temps partiel avec maintien des droits	Déclaration ponctuelle qui doit être réalisée dès qu'un contrat de travail à temps partiel est conclu et à chaque diminution de la durée de travail convenue.
WECH005	WECH005 - Déclaration mensuelle d'heures de chômage temporaire ou de suspension de crise employés	Cette déclaration doit être réalisée après la fin du mois au cours duquel des heures effectives de chômage temporaire ou suspension de crise employés sont survenues. Les causes du chômage temporaire constituent les sous risque de la déclaration.

WECH006	WECH006 - Déclaration mensuelle de travail à temps partiel	Cette déclaration s'effectue à la fin de chaque mois calendrier pour lequel le travailleur ou l'enseignant à temps partiel concerné est susceptible de percevoir une allocation de garantie de revenu (AGR).
WECH007	WECH007 - Déclaration mensuelle de travail en tant que travailleur occupé dans un atelier protégé	Cette déclaration s'effectue à la fin de chaque mois. L'employeur transmet mensuellement au secteur chômage les données requises pour calculer le montant de l'allocation du travailleur moins-valide occupé dans un atelier protégé.
WECH008	WECH008 - Déclaration mensuelle de travail dans le cadre d'un programme d'activation	La déclaration mensuelle dans le cadre d'un programme d'activation s'effectue à l'issue de chaque mois au cours duquel le travailleur concerné était occupé dans un des programmes d'activation.
WECH009	WECH009 - Déclaration pour l'octroi du droit aux vacances jeunes ou seniors	Les vacances jeunes et seniors ne peuvent être prises que pendant une occupation comme salarié et après l'épuisement des vacances rémunérées ordinaires. Il s'agit d'une déclaration ponctuelle qui doit être réalisée lorsque le travailleur le demande.
WECH010	WECH010 - Déclaration mensuelle d'heures de vacances jeunes ou seniors	Cette déclaration doit être réalisée pour la première fois le même mois que celui pour lequel on a fait une déclaration pour l'octroi du droit aux vacances jeunes ou seniors (scénario 9).
WIDE	WIDE - Identification employeur	L'application WIDE permet à une entreprise ou à son Mandataire de l'identifier auprès de l'ONSS.
WREP	WREP - Consultation du répertoire des employeurs	La consultation du répertoire des employeurs met à votre disposition les informations que l'employeur a communiquées à l'ONSS.
ZIMA-LIGHT	ZIMA-LIGHT - DRS Indemnités (Hirundo)	Application utilisée dans le cadre du contrôle d'accès Hirundo pour les DRS Indemnités
ZIMA001	ZIMA001 - Feuille de renseignements	Déclaration en cas d'incapacité de travail, de repos de maternité, d'écartement complet ou partiel du travail en cas de protection de maternité, de congé de paternité et de congé d'adoption. - Scénario avec mini-dmfa
ZIMA002	ZIMA002 - Déclaration mensuelle en cas de reprise d'un travail adapté	Déclaration mensuelle en cas de reprise d'un travail adapté.
ZIMA003	ZIMA003 - Attestation en vue de l'indemnisation des pauses d'allaitement	L'employeur communique les données permettant de déterminer le montant des indemnités à allouer pour les heures de pauses d'allaitement prises au cours du mois écoulé.
ZIMA005	ZIMA005 - Déclaration annuelle de vacances	L'employeur communique les données qui permettent d'appliquer la règle de refus des indemnités pour les jours couverts par un pécule de vacances ou une rémunération.
ZIMA006	ZIMA006 - Déclaration de reprise du travail	Via ce scénario l'employeur est invité à communiquer la date à laquelle le travailleur a repris le travail après la fin du risque social.
ZIMAMINID MFA	Mini-Dmfa	Mini DMFA dans le cadre de la demande DRS Indemnité

PAYIT	PAYIT - Consultation factures employeurs	Ce service en ligne permet aux Mandataires de rechercher et de consulter les factures que l'ONSS a délivrées pour un employeur affilié.
PFREQ	PFREQ - Demande de consultation du fichier du personnel	Demande de consultation de masse du fichier du personnel
PROACTIVITY	Proactivité - Retours des Mandataires vers l'ONSS	Ce service en ligne permet au Mandataire de donner du feedback en ce qui concerne les actions prises vis à vis des employeurs affiliés dans le cadre de la proactivité.
PUBLIATO	PUBLIATO - Accident du travail dans le secteur public	Déclaration des accidents du travail survenus dans le secteur public et réglés dans le cadre de la loi sur les accidents du travail du 3 juillet 1967.
REDCORQ	DMFA - Demande de consultation des déductions	Demande de consultation de la dernière situation des déductions d'une déclaration multifonctionnelle
RIP	RIP - Fichier du Personnel	Consultation du fichier du personnel
TRILLIUM		Trillium - Aperçu annuel des mesures en faveur de l'emploi
VBLV001	VBLV001 - Livre de validation	Dans le livre de validation électronique, l'employeur peut inscrire le numéro du formulaire de contrôle C 3.2 A en cas de chômage temporaire pour causes économiques et intempéries.
VOP	VOP - Prime de soutien flamande	Prime pour un employeur qui recrute ou a recruté une personne handicapée professionnelle dans le but de favoriser l'intégration des personnes handicapées dans la vie active.
WECH-LIGHT	WECH-LIGHT - DRS Chômage (Hirundo)	Application utilisée dans le cadre du contrôle d'accès Hirundo pour les DRS Chômage
WECH001	WECH001 - Déclaration de fin de contrat de travail ou prépension à temps plein / Preuve de travail	Cette déclaration doit être effectuée immédiatement, au plus tard le dernier jour de travail. Il s'agit d'une déclaration ponctuelle (fin de contrat de travail suite à un licenciement ou démission ou bien à une prépension). - avec mini-DMFA
WECH002	WECH002 - Déclaration constat du droit au chômage temporaire ou à la suspension de crise employés	Déclaration ponctuelle traitée pour une même occupation avec l'employeur. Les causes du chômage temporaire constituent les sous risque de la déclaration.
WECH003	WECH003 - Déclaration de début de travail à temps partiel avec maintien des droits	Déclaration ponctuelle qui doit être réalisée dès qu'un contrat de travail à temps partiel est conclu et à chaque diminution de la durée de travail convenue.
WECH005	WECH005 - Déclaration mensuelle d'heures de chômage temporaire ou de suspension de crise employés	Cette déclaration doit être réalisée après la fin du mois au cours duquel des heures effectives de chômage temporaire ou suspension de crise employés sont survenues. Les causes du chômage temporaire constituent les sous risque de la déclaration.

WECH006	WECH006 - Déclaration mensuelle de travail à temps partiel	Cette déclaration s'effectue à la fin de chaque mois calendrier pour lequel le travailleur ou l'enseignant à temps partiel concerné est susceptible de percevoir une allocation de garantie de revenu (AGR).
WECH007	WECH007 - Déclaration mensuelle de travail en tant que travailleur occupé dans un atelier protégé	Cette déclaration s'effectue à la fin de chaque mois. L'employeur transmet mensuellement au secteur chômage les données requises pour calculer le montant de l'allocation du travailleur moins-valide occupé dans un atelier protégé.
WECH008	WECH008 - Déclaration mensuelle de travail dans le cadre d'un programme d'activation	La déclaration mensuelle dans le cadre d'un programme d'activation s'effectue à l'issue de chaque mois au cours duquel le travailleur concerné était occupé dans un des programmes d'activation.
WECH009	WECH009 - Déclaration pour l'octroi du droit aux vacances jeunes ou seniors	Les vacances jeunes et seniors ne peuvent être prises que pendant une occupation comme salarié et après l'épuisement des vacances rémunérées ordinaires. Il s'agit d'une déclaration ponctuelle qui doit être réalisée lorsque le travailleur le demande.
WECH010	WECH010 - Déclaration mensuelle d'heures de vacances jeunes ou seniors	Cette déclaration doit être réalisée pour la première fois le même mois que celui pour lequel on a fait une déclaration pour l'octroi du droit aux vacances jeunes ou seniors (scénario 9).
WIDE	WIDE - Identification employeur	L'application WIDE permet à une entreprise ou à son Mandataire de l'identifier auprès de l'ONSS.
WREP	WREP - Consultation du répertoire des employeurs	La consultation du répertoire des employeurs met à votre disposition les informations que l'employeur a communiquées à l'ONSS.
ZIMA-LIGHT	ZIMA-LIGHT - DRS Indemnités (Hirundo)	Application utilisée dans le cadre du contrôle d'accès Hirundo pour les DRS Indemnités
ZIMA001	ZIMA001 - Feuille de renseignements	Déclaration en cas d'incapacité de travail, de repos de maternité, d'écartement complet ou partiel du travail en cas de protection de maternité, de congé de paternité et de congé d'adoption. - Scénario avec mini-dmfa
ZIMA002	ZIMA002 - Déclaration mensuelle en cas de reprise d'un travail adapté	Déclaration mensuelle en cas de reprise d'un travail adapté.
ZIMA003	ZIMA003 - Attestation en vue de l'indemnisation des pauses d'allaitement	L'employeur communique les données permettant de déterminer le montant des indemnités à allouer pour les heures de pauses d'allaitement prises au cours du mois écoulé.
ZIMA005	ZIMA005 - Déclaration annuelle de vacances	L'employeur communique les données qui permettent d'appliquer la règle de refus des indemnités pour les jours couverts par un pécule de vacances ou une rémunération.
ZIMA006	ZIMA006 - Déclaration de reprise du travail	Via ce scénario l'employeur est invité à communiquer la date à laquelle le travailleur a repris le travail après la fin du risque social.
ZIMAMINID MFA	Mini-Dmfa	Mini DMFA dans le cadre de la demande DRS Indemnité

Finland

TABLE 8: EXAMPLES OF BUSINESS CASES IN FINLAND

Mandate category	Mandate code	Description of presentation Powers
Immigration and emigration		
	Work-based immigration	With this Mandate, the Mandatee can manage notifications concerning residence permit applications and supervision of work on behalf of the Mandator.
Information services		
	Ordering information on an adoption case	With this Mandate, the Mandatee can order information on a specific adoption case on behalf of the Mandator.
	Ordering vehicle information	With this Mandate, the Mandatee can order information on a specific vehicle on behalf of the Mandator.
	Ordering information on a prenuptial agreement	With this Mandate, the Mandatee can order information on a specific prenuptial agreement on behalf of the Mandator.
	Ordering information on a divorce	With this Mandate, the Mandatee can order information on a specific divorce on behalf of the Mandator.
	Ordering information on a home birth	With this Mandate, the Mandatee can order information on a specific home birth (such as the exact time of birth) on behalf of the Mandator.
	Ordering a school certificate or diploma	With this Mandate, the Mandatee can order a specific school certificate or diploma on behalf of the Mandator.
	Ordering property title registration documents	With this Mandate, the Mandatee can order specific property title registration documents on behalf of the Mandator.
	Ordering an estate inventory deed	With this Mandate, the Mandatee can order a specific estate inventory deed on behalf of the Mandator.
	Ordering a Defence Administration identity document	With this Mandate, the Mandatee can order a Defence Administration identity document on behalf of the Mandator.

	Ordering information on wartime child evacuees	With this Mandate, the Mandatee can order information on specific Finnish wartime child evacuees on behalf of the Mandator.
	Ordering a report of family relationships	With this Mandate, the Mandatee can order a specific report of family relationships on behalf of the Mandator.
Earned income		
	Reporting pay data	This Mandate allows the Mandatee to complete the following pay data-related actions on behalf of the Mandator: <ul style="list-style-type: none"> - maintain the Mandator's basic data and pay data reports - submit pay data reports produced by the Mandator - request reports on the Mandator - send messages This Mandate also contains the Mandate to browse pay data.
	Browsing pay data	This Mandate allows the Mandatee to browse the following pay data: <ul style="list-style-type: none"> - the Mandator's basic data - pay data reports produced by the Mandator - reports on the Mandator - messages sent and received by the Mandator - the Mandator's archived documents
	Processing income data	This Mandate allows the Mandatee to do the following on behalf of the Mandator: <ul style="list-style-type: none"> - browse income data - send messages related to income data - request income data reports - maintain contact details related to income data
	Processing salary information	With this Mandate, the Mandatee can on behalf of the Mandator: <ul style="list-style-type: none"> - submit salary information - pay salaries and employer contributions - send notifications
Benefits		
	Submitting benefit data reports	This Mandate allows the Mandatee to complete the following benefit data-related actions on behalf of the Mandator: <ul style="list-style-type: none"> - maintain the Mandator's basic data and benefit data reports - submit benefit data reports produced by the Mandator

		<ul style="list-style-type: none"> - request reports on the Mandator - send messages <p>This Mandate also contains the Mandate to browse benefit data.</p>
	Browsing benefit data	<p>This Mandate allows the Mandatee to browse the following benefit data:</p> <ul style="list-style-type: none"> - the Mandator's basic data - benefit data reports produced by the Mandator - reports on the Mandator - messages sent and received by the Mandator - the Mandator's archived documents
Forest, water and mineral resources		
	Invitations to tender for forest management and timber sales	<p>This Mandate allows the Mandatee to submit an invitation to tender for forest management and/or timber sales on behalf of the Mandator.</p>
	Accepting tenders for forest management and timber sales	<p>This Mandate allows the Mandatee to accept or reject tenders related to forest management and timber sales on behalf of the Mandator.</p>
	Processing of forest resources data	<p>This Mandate allows the Mandatee to do the following on behalf of the Mandator:</p> <ul style="list-style-type: none"> - browse the Mandator's forest data - draw up a notification of forest use - draw up documents related to forest management and forest improvement aids (e.g. Kemera) - send a service notification
	Signing a timber sales and forest management agreement	<p>This Mandate allows the Mandatee to sign a timber sales and forest management agreement based on the selected tender on behalf of the Mandator.</p>
Healthcare		
	Managing matters related to healthcare	<p>This Mandate gives the Mandatee the authority to act on behalf of the Mandator in healthcare services. The Mandatee may:</p> <ul style="list-style-type: none"> - view the information on the Mandator's state of health - make and change healthcare appointments - submit and receive information on the Mandator's state of health
Job seeking and jobs		

	Management of job advertisements	This Mandate allows the Mandatee to create, view, modify and remove a job advertisement on behalf of the Mandator.
	Examination of jobseeker information and contacting applicants	This Mandate allows the Mandatee to view jobseeker information and contact jobseekers on behalf of the Mandator.
	Updating the description of a job provider	This Mandate allows the Mandatee to update the information of the job provider, including contact details for recruitment, the text of the marketing description, and the logo of the job provider on behalf of the Mandator.
Natural resources, animals and plants		
	Export and import certificates for animals, food products and animal-based and plant-based products	With this Mandate, the Mandatee may provide the information required for the export and import certificates for live animals, food products, and animal-based and plant-based products on behalf of the Mandator.
Property maintenance		
	Viewing property maintenance information	With this Mandate, the Mandatee can on behalf of the Mandator view the information related to the maintenance services of a property, including costs (e.g. energy, water and waste information).
	Maintaining information related to property maintenance services	With this Mandate, the Mandatee can on behalf of the Mandator change the information related to the maintenance services of a property within the limits of service-specific restrictions.
Taxation		
	Managing tax affairs	With this Mandate, the Mandatee can manage the Mandator's tax affairs and access the Mandator's tax information. This includes: <ul style="list-style-type: none"> - An organisation's tax affairs - A private sector entrepreneur's personal and business-related tax affairs - An individual's personal tax affairs
	Filing of tax returns and other reports	With this Mandate, the Mandatee can file tax returns and other reports related to managing tax issues on behalf of the Mandator.

Work and unemployment		
	Viewing information on unemployment insurance contributions	With this Mandate, the Mandatee can view information on unemployment insurance contributions and training compensations.
	Maintaining information on unemployment insurance contributions	With this Mandate, the Mandatee can maintain information on unemployment insurance contributions and training compensations.
Business operations		
	Preparation, planning and development of business activities	With this Mandate, the Mandatee can manage the information needed in the preparation, planning and development of business activities on behalf of the Mandator.

5.3. Annex III – Lists of use cases

Belgium

List of use cases - SSM

For SSM, all of the following use cases are identical for each business case:

- Mandate consultation by Mandator or Mandatee
- Mandate consultation by civil servant (typical : helpdesk operator)
- Download results of a search by Mandator or Mandatee or civil servant
- Mandate creation by Mandator
- Mandate creation by Mandatee
- Mandate creation by civil servant (no signature of counterparty needed)
- Counterparty accepting/signing a Mandate (as Mandator or as Mandatee)
- Counterparty accepting / signing Mandates in bulk (as Mandator or as Mandatee)
- Mandate revocation by Mandator or Mandatee
- Mandate revocation by civil servant
- Modify Mandate end date as Mandator or Mandatee
- Modify Mandate end date as civil servant
- Obsolete Mandate Reactivation by Mandator or Mandatee (this is in fact a simplified creation)
- Obsolete Mandate Reactivation by civil servant (no signature of counterparty needed)
- Bulk creation of Mandates by Mandatee
- Bulk revocation of Mandates by Mandatee
- Bulk transfer of Mandates by Mandatee (in case of bankruptcy, cessation or merger of activities)
- Bulk transfer of Mandates by civil servant
- Enlarge Mandate between two parties to another domain by Mandatee or Mandator (this is in fact a simplified creation)
- New Mandate type creation by civil servant administrator
- New Mandate type activation by civil servant administrator
- New Mandate type deactivation by civil servant administrator
- Mandate type modification by civil servant administrator
- System validation of a newly created or modified Mandate
- System validation of file for mass creation of Mandates

Spain

As Mandator:

- Create
- Revoke
- Modify the validity period
- Consult

As Mandatee:

- Accept Powers
- Renounce

- Consult

In addition, the systems automatically perform the following actions:

- Expire (when the validity period ends)
- Cancel (when the Power has not been accepted by the Mandatee within the established period).

5.4. Annex IV – Online questionnaire answers

Austria

Do you have a system for eMandates in place?

Yes

What are the eMandate roles in your national information system (e.g. Mandator, Mandatee, witness, archiver, etc.)?

- Representative (Mandatee)
- Mandator
- Intermediary (optional, if representation gets delegated to further representatives)

What are the main types of eMandates (e.g. civil general Mandate, commercial general Mandate, special Mandate, individual Mandate, etc.)?

A list of pre-defined Mandates is available at <https://vollmachten.stammzahlenregister.gv.at/mis/>

The main (general) pre-defined types are:

- General representation (e.g. statutory representation of a legal entity like by a CEO)
- Procuracy
- Postal Mandate
- Professional representatives (lawyers, notaries, civil engineers) or official authorised to represent citizens

Service-specific or sector-specific pre-defined Mandates are:

- Access to the E-Health Record
- Applications to the Data Protection Authority
- Services of the Chamber of Commerce

In addition, bilateral Mandates can be established with arbitrary content.

What are the possible rights/privileges associated to each type of eMandate (the Mandatee has universal right to represent the Mandator, Mandatee's rights are limited to certain types of acts, Mandatee's rights are limited only to one or more individual acts, etc.)?

Mandates can range from universal rights to arbitrary limitations. Some pre-defined constraints like duration of transaction limits are defined. Note, that some of the pre-defined Mandates mentioned above have implicit constraints (e.g. an E-Health Record Mandate can only be used in this application, or a general representation by a statutory representative assumes universal rights unless specifically constrained).

What are the supported actions on eMandates (e.g. create, cancel, transfer, etc.)?

A distinction between statutory representatives (registered in an authoritative source), delegates Mandates (a statutory representative delegates rights e.g. to staff), and bilateral Mandates are to be made:

- For statutory Mandates, the Mandate is retrieved on-the-fly whenever it is used in an application. Its lifecycle is determined by the authoritative source (i.e. an electronic Mandate can be used from the very moment a legal representative gets entered to the authoritative source like a Company Register; this is independent of whether the representative holds an eID).
- For bilateral Mandates, the Mandator can create and revoke a Mandate. Creation is through eID-based Web access to a Mandate Register (this access requires the Mandator to hold an active eID). The representative gets informed of a Mandate have been created (like by email). The representative does not need to hold an eID when the Mandate gets created (but needs an eID when the Mandate gets used).

Depending on the case, delegated Mandates get registered in the Mandate Register or can be defined in the Austrian Business Service Portal. Like with bilateral Mandates, the lifecycle contains creation, use and revocation.

When a Mandate is used in a service, the representative uses her eID when authenticating to the service and all the registers mentioned above (authoritative sources like the Company Register or the Register of Associations, the Mandate Register, and the Business Service Portal) are queried to obtain fresh information of the representations and associated Powers of the representative (the representative selects one Mandate, if several representations are found).

Who has access and can use the information about Powers and Mandates stored in your information system (e.g. all public sector bodies, only some public sector bodies, public sector bodies and private companies, etc.)?

Initiation of using a Mandate at a service is always by the representative when accessing a service that supports authentication on behalf. The representative ticks an “authentication on behalf” button when authentication to a service (i.e. Web application) and selects the Mandate to use (e.g. if several Mandates exist). The service receives the Mandate as part of the authentication assertion (an additional Attribute in the SAML assertion).

Currently, the use of electronic Mandates is limited to public sector bodies. An amendment of the legal basis in 2017 extends the use to the private sector. Its implementation is ongoing but hasn't been completed yet.

The Mandator always has access to the Mandate lifecycle processes (create, inspect, and revoke).

Mandators and representatives can inspect when a Mandate has actually been used (and at what service)

Do you have a vocabulary of Representation Powers and Mandates at national level?

Yes

If you have a vocabulary, is the vocabulary developed for machine-readable descriptions of Representation Powers and Mandates (i.e. as structured data)? Or are the descriptions in a format that is non-machine-readable (e.g. narrative in PDFs)?

Electronic Mandates are structured XML data (migrating the Mandate content to Attributes of the SAML assertion is planned, but not yet implemented). Frequent Mandate types are indicated by an object identifier (OID) listed at <https://vollmachten.stammzahlenregister.gv.at/mis/>). The XML specification contains the main constraints needed by applications (like transaction limits or validity periods). In addition to pre-defined types and constraints, arbitrary limitations can be included (free text areas. Such arbitrary constraints, if included, usually need also manual inspection).

If you have a vocabulary, how do you model Power and Mandates from a semantic point of view? Does your data model use specific Attributes such as classes and properties, controlled vocabularies to facilitate the understanding of the Power and Mandates statements? Is your data model represented in a specific format?

Frequently used data is modelled in the XML scheme, standard Mandate types are indicated by specific OIDs. To remain flexible, further OIDs can be introduced, or the free-text areas allow for specific cases.

If you do not have a vocabulary, how do you foresee dealing with the interoperability of eMandates?

National interoperability is supported through agreeing to the specification through the Austrian eGovernment cooperation platforms (Digital Austria).

International interoperability is lacking an agreed semantic model. We would envision that such a model starts with a set of basic Mandates covering the most frequent cases. It should be developed in a way that those few states that already have structured Mandates can do a semantic mapping.

Which type of interactions does your vocabulary cover (e.g. natural person acting on behalf of a legal person, legal person acting on behalf of a legal person, etc.)?

Arbitrary cases are supported and used. I.e., a natural person can represent a natural or a legal person, as well as a legal person can represent a natural person or a legal person (plus cases of professional representation that can have specific representation rights; or cases where Mandates can further get delegated (e.g. a company Mandating a law firm, a lawyer in the law firm Mandating a clerk))

Do you have more than one information source on Representation Powers and Mandates (e.g. information sources at regional or state level)?

No

If you have more than one information source, are they interoperable?

N/A

How do you make (or plan to make) them interoperable?

N/A

If you have multiple information sources but they are not interoperable, how do they exchange information?

N/A

What challenges would keep your information sources from achieving cross-border interoperability with other Member States' information sources?

If no other MS would – under eIDAS – notify legal person eID or representation; vice versa if no other MS would accept representation in their services broadly (in a non-ad-hoc way). In both cases, an interoperability effort would be pointless.

In relation to Powers and Mandates, which authorisation systems are used in your national information system (e.g. an open-source software component, an ad-hoc solution, etc.)?

The electronic Mandate system is an integral part of the eID building block “MOA-ID” that relying parties anyhow use when supporting eID. I.e., using Mandates is basically a matter of configuration of the national eID building block.

What legal, organisational, semantic and/or technical challenges can you foresee regarding the integration of cross-border eMandates in your national information system?

For universal rights, the current eIDAS Attribute profile already serves the purpose.

However, given the actual use of Mandates in sector-specific services (like E-Health Record) semantic mappings would be needed.

A further challenge might be given due to just few MS currently having experience with structured Mandates. A way forward might be that these MS join forces in gaining experience in cross-border use.

Czech Republic

Do you have a system for eMandates in place?

No

What are the eMandate roles in your national information system (e.g. Mandator, Mandatee, witness, archiver, etc.)?

We do not have central system for eMandates, but public administration systems needs to work with Mandates like Parent, Mandator, statutory person, guardian, lawyer, healthcare professional, etc.

What are the main types of eMandates (e.g. civil general Mandate, commercial general Mandate, special Mandate, individual Mandate, etc.)?

Civil general Mandate (parent, guardian, etc.), commercial general Mandate (statutory person), special Mandate (healthcare professional), individual Mandate (Power of Attorney).

What are the possible rights/privileges associated to each type of eMandate (the Mandatee has universal right to represent the Mandator, Mandatee's rights are limited to certain types of acts, Mandatee's rights are limited only to one or more individual acts, etc.)?

The Mandatee has universal right to represent the Mandator, Mandatee's rights are limited to certain types of acts, and Mandatee's rights are limited only to one or more individual acts.

What are the supported actions on eMandates (e.g. create, cancel, transfer, etc.)?

Create, cancel, extend, manage, and refuse.

Who has access and can use the information about Powers and Mandates stored in your information system (e.g. all public sector bodies, only some public sector bodies, public sector bodies and private companies, etc.)?

- Owner of Mandate with the usage of electronic identity (according to eIDAS)
- Mandatee
- Public administration with right to access according to special legislation

Do you have a vocabulary of Representation Powers and Mandates at national level?

No

If you have a vocabulary, is the vocabulary developed for machine-readable descriptions of Representation Powers and Mandates (i.e. as structured data)? Or are the descriptions in a format that is non-machine-readable (e.g. narrative in PDFs)?

All only according to general and special legislation

If you have a vocabulary, how do you model Power and Mandates from a semantic point of view? Does your data model use specific Attributes such as classes and properties, controlled

vocabularies to facilitate the understanding of the Power and Mandates statements? Is your data model represented in a specific format?

All only according to general and special legislation

If you do not have a vocabulary, how do you foresee dealing with the interoperability of eMandates?

All only according to general and special legislation

Which type of interactions does your vocabulary cover (e.g. natural person acting on behalf of a legal person, legal person acting on behalf of a legal person, etc.)?

All only according to general and special legislation

Do you have more than one information source on Representation Powers and Mandates (e.g. information sources at regional or state level)?

Yes

If you have more than one information source, are they interoperable?

Yes

How do you make (or plan to make) them interoperable?

With the usage of eGovernment Online Service Bus and exchange of data through services.

If you have multiple information sources but they are not interoperable, how do they exchange information?

From the source of civil registry (parent, legal capacity) with the help of eGovernment services of Base registries. Others unknown.

What challenges would keep your information sources from achieving cross-border interoperability with other Member States' information sources?

- Legislation
- Definition of LoA between MSs
- GDPR, ePrivacy

In relation to Powers and Mandates, which authorisation systems are used in your national information system (e. g. an open-source software component, an ad-hoc solution, etc.)?

Identification as authentication is provided by National Identity Authority (NIA) from different Identity providers.

Next there are few central authorisation system for different roles like JIP/KAAS for clerks or NRZP for healthcare professionals.

What legal, organisational, semantic and/or technical challenges can you foresee regarding the integration of cross-border eMandates in your national information system?

- Legislation
- Definition of LoA between MSs
- GDPR, ePrivacy

Portugal

Do you have a system for eMandates in place?

Yes

What are the eMandate roles in your national information system (e.g. Mandator, Mandatee, witness, archiver, etc.)?

We have the Mandator, Mandatee, Attribute provider and service provider.

What are the main types of eMandates (e.g. civil general Mandate, commercial general Mandate, special Mandate, individual Mandate, etc.)?

The main type of e-Mandates is the commercial general Mandate, limited to certain types of acts.

What are the possible rights/privileges associated to each type of eMandate (the Mandatee has universal right to represent the Mandator, Mandatee's rights are limited to certain types of acts, Mandatee's rights are limited only to one or more individual acts, etc.)?

Mandatee's rights may be:

- Universal right to represent the Mandator,
- Limited to certain types of acts
- Limited only to one or more individual acts.

What are the supported actions on e-Mandates (e.g. create, cancel, transfer, etc.)?

The supported actions are creation, usage and revocation.

Who has access and can use the information about Powers and Mandates stored in your information system (e.g. all public sector bodies, only some public sector bodies, public sector bodies and private companies, etc.)?

Comercial Mandates must be registered on the website ww.procuracoesonline.mj.pt with public open access. Powers and Mandates are stored by the entity responsible for updating the Attributes in cause.

Do you have a vocabulary of Representation Powers and Mandates at national level?

Yes

If you have a vocabulary, is the vocabulary developed for machine-readable descriptions of Representation Powers and Mandates (i.e. as structured data)? Or are the descriptions in a format that is non-machine-readable (e.g. narrative in PDFs)?

Yes. It is structured into Attributes and sub-Attributes.

If you have a vocabulary, how do you model Power and Mandates from a semantic point of view? Does your data model use specific Attributes such as classes and properties, controlled

vocabularies to facilitate the understanding of the Power and Mandates statements? Is your data model represented in a specific format?

Attributes and sub-Attributes.

If you do not have a vocabulary, how do you foresee dealing with the interoperability of e-Mandates?

N/A

Which type of interactions does your vocabulary cover (e.g. natural person acting on behalf of a legal person, legal person acting on behalf of a legal person, etc.)?

Natural person acting on behalf of a legal person, any other Attributes or Powers.

Do you have more than one information source on Representation Powers and Mandates (e.g. information sources at regional or state level)?

Yes

If you have more than one information source, are they interoperable?

N/A

How do you make (or plan to make) them interoperable?

We have SCAP (professional Attributes certification system). For legal persons, when using SCAP, there is only one source.

If you have multiple information sources but they are not interoperable, how do they exchange information?

N/A

What challenges would keep your information sources from achieving cross-border interoperability with other Member States' information sources?

Legal and data protection challenges

In relation to Powers and Mandates, which authorisation systems are used in your national information system (e.g. an open-source software component, an ad-hoc solution, etc.)?

Citizen Card (Cartão de Cidadão) and Digital Mobile Key (Chave Móvel Digital)

What legal, organisational, semantic and/or technical challenges can you foresee regarding the integration of cross-border e-Mandates in your national information system?

The legal challenges of European Union cross-border integration of e-Mandates will be settled under the eIDAS Regulation (Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market).

Spain

Do you have a system for eMandates in place?

Yes

What are the eMandate roles in your national information system (e.g. Mandator, Mandatee, witness, archiver, etc.)?

- Mandator: Could be a natural or legal person.
- Mandatee: Could be a natural or legal person.
- Witness: public officer or notary that witness the act of creating a Mandate. In the case of administrative and judicial Powers they can be made without a witness through the electronic website of the administration (Administrative Mandates⁹⁸, Judicial Mandates⁹⁹), electronic identification and signature of the Mandator and the Mandatee will be necessary. For notarial Powers appearing in person is mandatory.
- Legal Service of the Administration: The Legal Service of the Administration guarantees sufficiency of Powers when the Mandator or the Mandatee is a legal person, to verify that the person acting as the company's Mandatee has "sufficient Power" to create or accept new Powers.
- Processor: Public officer or software that consults the Power during the processing of a procedure.
- Manager of Powers of an organisation: The procedures can be grouped into categories, which are groups of procedures that allow a single operation to grant a global Power for all of them. The grouping of procedures is determined by the Manager of Powers of an organisation.
- Representative ("compareciente"): Only for judicial Powers. The representative would be the person submitting the documents related to a Mandate, in the name of the Mandator.

What are the main types of eMandates (e.g. civil general Mandate, commercial general Mandate, special Mandate, individual Mandate, etc.)?

Types of eMandates are:

98

https://sede.administracion.gob.es/PAG_Sede/ServiciosElectronicos/RegistroElectronicoDeApoderamientos.html

99

https://sedejudicial.justicia.es/sje/publico/sjepublico/tramites_y_servicios/detalle_servicio/!ut/p/a0/04_Sj9CPyKssy0xPLMnMz0vMAfGjzOLdLVyMPPy9Dbz8Lc0tDRy9XXzNgwJ9jQxMTPQLsh0VAR5jKLQ!/?itemId=266711&categoria=Servicios&tags

- a. *Administrative eMandates*, regulated by Law 39/2015¹⁰⁰, Royal Decree 668/2015 (art.15)¹⁰¹, Ministerial order HAP/1637/2012¹⁰². These Mandates are stored in two types of registries:
- General eMandate registries: State government, regional governments and local governments.
 - Specific eMandate registries: Tax Agency, Social Security, Department of Traffic.
- d) *Judicial eMandates*, regulated by Law 18/2011¹⁰³. There is only one registry for these Mandates.
- e) *Mandates of notaries*, regulated by the Civil Code¹⁰⁴. There is only one registry for these Mandates.

What are the possible rights/privileges associated to each type of eMandate (the Mandatee has universal right to represent the Mandator, Mandatee's rights are limited to certain types of acts, Mandatee's rights are limited only to one or more individual acts, etc.)?

1. *Administrative eMandates*: Types of administrative eMandates are regulated by Law 39/2015 (article 6)¹⁰⁵:

- f) A general Power for the Mandatee to act on behalf of the Mandator in any administrative act and before any Administration.
- g) A Power for the Mandatee to act on behalf of the Mandator in any administrative act before a specific Administration or Organisation, as:
- State government.
 - Autonomous Communities (regional governments).
 - Local Entities (local governments).
 - Public bodies.
 - Other institutions.
- h) A Power for the Mandatee to act on behalf of the Mandator only to carry out one or several specific procedures specified in the eMandate.

2. *Judicial eMandates*: Types of judicial eMandates are regulated by Law 18/2011 (article 32bis)¹⁰⁶:

- i) A general Power for the Mandatee to act on behalf of the Mandator in any judicial procedure.

¹⁰⁰ <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a6>

¹⁰¹ <https://www.boe.es/buscar/doc.php?id=BOE-A-2015-8048>

¹⁰² <https://boe.es/buscar/act.php?id=BOE-A-2017-7719>

¹⁰³ <http://www.boe.es/buscar/act.php?id=BOE-A-2011-11605&p=20151006&tn=1#a32bis>

¹⁰⁴ <https://boe.es/buscar/act.php?id=BOE-A-1889-4763&p=20170629&tn=1#tix-2>

¹⁰⁵ <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a6>

¹⁰⁶ <http://www.boe.es/buscar/act.php?id=BOE-A-2011-11605&p=20151006&tn=1#a32bis>

- j) A Power for the Mandatee to act on behalf of the Mandator only to carry out specific types of judicial procedures.
- k) A specific Power for the Mandatee to act on behalf of the Mandator only to carry out a specific judicial procedure.

3. *Mandates of notaries*: Types of notarial eMandates:

- l) General Powers: The Mandator grants Powers to the Mandatee to act in all or in some areas that should be specified in the Power.
- m) Specific Powers: A Power for the Mandatee to act on behalf of the Mandator only in a specific type of legal act on which the action will fall (purchase of a property, acceptance of an inheritance, etc.).

What are the supported actions on eMandates (e.g. create, cancel, transfer, etc.)?

As Mandator:

- Create
- Revoke
- Modify the validity period.
- Consult

As Mandatee:

- Accept Powers
- Renounce
- Consult

Besides, the systems automatically perform the following actions:

- Expire (when the validity period ends)
- Cancel (when the Power has not been accepted by the Mandatee within the established period)

As a result of an action on the eMandate, it can be in one of the following status:

- Unauthorised: Need acceptance from the Mandatee.
- Authorised: Just created that does not need acceptance from the Mandatee or that has been accepted by the Mandatee.
- Expired: It has exceeded the validity period.
- Cancelled: The Mandatee has not accepted the Power within the established period.
- Renounced: The Mandatee has renounced the Power.
- Revoked: Powers revoked by the Mandator.

Who has access and can use the information about Powers and Mandates stored in your information system (e.g. all public sector bodies, only some public sector bodies, public sector bodies and private companies, etc.)?

Administrative Powers:

- General Powers: All public administrations, including State Government, Autonomous Communities, Local Entities, Tax Agency, Social Security and Department of Traffic.
- Powers to act in a specific Administration: Only the specific Administration. The Powers that are issued to act in a specific Administration (Autonomous Communities, Local

Entities, Tax Agency, Social Security or Department of Traffic) can only be consulted by the Administration in which that Power can be executed.

- Powers to act in a specific procedure: Only the competent authority in that procedure. The Powers that are issued to act in a specific procedure can only be consulted by the administration to which the procedure belongs.
- Mandator and Mandatee can consult their own Powers.

Judicial Powers: All courts can access all types of judicial Powers.

Notarial Powers: All notaries and the State Government (including Tax Agency, Social Security or Department of Traffic) can access all types of notarial Powers. These Powers can be accessed also by the Autonomous Communities and Local Entities that have signed an agreement to access these Powers.

Do you have a vocabulary of Representation Powers and Mandates at national level?

Yes

If you have a vocabulary, is the vocabulary developed for machine-readable descriptions of Representation Powers and Mandates (i.e. as structured data)? Or are the descriptions in a format that is non-machine-readable (e.g. narrative in PDFs)?

Both of them. Our vocabulary is provided as structured data to technical people, and it is provided as PDF for anonymous people, through the public eGovernment portal¹⁰⁷. However, these structure data files are intended for using within a web service that provides information about registered Powers and Mandates.

If you have a vocabulary, how do you model Power and Mandates from a semantic point of view? Does your data model use specific Attributes such as classes and properties, controlled vocabularies to facilitate the understanding of the Power and Mandates statements? Is your data model represented in a specific format?

There is a central management application for Powers and Mandates which provides a web service for queries. This web service uses two specific message types for request and response actions, respectively.

These two message types are represented in XML Schema definition language (XSD) and they use complex and simple data types, some of them within domains defined by local authoritative lists.

If you do not have a vocabulary, how do you foresee dealing with the interoperability of eMandates?

There is a web service to query any kind of Powers registered in the central information system. It is also planned to offer a new web service to record general Powers.

¹⁰⁷ <https://administracionelectronica.gob.es/ctt/rea/descargas#.WyN7RaKvzmg>

Which type of interactions does your vocabulary cover (e.g. natural person acting on behalf of a legal person, legal person acting on behalf of a legal person, etc.)?

Covers all possible interactions established by law. These are described in the first section of this questionnaire (eMandates in your national information systems), and includes natural person acting on behalf of a legal person and legal person acting on behalf of a legal person.

Do you have more than one information source on Representation Powers and Mandates (e.g. information sources at regional or state level)?

Yes

If you have more than one information source, are they interoperable?

Yes

How do you make (or plan to make) them interoperable?

Administrative eMandates: Interoperability is mandatory by law 39/2015 (article 6)¹⁰⁸: “The general and particular electronic registries of Powers belonging to each and every one of the Administrations must be fully interoperable with each other, so as to guarantee their interconnection, computer compatibility, as well as the electronic transmission of the requests, writings and communications.”.

There is a web service to query any kind of Powers registered in the central information system.

Query of other registries are not necessary as the Powers within these registries only have effects in the administrations in charge of the specific registry.

Notarial eMandates: Interoperability with notarial eMandates is mandatory by law 39/2015 (article 6)¹⁰⁹: “The general and specific eMandates registries will make it possible to prove validly the representation of those who act before the Public Administrations on behalf of a third party, by consulting other similar administrative registries, the mercantile registry, the property registry, and the notarial registry.

Mercantile registry, property registry, and notarial registry will be interoperable with general and specific eMandates registries.”

There is a web service to query any kind of Powers registered in the notarial information system for eMandates.

Judicial eMandates: There is only one registry and it is accessed by all the Courts. No other Public Administrations is entitled to access this registry.

¹⁰⁸ <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a6>

¹⁰⁹ <https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a6>

If you have multiple information sources but they are not interoperable, how do they exchange information?

Not applicable.

What challenges would keep your information sources from achieving cross-border interoperability with other Member States' information sources?

Our national information system for eMandates is already connected with other national sources of eMandates through web services, so it is prepared to interoperate with other systems. Despite this, the main challenge for the interoperability may be not having a common European vocabulary. The legal frameworks of the different MSs can make difficult to agree on a common semantic.

In relation to Powers and Mandates, which authorisation systems are used in your national information system (e. g. an open-source software component, an ad-hoc solution, etc.)?

The Spanish Mandate Management System (REA) is an ad-hoc solution. The Judicial Mandate Management System (REAJ) is also an ad-hoc solution.

What legal, organisational, semantic and/or technical challenges can you foresee regarding the integration of cross-border eMandates in your national information system?

One of the main challenges may be the lack of a common semantics. For this reason, a project between several MSs (Austria, Slovenia, Netherlands and Spain) has been proposed in the last CEF eID call.

This project aims to bridge this gap by providing solutions for cross-border Powers of Representation and eMandates by taking into account all these barriers (legal, organisational, semantic and technical). The goal is to have a harmonised definition of eMandates and to enhance the eIDAS Interoperability Framework with appropriate elements for connecting national Mandate management infrastructures.