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

USE CASES AND ARCHITECTURE

31/10/2018

Document characteristics

Deliverable name	Analysis and conclusions on existing electronic Mandate systems in the European Union – Use cases and architecture
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

LIST OF FIGURES

LIST OF TABLES

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 will have to 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 for 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 data, 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 eIdentification and eAuthentication in that system.
eCODEX	e-Justice domain enabling citizens and businesses to have cross-border access of 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 forms that the capability exchanges with other capabilities to support the execution of value streams.
eIdentification	The process of using personal 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 Mandatee has been assigned one or more Powers of a Mandator.
eMandate process requirement	Requirement that an actor must meet to be legitimately involved in an eMandate and make the Mandate valid.
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.
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.
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 a 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 in a Registry
Registry	The system where the information is stored.

Relying Party	A service provider that requires information in 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.
eMandates 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 use of electronic Representation Powers and Mandates cross-borderly, the European Commission (**DIGIT, with the support of DG CNECT**), through the ISA^2 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 Member State (MS) to be processed automatically by the information system in another MS.

Phase 1 of this Action assessed **MSs' preparedness for cross-border interoperability** of electronic Representation Powers and Mandates. **A short-list of five services** was identified as priority business cases for cross-border scenarios. Each MS'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 a feasibility criteria. Finally, a **set of twelve recommendations** were issued as next steps towards cross-border and cross-sector interoperability for eMandates.

The analysis and conclusions of the desk research on eMandate systems in selected Member States, has led to put forward a **proposal of hybrid federation**, i.e. a combination of a trust-oriented plus data-oriented architectural approach, and **the reuse of existing vocabularies** for the modelling of a flexible and expressive European Core eMandate Vocabulary.

Finally, based on the recommendations made, the report concludes with the identification of **challenges in each one of the interoperability layer** (legal, organisational, semantic, technical and governance).

The Use Cases, processes and information requirements identified during this phase (and previous phases) will be used in a subsequent **Task 02** to draft the detailed **specification** of this **European Core eMandate Vocabulary**.

2. INTRODUCTION

2.1. ISA^2 Programme Action 2016.12

In order to instigate and facilitate the use of cross-border electronic Representation Powers and Mandates , the European Commission (**DIGIT, with the support of DG CNECT**), through the ISA^2 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 system in another MS.

This ISA^2 Action builds upon and follows the results of the following previous and ongoing European initiatives[1]:

- 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 ISA^2 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] ISA^2 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

2.2.1. Short-list of MSs to be assessed

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

2.2.2. Short-list of prioritised services for cross-border RPaM

Second, a short-list of five prioritised services where cross-border Representation Powers and Mandates would be 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 to a patient's summary cross-border.

2.2.3. Assessment of AS-IS situation

Thirdly, the AS-IS situation in each MSs 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 MS's maturity across the four European Interoperability Framework's layers (legal, organisational, semantic and technical).

The overall maturity of MSs corresponds to the "applied level" (score 3), i.e. not very mature. Austria, The Netherlands, and Finland were the best-scored MSs, with respective scores of 4.3, 4.1 and 3.6.

Additional studies were made for those three pioneer MSs, to produce a detailed overview of the eMandate types, uses and information requirements. Similarities between the systems were revealed.

2.2.4. 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 Mandate cross-border was defined, with corresponding Use CaseUse CaseUse CaseUse Cases and activity diagrams.

We summarised the business cases and Use CaseUse CaseUse CaseUse Cases in the following matrix:

TABLE 1: BUSINESS CASES AND USE CASEUSE CASEUSE CASEUSE CASES MATRIX

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

			procurement		tax declaration	
Mandate's creation	Mandator authentication	x				
	Mandator identity verification	x				
	Mandate storage	x				
Mandate's 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's summary usage					x

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

text	Business cases
text	Use CaseUse CaseUse CaseUse Cases
text	Specific Use CaseUse CaseUse CaseUse Case

2.2.5. 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 10 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 MSs' existing eMandates systems:
  - Austria's Electronic Mandate Service;
  - Belgium's Self-Service Mandate;
  - The Netherlands' eHerkenning;
  - Spain's @Podera;
  - Finland's Katso interface.

2.2.6. Recommendations and next steps

Phase 1 of the ISA^2 2016.12 Action also identified **a set of 12 recommendations** that can be considered as **next steps** towards achieving cross-border and cross-sector interoperability for Representation Powers and Mandates. These aspects included, 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 to build 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 Nº1993, under framework contract Nº DI/07445.

This project is framed within **Action 2016.02 "Semantic Interoperability for Representation Powers and Mandates"** from the **Interoperability Solutions for Public Administrations ISA^2 Programme**.

The present document complements the desk research carried out on eMandate systems in selected Member States, whose analysis was presented in the deliverable "Analysis and conclusions on existing electronic mandate systems in the European Union". The proposals of Use CaseUse CaseUse CaseUse Cases, architecture, and data model are based on the knowledge gained through the desk research and on the state-of-affairs mapped.

.

The expected work results 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 MSs, 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 across 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 Service provided by a Public Administration or a Private organisation.

(Source ISA^2, "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 ISA^2, "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 describes also 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 ISA^2, "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 to a politician as a WAV file, etc.

(Source ISA^2, adapted from the definition of “eBusiness Document”).

ePower

“An eDocument that proves that a Natural Person. 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 the 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 stored in an eMandate Registry containing the necessary data for a Service Provider to allow a User the access to one or more of its Systems and use one or more Services.

(Source ISA^2, “Representation Powers and Mandates” glossary)

eMandate

“An eDocument that proves that a Mandator 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 the 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 stored in an eMandate Registry containing the assignment of Powers necessary for a Service Provider to allow a Mandatee the access to one or more of its Systems and use one or more Services.

(Source ISA^2, “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 stored.

Example: the eMandate Registry @podera in Spain.

Additional Information:

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

2.5. Methodology

2.5.1. Choice of case studies

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

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

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 MS.

In the first phase of the Action, the assessment **framework scored Austria, Finland and The Netherlands with the best interoperability scores**, out of 14 MSs. Those three MSs and their eMandate systems were also part of the **final list of 10 solutions proposed as feasible solutions meeting 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 also contains Belgian (SSM) and Spanish (@Podera) systems. Plus, the **detailed answers to the online questionnaire** confirmed that Spain could be an interesting case study. For this reason, the Belgian and Spanish systems were also analysed in this desk research.

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.

2.5.2. 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 systems and data models' Attributes for the three pioneer MSs: Austria, The Netherlands and Finland.

The business cases and Use CaseUse CaseUse CaseUse 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 can 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.

2.5.3. Methods

The desk research task was conducted through:

- An 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 amount of documents were analysed. The first documents were the **deliverables from the first phase** of the ISA^2 Action project as well as the additional documents referenced there, among others 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 the 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 the 16th May and remained open until 15th June**. Four MSs answered to the online survey: **Austria, Spain, Portugal and 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-minutes phone interviews were organised** with experts and groups of experts identified in each MS. The experts identified were, in most of the 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 to the 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 focuses cross-border interoperability experiences and challenges, and gives some recommendations that could serve as inputs for Task 02.

- Section 3.1 lists the eMandate Management Use Cases that may be necessary to include in a cross-border eMandate system;
- Section 3.2 analyses the architectural approaches adopted by four Trans-European Systems and recapitulates on the MS national solutions;
- Section 3.3 presents the possible scenarios identified for a cross-border Recognition system;
- Section 3.4 reviews the existing data models of four Trans-European Systems and of the MS analysed, and proposes the specifications of a cross-border eMandate vocabulary;
- Section 3.5 analyses the existing legal interoperability instruments that could impact a cross-border eMandate system.

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

3. CROSS-BORDER INTEROPERABILITY: EXPERIENCES AND PROPOSALS

This analysis takes place within the context of an initial task with two main objectives:

a) To develop a proposal of an eMandate Data Model (eMDM); and

a) To put forward an approach for the federation of the sources of the eMandates and related information.

The two objectives can be seen as decoupled. A specific data model should not impact the architectural proposal, and an architecture for interoperability should be able to function regardless of the business payloads being exchanged amongst the systems.

The architecture depends on the assurance that the business capabilities are available and well-coordinated. Its functioning also depends on the expected implementation and the reliability of the stakeholder business capabilities, as well as on the correct use of the generic and specific enablers and business processes, workflows and artefacts. In the end, the architecture reflects whether the **organisational interoperability** has been appropriately implemented[6].

In turn, the understanding of business processes supported by the architecture helps clarify (and elicit) the information requirements and business rules necessary to incept the data model, i.e. to ensure the **semantic interoperability**.

In this document, various proposals are presented to achieve the two objectives of the initial task: the development of an eMDM and of a federation approach. The knowledge map (K-Map) below[7] summarises the approaches, experiences and models that have been analysed to develop the basis of these proposals.

[6] See EIF's Interoperability Governance and 'European organisational interoperability vision' (ISA Action 5.2 European Interoperability Strategy Governance Support). (Not available online).

[7] Knowledge map (K-Map), see LICEF's site for a complete description of this abstract knowledge representation methodology: http://lice.licef.ca/index.php/gmot-motplus-et-mot/.

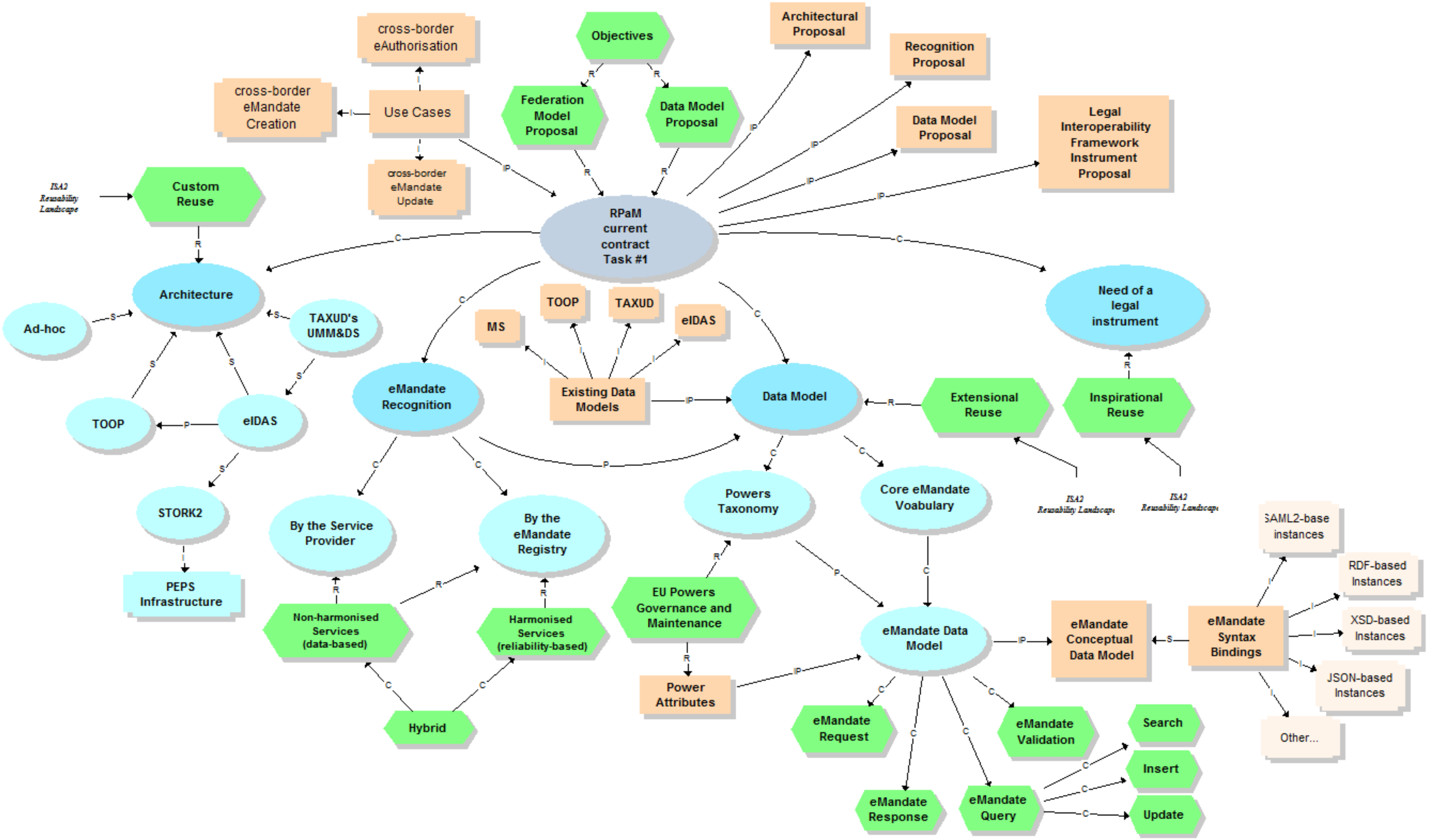


FIGURE 1: WAY FORWARD TO THE PROPOSAL OF A EUROPEAN EMANDATE SEMANTIC MODEL

One general principle/recommendation emerges reiteratively from the analysis and from interviews with the MS: reuse, reuse and reuse; either for inspiration, customisation or extension[8]. This principle will be a constant in the draft proposal put forward in this document. This proposal is organised around four topics:

b) **Architectural approaches**, for the federation of Mandate sources and related information;
a) **Recognition approaches**, about where the recognition of eMandates should lie;
b) **Data Model approach**, on how to approach the modelling of a common European eMandate Data Vocabulary;
c) **Legal Interoperability Framework approach**, listing the aspects to be taken into consideration when promoting a specific eMandate legal instrument. This instrument, or an extension of it, may refer to the three topics above as legal requirements to be taken into account by implementers.

The remainder of this chapter is organised around these four topics. For each topic, the corresponding section highlights some recent European and national experiences, presents the current challenges, and proposes principles and actions from which to start modelling a pan-European eMandate Data Model.

3.1. Cross-border interoperability

In the scope of this project, cross-border interoperability implies the exchange of information between two or more systems that are managed by public authorities or private organisations located in different countries of the European Union.

These systems offer public and private services, such as an “application for a residence permit” (public service), an “application for a certificate” (public service), “opening a bank account” (private service), “subscribing an insurance” (private), etc. Both types of services, public and private, are within the scope of this project.

In this document, the authority or organisation responsible for the provision and management of the service is named “service provider” (SP).

In general, the information that is exchanged is contained in an “eMandate”. The objective of this project is, precisely, to define the form and content that a common EU eMandate could have. Many Member States have already developed systems aimed at registering mandates at the national level. This document will analyse how these systems can be used as sources of the eMandates that are the key to accessing cross-border services.

Please note that in this document, the system that stores eMandates is called the “eMandate Registry”. We would like to convene that the term “eMandate Registry” is reserved to the system where the eMandates are stored and that the terms “Register” or “Registrar” are reserved to the “authority” responsible for the management of that system. As for any other registry, the Register must commit to the assurance of the quality and authenticity of the data stored therein.

[8] ISA2 worked intensively on the different ways of sharing and reusing. One interesting deliverable by ISA is the “Reusability Landscape” where concepts such as “usability”, “reusability”, “inspirational reusability”, etc. are introduced. See, for instance, the Access to Base Registries (ABR) Catalogue of Solutions quadrants in Joinup: https://joinup.ec.europa.eu/collection/access-base-registries/abr-catalogue-solutions.

The figure below illustrates this idea. The physical location of the user is not relevant. What is relevant is whether the SPs and the eMandate Registry are in different EU Member States and whether the user is a citizen, a resident or a registered organisation.

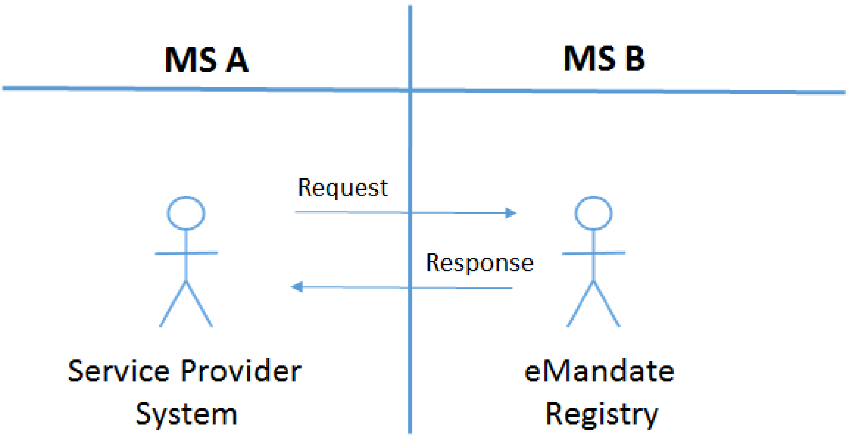


FIGURE 2: CROSS-BORDER INTEROPERABILITY

3.2. The meaning of "is in"

For the purposes of this document, and for the sake of simplicity, we use the expression "is in" (as in "the user is in MS-A") to indicate the following:

- In the case of a natural person: the person is a European citizen or is a resident of a EU Member State; (there may be other circumstances that empower the natural person, e.g. being employed in a EU MS);
- In the case of a legal person: the person, its subsidiary, branch or office is registered in a EU Member State.

This will be further used and understood in the sections below.

3.3. Harmonised and non-harmonised services

Before explaining each use case in further detail, it is important to understand that, in cross-border interoperability, the stakeholders that exchange information must always rely to a certain extent on data supplied by a third system. In our context, this system is abroad, under another MS authority. In general, trust is not a given pre-condition but is built progressively, as the result of transactions that prove valid and secure over time.

It is also necessary to distinguish between private services and public services.

3.3.1. Harmonised and non-harmonised services

If the data and services that interoperate are based on **common EU legislation and agreed processes and instruments**[9], it is possible to harmonise the services so that one MS recognises the validity and authenticity of the information provided by another MS, as if it were provided

[9] "Instrument" is used here in a broad sense, meaning ad-hoc legal and technical solutions to ensure the responsibilities and business capabilities of the stakeholders supporting the systems that interoperate.

by an authority of its own country. In the context of the European Union, this harmonisation should be possible, at least for common public administrative procedures[10]. This should build a "ring of trust" based on the responsibilities and liabilities that each stakeholder assumes when committing to interoperate. Harmonised services can be seen as services that are identical or very similar in terms of objectives, processes, inputs and outputs for all EU MS. Users should be able to access harmonised services regardless of the MS where the service is implemented, provided that the user is also in a EU MS.

Hence, it is necessary to distinguish between systems that provide "harmonised" services and those that do not.

In the first case "harmonised services", the system providing the service (the service provider, or SP) would rely on the responses supplied by one of the MS eMandate Registry belonging to the ring of trust.

In the second case, "non-harmonised services", the only possibility for the SP is to obtain data that is sufficiently detailed and of sufficient quality; and optionally, evidences supporting the authenticity and validity of that data. In this second case, trust is built over time and with the provision of technical solutions to support transactional security, data quality cross-checking, data integrity, non-repudiation, etc.

See also the section "3.13 Recognition", where these two approaches are described from the architectural and data model perspectives.

In many MS, the organisation that provides the service is the same one that owns the system; in which case, the public administration is also the service provider. But this is not true in all cases, as in some MS the public administration outsources the provision of this service to private organisations that act on its behalf.

3.3.2. Private services

In the case of services offered by private sector providers (e.g. banking or insurance-related services), "harmonised services" would correspond to private contracts or specific agreements between private organisations. For example, if a pan-European (or international) agreement is made between a bank in MS-A to rely on another bank in MS-B to identify and authenticate a user that is a client of the bank in MS-B. This agreement is even less restrictive than it would be for the public sector, as the user could be any person regardless of nationality or residence.

For the non-harmonised services (no existence of agreements between private organisations), the SP would have to recur to the verification of the authenticity of the natural person and his/her registration as a user of the service provider system. Private organisations (like banks) are moving towards the use of ICT solutions to avoid the user having to move physically in order to prove the authenticity of his/her identity. One way of doing this is by relying on the user's biometric data[11].

[10] One example could be the actions in front of public administrations described in the proposal of a Single Digital Gateway Regulation (SDGR).

[11] An internet search for "biometrics in banking" will retrieve articles similar to these: https://www.bayometric.com/biometrics-in-banking-and-finance/, https://biztechmagazine.com/article/2018/03/how-will-biometrics-affect-the-future-of-banking-security or https://blog.ipswitch.com/4-important-factors-of-biometrics-in-banking.

In the case of private services, the owner of the service is not necessarily the same organisation as the one that provides the service. For example, there may be large platforms offering the same services to many different organisations (similar to platforms specialised in building dynamic travel packages including plane tickets, hotels, restaurants, tours, etc. to different travel agencies).

3.4. The EU Powers taxonomy

The use cases described above are based on the premise that Powers are well defined and maintained by a EU governance body. For the time being, a catalogue of Powers that can be used by any EU Institution or EU public administration (national, regional or local) does not exist. One approach for the development of such a catalogue could be the implementation of a machine-readable taxonomy[12] with the following characteristics:

- The taxonomy is defined and maintained by a EU governance body which includes many different stakeholders from the public and private sectors. The maintenance of the information about specific public services would be the responsibility of each MS; which would require an ad-hoc legal instrument[13];
- Each node of the taxonomy represents a specific legal capacity (a Power). As an example of Power: “a Natural Person has the right to apply for an unemployment benefit”;
- Each Power may be linked to one or more services (especially for those that are not harmonised).
- Each Power may be linked to generic additional machine-readable constraints and information about the ePower (e.g. the ePower is only applicable to EU MS but not to EEA MS);
- Each service may in turn be linked to its specific “attributes”, i.e. the **type of data** that the services may need to interoperate cross-border[14] (e.g. “period of residence of the Natural Person”, “the company identifier, registered name and registered address for which the Natural Person worked”; etc.);
- Each service can also refer to additional machine-readable constraints and other additional information (e.g. time-window of the availability of the service provider system, location of SLAs about the service, etc.).

A technical solution for this approach will be incepted in the deliverable corresponding to Task #2 of this project, in which a data model will be developed. But some simple (high-level) examples will be provided in this document for the sake of illustration (see Use Case 1). **Bear in mind that the examples provided in this document are only for illustration purposes: the final taxonomy is very likely be significantly different**.

The figure below shows a possible organisation of this taxonomy:

[12] This solution will be further described in the deliverable corresponding to Task #2 of this project, where a proposal of a data model will be developed.

[13] One example of a similar solution would be e-Certis 2, see Article 61 of Directive 2014/24/EU (the implementation of which is currently being funded by ISA²): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0024&from=EN, https://joinup.ec.europa.eu/collection/ict-standards-procurement/eprocurement and https://ec.europa.eu/tools/ecertis/search).

[14] This refers to the “type” of data, not the actual values such as “start date: 2018-01-02; end date: 2018-12-12” and “BRIS EUID: ES-RMC-23453435-9; “ACME, Ltd.”, “Auderghem Avenue, 182; 1000 Brussels; Belgium”. The actual values are specified in the instances of messages being exchanged between the systems.

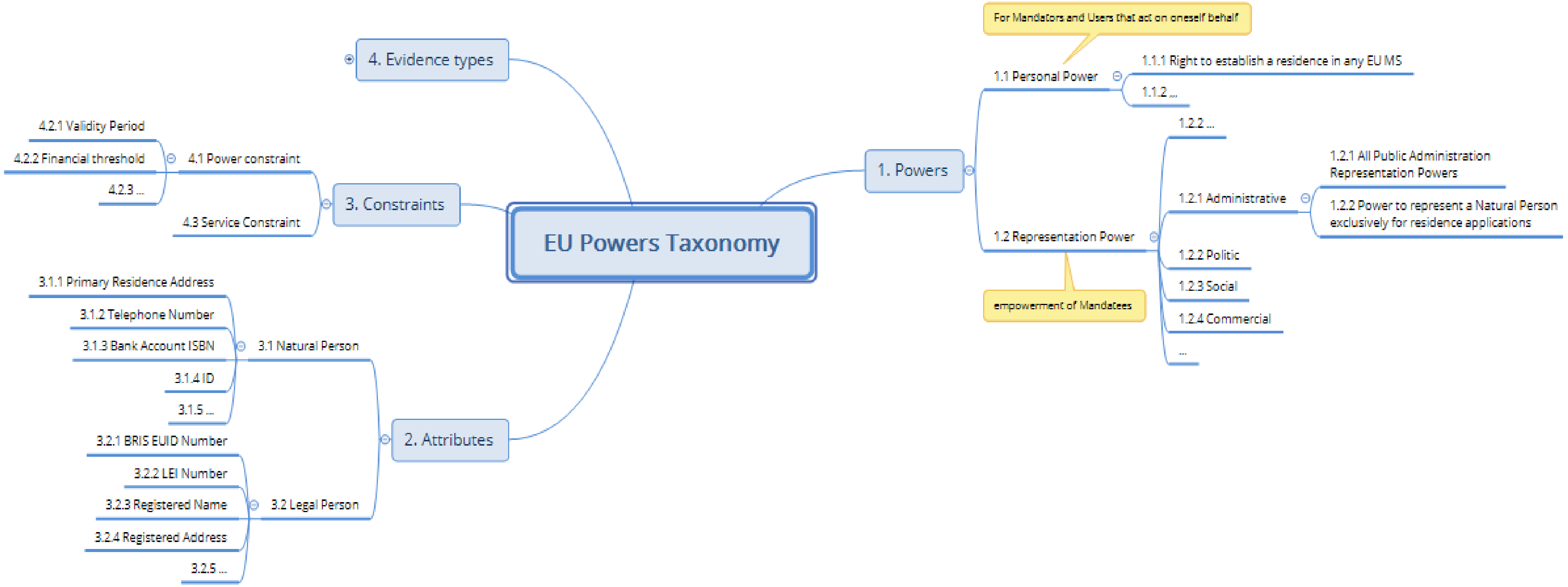


FIGURE 3: POSSIBLE ORGANISATION OF THE EU POWERS TAXONOMY

This approach is based on four “pillars”: Powers, Attributes, Constraints and Types of Evidences.

The approach aims for the definition of very precise features for each type of service, like the specification of which Powers the Mandator and the Mandatees have, which data should be verified for the Mandator and the Mandatee, what constraints shall be applied for each Power, and the type of evidences that need to be facilitated (e.g. reference to the source of evidences or additional information).

Both service providers and eMandate Registries would need to know how to establish these links for harmonised and non-harmonised services. This implies the need for an additional taxonomy where the services are linked to Powers, Attributes, Constraints and possibly to Types of Evidences (let us call it the “EU Service Catalogue”). The figure below illustrates this concept:

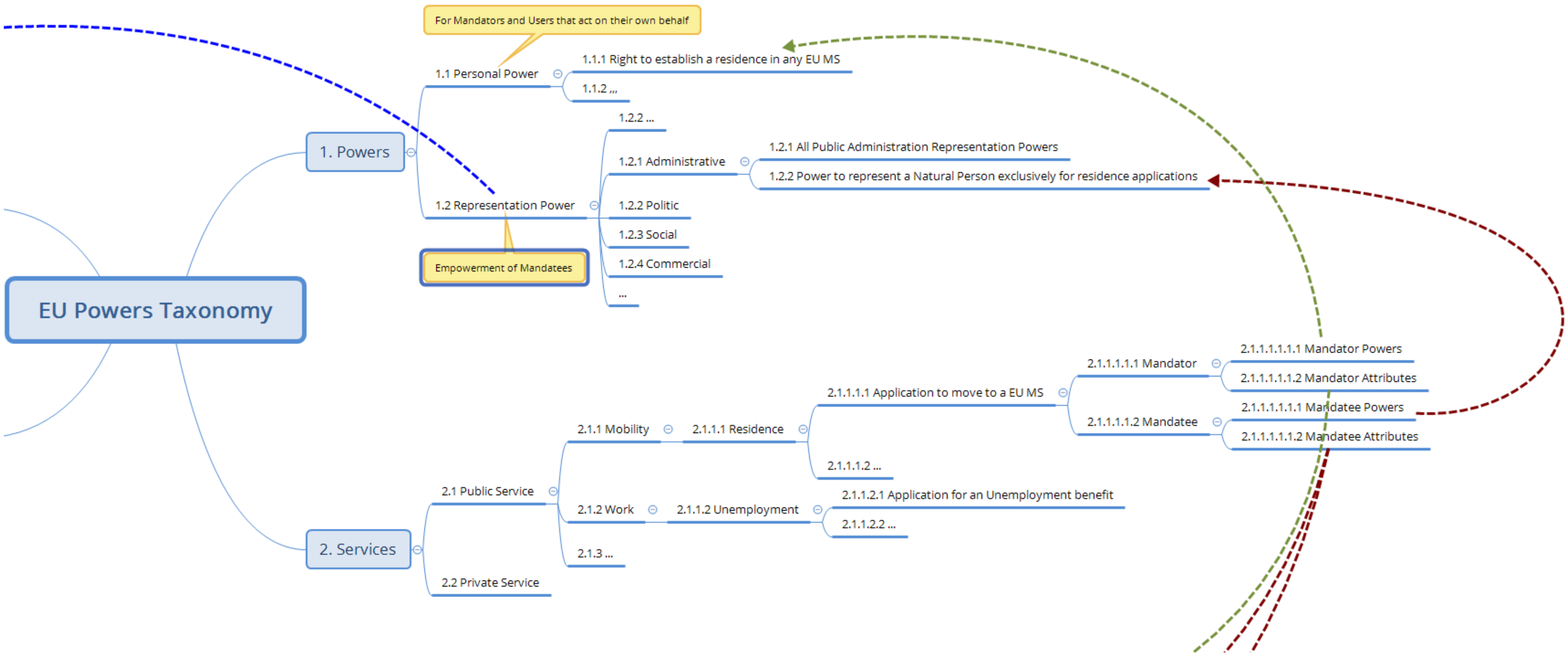

For Mandators and Users that act on their own behalf
EU Powers Taxonomy
1. Powers
1.1 Personal Power
1.1.1 Right to establish a residence in any EU MS
1.1.2 ...
1.2 Representation Power
Empowerment of Mandatees
1.2.2 ...
1.2.1 Administrative
1.2.1 All Public Administration Representation Powers
1.2.2 Power to represent a Natural Person exclusively for residence applications
1.2.2 Politic
1.2.3 Social
1.2.4 Commercial
...
2. Services
2.1 Public Service
2.1.1 Mobility
2.1.1 Residence
2.1.1.1 Application to move to a EU MS
2.1.1.1.1 Mandator
2.1.1.1.1.1 Mandator Powers
2.1.1.1.1.2 Mandator Attributes
2.1.1.1.2 Mandatee
2.1.1.1.1.1 Mandatee Powers
2.1.1.1.1.2 Mandatee Attributes
2.1.1.2 ...
2.1.2 Work
2.1.1.2 Unemployment
2.1.1.2.1 Application for an Unemployment benefit
2.1.1.2.2 ...
2.1.3 ...
2.2 Private Service

FIGURE 4: SERVICE CATALOGUE (1)

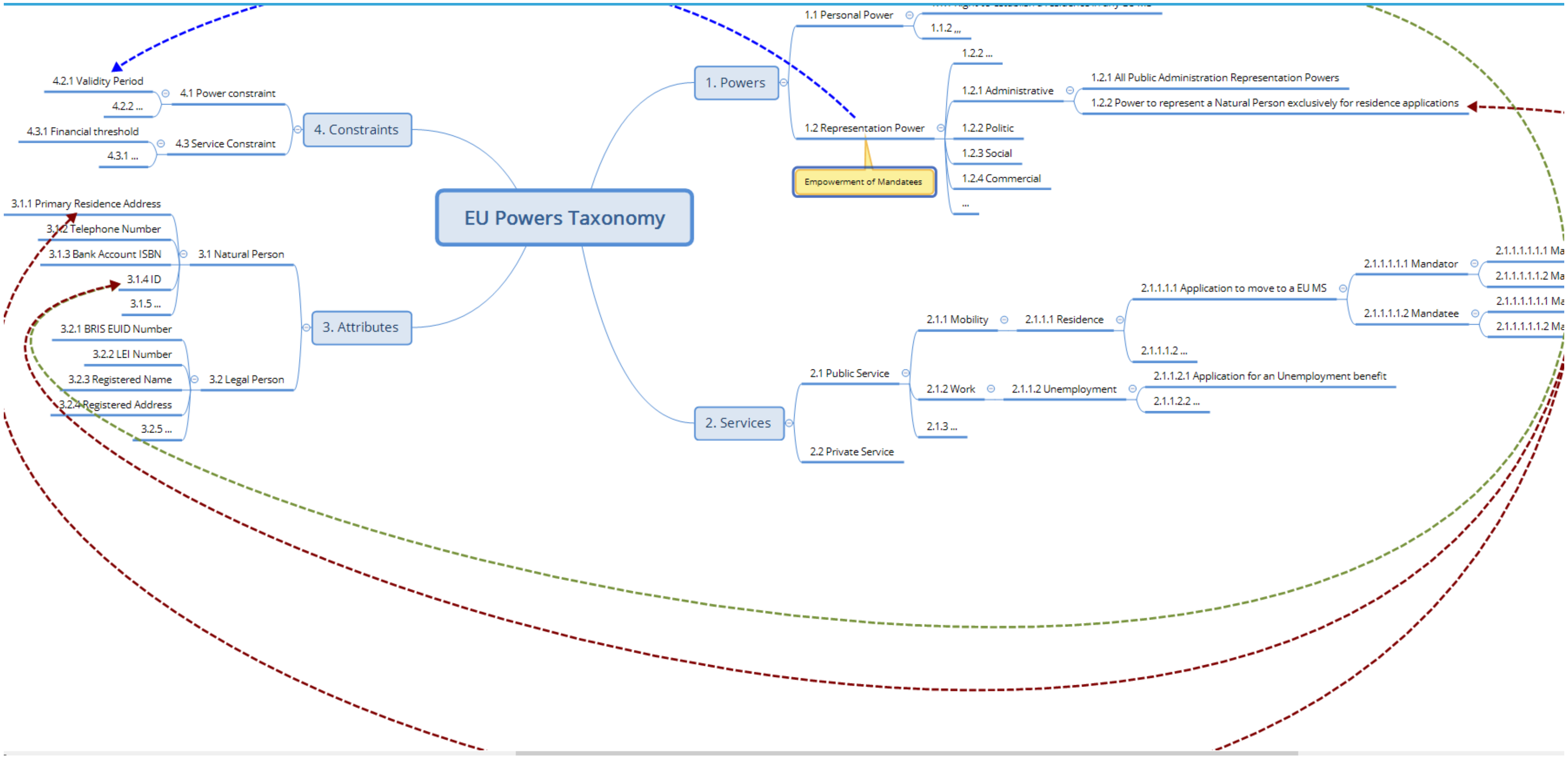


Figure 15: Service Catalogue (2)

If the service is harmonised, this “EU Service Catalogue” could be made publicly available by its governance body to both service providers and eMandate Registries, so their systems can use it to facilitate the creation and update of eMandates.

However, it may not be advisable to mix public and private services in one single Service Catalogue (contrary to what is presented above). Private partnerships of harmonised services should define and maintain their own Powers Service Catalogue.

See sections “Use Case 1 – Cross-border User authorisation / Non-harmonised Services / Public Services” and “Use Case 2 – Creation of an eMandate” for how this second taxonomy could be used by the SP and by the eMandate Registry.

3.5. Use Cases

When thinking about which aspects may be necessary in order to access a cross-border system, especially on behalf of another person, at least the following situations should be considered (other sub-cases are included therein, e.g. the validation of a eMandate is a sub-case of Use Case 1):

- **Use Case 0 – Cross-border user eAuthorisation**: A natural person wants to use on his/her behalf a service that is in another EU MS.
- **Use Case 1 – Cross-border Mandatee eAuthorisation**: A natural person in MS-A, acting on behalf of another natural or legal person, wants to access a service that is in MS-B.
- **Use Case 2 – Creation of an eMandate**: A natural person in MS-A wants to create an eMandate to empower one or more persons that are in MS-B.
- **Use Case 3** – **Delegation of Powers**: A Mandatee (natural or legal person), with the Power to delegate[15], assigns the Power of the Mandator to another Mandatee.
- **Use Case 4 – ePower/eMandate update**: A Person in MS-A wants to modify or revoke an existing ePower or eMandate that is registered in MS-B.
- **Use Case 5 – eAuthorisation of a person**: A legal person represents another person (natural or legal, the “ultimate” Mandator). This legal person in turn has empowered a natural person as its representative. This representative wants to get access to a cross-border service (in MS-B, SP-B) and act on behalf of the Mandator.

Be aware that, in this deliverable, this list of Use Cases is intended to clarify the proposals about **how to approach** the ePowers and eMandates data model and the federation of eMandate Registries that follow in this very document (which are the objectives of Task 1).

In Task 2, these use cases will be deeply reviewed and further elaborated. The objective of the **Task 2 use cases** is different: they **will be used to elicit the information requirements** of the data model. Therefore, the development of the Use Cases in Task 2 of may differ from the development of the Use Cases in Task 3.

[15] The “Power to delegate” is a type of Power that needs to be defined in the “Powers Taxonomy”.

3.6. Use Case 0 – Cross-border user eAuthorisation on the basis of a "Personal Power"

"A natural person[16] wants to use on his/her behalf a service that is in another EU MS".

In a European cross-border scenario, there can be two types of users: European citizens, or non-European citizens who are residents of a European MS.

It is worth nothing that for non-European citizens residing in a EU MS, "personal power" can be restricted. Consequently, access to some services can also be restricted, such as being able to move from one MS to another to establish residence.

For this reason, **our recommendation** is that the eIDAS solution, once extended as proposed, is used only **to enable cross-border eAuthorisation**. The proposal would consist of adding one or possibly two attributes to the current implementation, asking whether the person behind the user is a EU citizen or a EU MS resident.

Currently, a EU citizen in one MS cannot access the services provided by an SP in another MS unless the user is somehow registered in that system. This is the first challenge that a cross-border eMandate-based system will encounter. If this is not solved, it is not possible to implement the notion of a cross-border "Mandator", as the first thing to verify is whether the Mandator has "the power" of accessing the service. For this to be verified, the SP needs to check the actual data values corresponding to the user. This data may be contained in an electronic document. Let us call it this eDocument the "**ePower**" (see definition above in the section ***2.4 Definitions*** about the disambiguation between (e)Power, Representation Power and (e)Mandate).

For this Use Case 0, the person behind the user gets the ePower (i.e. "is empowered") by one SP, either located in another MS or in the same MS that the user is in. Hence, in this use case, "empowerment" is quite equivalent to the notion of "being invested with the legal rights and user privileges to access one Service Provider System". Once the ePower is created, it can be registered in a base registry as an evidence (e.g. in an "eMandate Registry").

But how can a cross-border service verify the existence and validity of this ePower and thus trigger the eAuthorisation?

3.6.1. Harmonised services

3.6.1.1 Public services

A harmonised service should imply that the user has the same rights in any MS as the MS where s/he is physically located. In principle, for any harmonised service, the only data that needs to be corroborated is:

- That the user is authentic, meaning that s/he is actually the person that provided the identification; and
- That the user "is in" a EU MS, i.e. is a citizen or a resident of a EU MS.

[16] In our context, "users" are always "natural persons". For the time being, we cannot take into account "systemic users" (i.e. hardware and software or firmware) acting on behalf of another person, either natural or legal; but this is a non-fictional scenario that should be envisioned, especially for frequent repetitive actions. In that case, the system would act as a Mandatee.

The first operation can be performed by the eIDAS infrastructure, and the second is implied in the first, as the eIDAS regulation and infrastructure only applies to EU citizens.

All non-EU citizens that are residents in a EU MS are provided with an ID. If this card were an eID device, then eIDAS could be used to identify and authenticate them.

Example

A natural person in MS-A is preparing to establish residence to move to MS-B, where s/he intends to work and live for several years. This user starts by applying online for a residence permit in the city of MS-B where s/he wants to move to.

Pre-conditions related to this example

- The user is a EU citizen;
- The technical solution already exists for eIdentification and eAuthentication (this would be covered by the current eIDAS infrastructure);
- Extension of the eIDAS legal framework would be necessary to include non-EU citizens that are residents in a EU MS;
- eID devices (e.g. eID cards, adapted mobile technologies, etc.) would be necessary for non-EU residents in all EU MS.

Possible flow related to this example

- The user identifies him/herself as s/he would do in the equivalent public service in MS-A, where s/he currently is;
- MS-B uses eIDAS to identify and authenticate the user;
- If the attributes supplied through the eIDAS are confirmed as correct and authentic, the service allows access to the user.

GDPR-related note

In principle, the user does not need to consent to service provider B (SP-B) sharing basic ID data with service provider A (SP-A), as it is the user who provided this data when trying to access SP-A, and SP-B would only need to respond with a technical acknowledgment (e.g. OK or KO, meaning let user in, or don’t let user in).

ePower: summary, conclusions and further implications

- The recognition of the Powers is performed by SP-B.
- Because in the case of harmonised public services the eAuthentication as a EU citizen automatically implies the right to access the equivalent cross-border service, the evidence of the legal capacity of the user (the “ePower”) to access the system is provided by MS-B through eIDAS in the form of the eIDAS attributes currently used for the eAuthentication.
- In this case, the registration of the ePower would not make sense.

3.6.1.2 Private services

In the case of services supplied by private organisations, the evidence that the identity provided by the user is authentic and has the Power to access the service (as defined in the “ePower”) would be provided by an organisation in a different MS that has subscribed to a bilateral (or multilateral) agreement with the other organisations that offer the same service with identical (or very similar) conditions.

Example

A user that is the client of a bank (SP-A) in one MS, wants to create a bank account in a different bank (SP-B) located in a different MS.

Pre-conditions

- An agreement exists between the organisations that provide the service.
- The agreement establishes that SP-A relies on the response by SP-B.
- The user is registered in SP-A, which may imply that the personal data on this user is also transferred to the organisation behind SP-B.

Possible flow

- The user identifies him/herself as s/he would do in front of SP-A.
- SP-A uses an ad-hoc internal interoperability infrastructure [17] to determine the organisation where the user is registered.
- SP-A requests from SP-B the confirmation of the validity and authenticity of the data supplied by the user.
- Upon positive confirmation, SP-A lets the user access its system.

GDPR-related note

In principle, the user does not need to consent to SP-B sharing basic ID data with SP-A, as it is the user who provided this data when trying to access SP-A, and SP-B would only need to respond with a technical acknowledgment (e.g. OK or KO, meaning let user in, or don't let user in).

In the case that SP-A should need further personal data about the user[18], SP-A would have at least two options:

1) Ask the user for the data, in which the consent is implicit in the fact that the user provides the data voluntarily; or
2) Ask SP-B to provide the data, which would require the user to consent in front of SP-B to share this data with any organisation that is a member of the trust-ring.

ePower: summary, conclusions and further considerations

- The recognition of the Powers is performed by SP-B. The user is registered with SP-B, all the data needed to check the authenticity of the user's ID and the validity of the user's capacity (power) to act in front of SP-B Service is under SP-B control.
- The evidence supplied by SP-B (the "ePower") could be reduced to a simple acknowledgment tag (OK or KO).
- Based on their bilateral agreement, SP-A must rely on the response supplied by SP-B.
- The registration of the ePower in an eMandate Registry would not make sense.

[17] The "ad-hoc interoperability infrastructure" here highlights the fact that, in principle, private sector organisations cannot use eIDAS or other public sector resources for their private interests, and therefore have to agree on the adoption (or development) of an existing "added value network" for the purpose of eIdentification, eAuthentication and eAuthorisation. The TOOP infrastructure could see these situations as an interesting business opportunity.

[18] This would be a usual situation, namely for communication purposes directly between the SP and the user.

3.6.2. Non-harmonised services

3.6.2.1 Public services

The fact that the service is not harmonised implies that:

- Services that aim at identical or similar goals may be based on different principles, or have different legal requirements, processes, inputs and outcomes.
- The SP does not rely on a “standard” response from an “authority” located in another Member State (as it does in the case of harmonised services), but on very sector- or service-specific data (e.g. power attributes) that this authority supplies.

Example:

A user that is a citizen of EU MS-A and resides in MS-A wants to obtain an unemployment benefit from MS-B. This user lived and worked for a period of time in MS-B and has the right to apply for that benefit using SP-B (i.e. a service supplied by a public administration of MS-B).

Pre-conditions:

- The natural person behind the user has the legal capacity to use the service. Some business-related information is required and needs to be verified before allowing access (i.e. information regarding the labour history of the natural person).
- The technical solution already exists for eIdentification and eAuthentication (this would be covered by the current eIDAS infrastructure).
- The EU Powers Taxonomy exists and is available online (See section “3.4 The EU Powers taxonomy”).
- SP-A needs to rely on the quality of the data supplied by SP-B. In the context of public services, this is ensured by default by the legal obligation of all members to guarantee the quality of the data their administrations keep. Data quality is determined by many aspects such as veracity, authenticity, integrity, consistency, formal correctness, and others. In the context of Europe, this mission (ensuring the quality of the data) is the responsibility of the official Base Registries and national databases. The fact that Base Registries are normally specialised in one single topic facilitates both the uniqueness of the source of data (once-only-principle) and the verification of the quality of the data. However, the analysis of the current situation of Base Registries in the EU MS shows that only a small minority of them do proactively verify the veracity of the information that is registered. The rest rely on the evidences supplied at registration time[19].

Possible flow:

- The user enters the service in MS-B (SP-B) and identifies him/herself using an eID device issued by MS-A.
- SP-B identifies and authenticates the user; eIDas can be used for this operation.
- **Sub-flow 1**: SP-B retrieves the labour information available in MS-B about this person. In this case, there is no cross-border interoperability and the legal capacity required to

[19] See ISA2 Action “Access to Base Registries”, namely the factsheets on the state of affairs regarding the Base Registries in the European Union: https://joinup.ec.europa.eu/collection/access-base-registries/abr-member-states-factsheets.

let the user access the service is guaranteed by the data supplied to SP-B through other MS-B national public services (e.g. Social Security, Labour Ministry, Tax Agency, etc.).

- **Sub-flow 2**: Additionally, SP-B may want to cross-check data with MS-A by requiring from an SP-A (a service provider located in MS-A) data about the labour file of the person in MS-A for the period when s/he was presumably living and working in MS-B:
  - SP-B "discovers" which service provider keeps the labour file. One way of solving this could be the use of a EU Catalogue of Services (e.g. authoritative systems like Base Registries) that "maps" the different services existing in all MS and facilitates the identification of the provider for that specific service in any of the EU MS. At present, a broad/generic pan-European solution like this does not exist, but several trans-European systems (TES) and EU projects have implemented or are implementing partial solutions that solve a similar need[20].
  - SP-B requests data specifically related to the labour history of the person from an SP-A. For this, SP-B shares some information about the person with SP-A (e.g. identification, period of residence and working in MS-B, data about the company or companies for which the person worked, etc.). The request aims to get confirmation from SP-A that the person resided and worked in MS-A during the period and for the companies specified.
  - SP-A could respond with an electronic document where the information needed by SP-A is present and confirmed: i.e. an electronic certification of administrative facts from MS-B. This eCertificate document may attach supplementary information normally specified as references (URLs), pointing at evidences that are available online and are freely accessible to SP-A. The electronic certificate would/should contain response values for the type of data specified in a pan-European catalogue of ePowers (see 3rd pre-condition regarding the EU Powers Taxonomy, within this same example).

GDPR-related note:

For sub-flow 2, SP-A would need the consent of the user in order to share his/her personal data with SP-B.

ePower: summary, conclusions and further implications

- The recognition of the Powers is performed by SP-A.
- **Sub-flow 1**: The Power is defined in the pan-EU ePower Taxonomy. The actual data values that need to be verified by SP-A to unlock the access is retrieved from the Base Registries in MS-A. In other words, the "empowerment" of the person behind the user is done by the public administration where the user is in.
- **Sub-flow 2**: The "empowerment" of the person behind the user is thus done by the SP-A, based on the evidences collected from one or several public authorities (e.g. a Base Registries).
- If the Sub-flow 2 is executed, all the data collected about this empowerment could be exported by the user into a machine-readable electronic document (an eDocument of type ePower). This ePower could be registered in a EU MS national eMandate Registry with the purpose of being reused by other cross-border public or private services with identical or similar information requirements. The ePower could to be based on a

[20] Some examples would be: BRIS (Business Registers Interconnection System), ABR (Access to Base Registries), TAXUD's UUM&DS, eCerties, others.

common standard vocabulary, such as the one that will be proposed in this project (Task 2 of this project aims at developing such a common vocabulary).

3.6.2.2 Private services

The fact that the service is private and not harmonised may imply that:

- There is not any homogeneity between the services in the different EU MS nor even within one MS;
- There is not any contract, agreement or legislation with other private (nor public) services providers,

Example

A user in MS-A wants to buy a house in MS-B online. S/he tries different service providers in MS-B, and all of them behave differently and request different types of information about the user.

Pre-conditions

- The user can identify him/herself using a solution provided by the service provider (e.g. biometric data that the SP can store and reuse between operations and transactions, or even between different services of the same organisation through one or different SPs).
- The user is not reluctant to provide a guarantee to start operating (e.g. a credit card number that is validated by the SP and an amount that may be blocked from the account linked to that card). The philosophy is that a user that is willing to supply an economic guarantee is not willing to easily renounce use of the service or to swindle the private organisation behind the SP).
- The user may be required to provide the SP with electronic evidences that are stored in either private or public Registries (e.g. a Financial Solvency Certificate, a declaration on oath, etc. registered in a Central Registry of Notaries or in Public Base Register in an EU MS). This implies that the SP can[21] access the Registry online, get the evidences from there and process the content of the evidences automatically.
- The SP is able to process the evidences automatically, which implies that either the SP knows the specific format and content of the eCertificate supplied by the Registry or that the Registry is using a "standard" vocabulary. In the second case, this standard vocabulary could be the pan-EU taxonomy proposed above. In the end, such a taxonomy could become an ever-growing data graph (an ontology) aiming to cover any type of power used in both the public and private sectors.

Possible flow

- The user first registers in the SP system. For this s/he provides the system with evidences used by the SP to identify and authenticate the person behind the user, e.g. biometric data like a picture of his/her face (for automatic facial recognition and/or iris recognition), a sound-track file with the user's voice (voice recognition), a picture of

[21] "Can" here means that the Registry is accessible online, but also that the SP has the authorisation to access it, i.e. that the user has explicitly registered his/her consent for that SP to access the Registry. This may imply complex sub-scenarios like the cases where the evidences are public but not free of charges, in which cases an online payment service needs to be involved too (which is practically always the case when the Registry is private and can occur also when it is public. See BRIS for a possible payment model involving cross-border payments between users and EU Public Administrations).

his/her fingerprint recognition, etc. S/he could also have to provide a credit card account or provision the SP with an economic amount.

- The SP may need punctual or regular electronic evidences to unlock the access to that particular service. For example, in the case of the purchase of a house, the owner of the property (or the SP itself) may be interested in having sound proof of the financial capability of the user. In this case, the easiest method is for the user to provide the URL of the Registries. An alternative would be that the SP discovers the sources of evidences and offers the user the possibility of selecting one or more source. In the private sector context, this is a very distant possibility for the time being.
- Once all the data requested is obtained and checked by the SP, the user can access the service.

GDPR-related note

The user will need to explicitly consent before the Public Administration Services that his/her personal data can be shared with the SP and the organisation behind the SP.

ePower: summary, conclusions and further implications

- The “empowerment” of the user is performed by the SP, based on factual data provided by the user and additional electronic evidences provided by other public or private SPs (e.g. Notaries, Base Registries, National Databases, others).
- As for the non-harmonised public services, this empowerment by a private sector’s SP could be exported by the user, after registration in the SP System, into a machine-readable electronic document (an eDocument of type ePower). This eDocument could be registered in a EU MS national eMandate Registry with the purpose of being reused by other private or public services with identical or similar information requirements. The ePower could to be based on a common standard vocabulary, such as the one that will be proposed in this project (Task 2 of this project aims at developing such a common vocabulary).
- The construction of an ever-growing Taxonomy of ePowers may end up in a gigantic complex graph of difficult management, especially for the private services (which would require an enormous effort in terms of governance and organisational and semantic interoperability). One solution is to split the Taxonomy into two different controlled vocabularies, one specific of the public sector and another for the private sector. It is possible that the commercial interests behind the organisations offering services could end up fostering the faster and sounder construction of a standardised private sector’s ePowers Taxonomy. If that is the case, this taxonomy could be a good enabler towards the facilitation of private harmonised services.

3.7. Use Case 1 – Cross-border Mandatee eAuthorisation on the basis of a “Representation Power”

“A Natural Person in MS-A, acting on behalf of another Natural or Legal Person, wants to access a Service that is in MS-B”.

As a general rule, the SP in MS-B (SP-B) will be interested in at least four aspects:

1. Determining who the user is and that s/he is acting on behalf of another person (the Mandator);
2. Obtaining the eMandate;

3. Verifying whether the Mandator has the Power to access the service or not;
4. Verifying that the eMandate is valid, i.e. it comes for a “source of truth”, it is formally correct and complete and the constraints are met.

3.7.1. Harmonised services

3.7.1.1 Public services

The fact that the service is public and harmonised implies that:

- The services are identical or very similar;
- There is EU legislation where the obligation is clearly established for all SPs to authorise any user that is in a EU MS and has an eMandate;
- The eMandate was registered and is stored by an Authority. Let us refer to it as the “eMandate Registry[22]”.

As a result of the above points, SP-B relies on the data supplied by an eMandate Registry located in an EU MS.

Example

A EU citizen in MS-A is preparing to move to MS-B, where s/he intends to work and live for several years. The user contracts a professional who is specialised in administrative matters (a natural person) and requests they take the necessary steps in front the MS-B administration. For that purpose, s/he creates an eMandate empowering this other natural person to act on his/her behalf.

Pre-conditions

- Any EU citizen is allowed to move to another MS country (this is covered by EU Law).
- The eMandate where the EU citizen (the Mandator) empowers the professional representing him/her (the Mandatee) is stored in a EU eMandate Registry.
- A technical solution exists for the eIdentification and eAuthentication of both the Mandator and the Mandatee (this would be covered by the current eIDAS infrastructure).
- The Mandator is in a EU MS and has the right to move to another EU MS country.
- The Mandatee is in a EU MS. For the time being, unfortunately, the only possibility to authenticate a natural person is to use a EU MS eID device. Interoperability with any other non-EU countries cannot currently be ensured. If the authentication of the Mandatee is not possible, the empowerment cannot be verified and the eAuthorisation will be rejected.
- The data that allows the unequivocal identification of the Mandator and the Mandatee is contained in the eMandate and matches the data used to access the service.
- A pan-European Registry of Registries (including all the eMandate Registries in all the EU MS) exists and is accessible online.
- The EU Powers Taxonomy exists and is available online. See section (See section “3.4 The EU Powers taxonomy”). The following Powers have been defined in the EU Powers Taxonomy:

[22] Be aware that the Authority may outsource the construction of the eMandate Registry System and the management of the eMandates to a third public or private organisation.

    - 1 →Power
    - 1.1 → Personal Power (Natural person acting on behalf of oneself)
    - 1.1.1 → Right to establish a residence in any EU MS
    - 1.1.n → …. (more specific categories and sub-categories of Personal Powers would go below)
    - 1.2 → Representation Power (Natural or legal person acting on behalf of another natural or legal person)
    - 1.2.1 →All Public Administration Representation Powers (right of a natural or legal person to represent a EU citizen or a EU resident in front of any EU Institution and MS Public Administration)
    - 1.2.n →… (more specific categories and sub-categories of Representation Powers would go below).

- This specific service exists in the EU Service Catalogue. Therefore, the SP knows exactly which Powers, Constraints and Attributes are necessary for the eAuthorisation.

Possible flow

- The user, in this case the Mandatee, enters the SP-B system.
- The SP-B system requests the user to enter the following information:
    - The user identification data, which is probably furnished by the user by means of an electronic device (e.g. a digital certificate in an eID card or a mobile device);
    - Whether the user acts on behalf of another person; or directly the ID of a specific eMandate. If the user does not provide the eMandate ID the SP could try to search for it through the EU Registry of Registries and present a list of existing eMandates in which the user is a Mandatee.
- The SP-B gets the eMandate through the EU Registry of Registries[23].
- As this is a harmonised service, SP-B is interested in knowing whether the Mandator has the Power to access the same service in MS-A. For harmonised services this amounts to verify whether the Mandator is a EU citizen (or has the Power coded as 1.1.1, see "pre-conditions" above). The eIDAS infrastructure could be used to identify and authenticate the user (see section "3.2 The meaning of "is in"'").
- A very first operation to be executed by SP-B is to check whether the eMandate is valid or not. If the eMandate is valid it means that all the constraints defined in the eMandate are met. For instance, if there is a time limit for the use of the eMandate and the period of use has elapsed, then SP-B should reject the access to its systems. Alternatively, it could reject the eAuthorisation based on a negative technical acknowledgement signal (ACK KO) by the eMandate Registry upon request of the eMandate[24] (e.g. "response: KO", "reason code: EXPIRED"; or "response: KO, "reason code: REVOKED"; etc.).
- If the eMandate is valid, SP-B needs to verify the empowerment of the Mandatee. To do this, SP-B checks the list of Powers that the Mandatee has. This information can be expressed as a list of codes in the eMandate. Each code represents the Power defined in the EU Powers Taxonomy. If the code 1.2.1 is specified in this list, SP-B concludes that

[23] The alternative where it is the user who provides (uploads) the eMandate would devoid this use case of interest: it would be a non-cross-border scenario and would not be relevant from the once-only-principle perspective. See also section "3.1 Cross-border interoperability".

[24] This second option would be preferable in our opinion, as it would avoid the transfer of personal data that ultimately won't be used because the eMandate is not valid.

the Mandator assigned the Power to the Mandatee (see example of a fragment of codes in the “pre-conditions” above).

- If the Mandator is a EU citizen, the constraints on the Power and the eMandate are met, and the Mandatee has the Representation Power requested, SP-B should allow the access to the user.

GDPR-related note

Explicit consent by the Mandator about the use of his/her personal data by the Mandatee and the SP would be necessary. Regarding the eMandate Registry, the fact that the eMandate is registered could be an implicit proof of consent in itself.

ePower: summary, conclusions and further implications

- The recognition of the right to access the service is made by the SP.
- This recognition is based on the data supplied by the eMandate Registry in a response to a request by the SP.
- The main data required are:
  - The ID of the Mandator,
  - The ID of the Mandatee
  - Any constraint applicable to the Mandator, Mandatee and eMandate
  - The Powers of the Mandator, and possible constraints on each Power
  - The Representation Powers of the Mandatee.

3.7.1.2 Private services

Harmonised services in the context of the private sector cross-interoperability implies that:

- A contract and agreements exist between the organisations that exchange information acknowledging the right to exchange information and establishing the conditions of the exchange and of the services. Let us call these organisations “partners”.
- The services offered are identical or very similar in terms of processes, business rules, inputs and outcomes (orchestrated processes, common vocabularies and artefacts, similar business capabilities, etc.).
- Any operation that a user can execute in one partner’s service can also be executed by that same user in the equivalent service of a different partner located in another MS.
- Public organisations cannot be partners, as this would fall under the public law and under the category of public harmonised service.

Example

A natural person that is already the client of a bank (SP-A), wants to open a bank account with a different bank (SP-B) located in a different MS. For this, this natural person (the Mandator) empowers another natural person (the Mandatee) to represent him/her in front of SP-B.

Pre-conditions

- The Mandator is a user registered in SP-A. SP-A keeps all the data about the Mandator necessary to unlock his/her access to its service.
- There is an eMandate where the Mandatee is empowered to represent the Mandator for this type of service.
- The eMandate is accessible online to all the partners through the EU Registry of Registries. Alternatively, it could be a Mandate or an eMandate registered and

preserved by SP-B. For this use case, we will presume that it is an eMandate and that it is accessible via the EU Registry of Registries.

- The eMandate is stored in an EU MS eMandate Registry. If the eMandate is not in the same MS as the Mandator or the Mandatee, it should not be relevant. Persons can have the Power to create eMandates in any EU MS (see section “3.9 Use Case 2 – Creation of an eMandate”).
- The Mandatee can be identified and authenticated, e.g. by biometrics means.
- The data that allows the unequivocal identification of the Mandator and the Mandatee are contained in the eMandate.
- The Power “Capacity to create bank accounts” is defined in the EU Powers Taxonomy.
- The SP knows exactly which Powers, Constraints and Attributes are necessary for this specific service (they are defined in a EU Service Catalogue, maintained by the partnership governance body).

Possible flow

- First access:
    - The user enters the SP-B service. In this case the user is the Mandatee.
    - The SP-B service requests the following data:
        - Whether the user is acting on behalf of another user or on his/her own behalf;
        - Whether the partner is in another MS where the Mandator is already registered;
        - In the case that the user is acting on behalf of another user, the identifier of the eMandate is requested;
        - The eID data of the Mandatee (e.g. biometric information of the Mandatee;
        - Other security data, like the telephone number of the Mandator in order to send a request for confirmation, for example.
    - If the Mandator does not confirm the operation (last bullet in the previous list) the eAuthorisation is rejected. Otherwise:
    - SP-B forwards a request message to MS-A eMandate Registry keeping all these data;
    - SP-B receives the eMandate via the EU Registry of Registries;
    - SP-B verifies that the eMandate is valid (all constraints are met);
    - SP-B identifies the Mandator and authenticates him/her as a registered user;
    - SP-B checks whether the Mandator has the access to use this particular service (creation of a bank account). It also checks that the Mandatee has the Power (the legal capacity) to act on the Mandator’s behalf in MS-B (for the creation of a bank account, some MS private services require that the Mandator be in the MS). In principle, the eMandate would not be necessary for this verification, and SP-B only needs the Mandator ID to check its own system;
    - SP-B identifies the Mandatee. If the Mandatee data is not registered with SP-B yet, SP-B records the data for future use. SP-B verifies that the Mandatee identification matches exactly the data contained in the eMandate;
    - SP-B checks whether the Mandatee has been empowered to create bank accounts on behalf of the Mandator. For this, SP-B looks up, in the eMandate, the code for the Power “Creation of a bank account” in the list of Powers assigned to the Mandatee;

    - If the empowerment is verified, and the rest of conditions are validated the Mandatee is allowed to access the service.
- Subsequent accesses: after the first eAuthorisation has been allowed, there are at least two possible alternatives:
    - SP-A stores all the data requested during the first access, including the data contained in the response by SP-B, and registers the Mandator as a user of its service; or
    - SP-A and SP-B repeat the same actions as the ones executed for the first access each time.

  In both cases, the eMandate needs to be retrieved and validated each time the Mandatee wants to access the service (namely to check that the Power has not been revoked and that the rest of the constraints are still being met).

GDPR-related note

The Mandator and the Mandatee will need to explicitly consent in front of the eMandate Registry that their personal data can be shared with the SPs and the organisations behind them[25] for the purposes of this type of service.

ePower: summary, conclusions and further considerations

- The recognition of the Powers is performed by SP-B.
- For the recognition, SP-A relies on the operations executed by SP-B and on the data provided in its response to a request for eAuthorisation.
- The eMandate could be stored in a public or private eMandate Register, which must be accessible online (unless it is another type of Mandate stored by SP-B. See "pre-conditions" above).

3.7.2. Non-harmonised services

3.7.2.1 Public services

The fact that the service is not harmonised implies that:

- Services that aim at identical or similar goals may be based on different principles, legal requirements, processes, business rules, inputs and outcomes.
- The SP does not rely on a "generic" response from an "authority" located in another Member State, but on the data supplied by the user (the Mandatee) and the eMandate Registry.
- The legislation of MS-A most likely requires a set of data not required in MS-B.
- The Mandator needs to create an ad-hoc eMandate for this specific service.
- The SP needs to be able to define its service in the EU Service Catalogue. This may not be possible due to the absence of legal instruments or to organisational barriers (e.g. non-agreements amongst MS services or with the governance body, etc.). An alternative to this is that the SP (or the MS) defines its own National Service Catalogue that links each service to the codes of the EU Powers Taxonomy. For the creation of the eMandate, the eMandate Registry will need to have access to this National Service Catalogue. Possible solutions would be: the user indicates the source of the National

[25] Remember that the SP and the "owner" of the service may be different organisations.

Service Catalogue (e.g. a URL), or the EU Service Catalogue includes every National Service Catalogue.

Example:

A natural person (Mandator) that is a citizen of EU MS-A and resides in MS-A wants to get an unemployment benefit from MS-B. This person lived and worked for a period of time in MS-B and has the right to apply for that benefit using SP-B (i.e. a service supplied by a Public Administration of the MS-B). The Mandator empowers another natural person to act on his/her behalf for this type of service.

Pre-conditions:

- The Mandator has the Power to establish his/her residence in any of the EU MS.
- There is an eMandate where the Mandatee is empowered to represent the Mandator for this type of service.
- The eMandate is stored in an EU MS eMandate Registry. If the eMandate is not in the same MS as the Mandator or the Mandatee, it should not be relevant. Persons can have the Power to create eMandates in any EU MS (see section
- The eMandate is accessible online to all the partners through the EU Registry of Registries.
- The Mandator and the Mandatee can be identified and authenticated, e.g. using the eIDAS infrastructure.
- The data that allows the unequivocal identification of the Mandator and the Mandatee are contained in the eMandate and match the data used to access the service.

Possible flow:

- The user, in this case the Mandatee, enters the SP-B system.
- The SP-B system requests that the user enter the following information:
    - The user identification data, which is probably provided by the user by means of an electronic device (e.g. a digital certificate in an eID card or a mobile device);
    - Whether the user is acting on behalf of another person;
    - If the user is acting on behalf of another person, SP-B will inform the user of the need to have an eMandate empowering the Mandatee with the specific Powers required to access the service. This implies that:
        - SP-B must specify which data (and if needed, reference the sources of evidences) the user must provide in the eMandate; and
        - The Mandator has to create a new eMandate to empower the user.
- In the case that the user does not have that eMandate, s/he would enter an eMandate Registry and create a new eMandate where all the Powers required by SP-B are well specified (the Powers of the Mandator and the Powers assigned by the Mandator to the Mandatee). See also section “
- ”.
- Whilst creating the eMandate, the user supplies the data requested by SP-B. For example:
    - SP-B requires:

    - **For the Mandator**: ID and the Power to establish a residence in a EU MS (for whatever reason, SP-B wants to cross-check this information with that provided by eIDAS);
    - **For the Mandatee**: ID, primary residence address and Power to represent a natural person for residence applications.
  - The Mandator specifies:
    - **For the Mandator**: The Attribute code "3.1.1" followed by the ID type and number; and the Power code "1.1.1";
    - **For the Mandatee**: The Attribute code 3.1.1 followed by the ID type and number, the Representation Power code "1.2.2" and the Attribute code "3.1.1" followed by the structured primary residence address of the Mandatee.

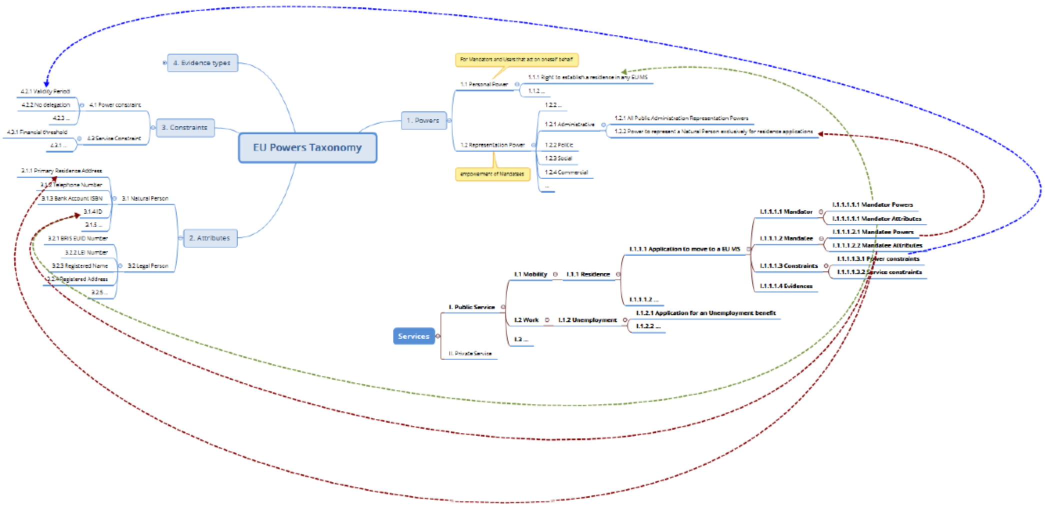


FIGURE 5: SPECIFICATION OF POWERS AND ATTRIBUTES FOR A SPECIFIC SERVICE

- The user goes back to the SP-B service and supplies the eMandate identifier.
- SP-B gets the eMandate through the EU Registry of Registries[26].
- SP-B verifies that the eMandate is valid (all constraints are met). If not, the eAuthorisation is rejected and the explanation for the rejection is communicated to the user. (See also this point in relation to harmonised services, above).
- SP-B verifies whether the Mandator has the Power to act in relation to this service. Following the example, this could be based on the identification and authentication of the user through eIDAS to check that the Mandator is a EU citizen. Alternatively, it could be confirmed if, in the eMandate section about the Mandator, the Power code "1.1.1" equivalent to "Right to establish a residence in any EU MS" is specified.
- Next, SP-B needs to verify the empowerment of the Mandatee by checking the list of Powers that the Mandatee has. As illustrated above, this information can be expressed as a list of codes in the eMandate. Each code represents the Power defined in the EU Powers Taxonomy. If all the codes and data about the Mandatee that are required for

[26] The alternative in which the User provides (uploads) the eMandate would devoid this use case of interest: it would be a non-cross-border scenario and would not be relevant from the once-only-principle perspective. See also section "3.1 Cross-border interoperability"

this SP are supplied, the empowerment should be considered as valid (the SP relies on the quality of the data supplied by the eMandate Register[27]).
- If the Mandator has the required Power, the required data are supplied, the constraints on the Power and the eMandate are met, and the Mandatee has the Representation Power requested for this specific service, SP-B should allow the access to the User.

GDPR-related note:

The Mandator and the Mandatee will need to explicitly consent in front of the eMandate Registry that their personal data can be shared with the SP and the organisations behind it[28] for the purposes of this type of service.

ePower: summary, conclusions and further implications

- The recognition of the Powers is performed by the SP, based on the data supplied by the eMandate Registry.
- The EU Powers Taxonomy must be flexible enough to allow the combination of different Actors, Powers, Services and Attributes.

3.7.2.2 Private services

If the service is private and not harmonised, it implies that SP-A and SP-B have no agreements and that the service models are different in terms of processes, business rules, inputs, outcomes, constraints, etc.

Example

A natural person (the Mandator) in MS-A wants to buy a house in MS-B online. The Mandator empowers a natural person (the Mandatee) to act on his/her behalf.

In this case, the user is the Mandatee. The user tries different SPs in MS-B. All of them behave differently and request different types of information about the Mandator and the Mandatee.

Pre-conditions

- The Mandator has the Power to buy real estate.
- The Mandatee has the Power to represent the Mandator for this type of act (the purchase of real estate or a broader power subsuming the purchasing of real estate).
- There is an eMandate where the Mandatee is empowered to represent the Mandator for this type of service.
- The eMandate is stored in a EU MS eMandate Registry. If the eMandate is not in the same MS as the Mandator or the Mandatee, it should not be relevant. Persons can have the Power to create eMandates in any EU MS (see section “3.9 Use Case 2 – Creation of an eMandate”).
- The eMandate is accessible online to all the partners through the EU Registry of Registries. Alternatively, it could be a Mandate or an eMandate registered and

[27] Additionally, the eMandate is probably signed electronically by the Mandator and the Mandatee. If it is signed normally, it implies the declaration of responsibility. The registration in the eMandate Registry and its delivery to other Public Administrations should also be submitted to non-repudiation control.

[28] Remember that the SP and the “owner” of the service may be different organisations.

preserved by SP-B. For this use case, we will presume that it is an eMandate and that it is accessible via the EU Registry of Registries.

- The Mandatee can be identified and authenticated, e.g. by biometrics means.
- The data that allows the unequivocal identification of the Mandator and the Mandatee are contained in the eMandate.
- The Mandator and the Mandatee can identify themselves using a solution provided by the SP (e.g. biometric data that the SP can store and reuse between operations and transactions).
- The user is not reluctant to provide a guarantee to start operating (e.g. a credit card number that is validated by the SP and an amount that may be blocked from the account linked to that card). The philosophy is that a user that is willing to supply an economic guarantee is not willing to easily renounce use of the service or to swindle the private organisation behind the SP).
- The user may be required to provide the SP with electronic evidences that are stored in either private or public Registries (e.g. a Financial Solvency Certificate, a declaration on oath, etc. registered in a Central Registry of Notaries or in a Public Base Register in a EU MS). This implies that the SP can[29] access the Registry online, get the evidences from there, and process the content of the evidences automatically.

Possible flow

- The user enters the system of an SP in MS-B (SP-B).
- SP-B requests that the Mandatee register as a user of the service.
- Along with the data required to register, SP-B asks whether the user is acting on behalf of another natural or legal person.
- Validations and operations related to service sign on are executed by SP-B (e.g. the verification that the credit card data supplied is valid and that a guarantee has been ensured).
- If the user is acting on behalf of another person, s/he must refer to or provide the eMandate empowering the user to represent the Mandator, as is also required for the harmonised service.
- SP-B gets the eMandate through the EU Registry of Registries (see alternative in the “pre-conditions” above).
- SP-B validates the eMandate (all constraints must be met).
- If the eMandate is validated, SP-B verifies that the Mandator has the Power to act in MS-B for this type of act. This can be a complex human-based operation, as it may imply the consultation of additional information (e.g. convictions, incapacitation, insolvency or bankruptcy situations, etc.) that is not available as structured machine-readable data.

[29] “Can” here means that the Registry is accessible online, but also that the SP has the authorisation to access it, i.e. that the user has explicitly registered his/her consent for that SP to access the Registry. This may imply complex sub-scenarios like the cases where the evidences are public but not free of charge, in which case an online payment service must be involved too (which is practically always the case when the Registry is private and can also occur when it is public. See BRIS for a possible payment model involving cross-border payments between users and EU Public Administrations).

- SP-B verifies the Powers of the Mandatee. If the code corresponding to a Power encompassing the right to purchase real estate is in the list of Powers assigned to the Mandatee, the user (Mandatee) is allowed to access the service.

GDPR-related note

The Mandator and the Mandatee will need to explicitly consent in front of the eMandate Registry that their personal data can be shared with the SPs and the organisations behind them[30] for the purposes of this type of service.

ePower: summary, conclusions and further implications

- The recognition of the empowerment is performed by the SP.
- For the recognition, the SP relies on the data provided by the user and by the eMandate Registry, and possibly also from other publicly accessible sources (e.g. debtors lists, business registries, convictions, etc).

3.8. Use Case 1.1 – Cross-border eAuthorisation of a legal person

"**A Legal Person (e.g. a company specialised in a specific business domain) has been empowered to act on behalf of another Person (Natural or Legal, the "ultimate" Mandator). This company in turn has empowered a Natural Person as its representative. The representative wants to get access to a cross-border Service (in MS-B, SP-B) and act on behalf of the Mandator**".

Regardless of whether the service is public or private and harmonised or not, this situation implies that:

- SP-B will have to validate two eMandates:
  - One in which the company empowers its representative; and
  - One in which the Mandator will be the end beneficiary of the service.
- It can be seen as a specialisation of Use Case 1 – Creation of an eMandate, where the user has been indirectly assigned delegated Powers (with the delegator being the legal person s/he represents). In other words, the user represents "transitively" the original Mandator.

All the operations executed by SP-B, the user and the eMandate Registry have already been described in Use Case 1. The difference is that, in this case, SP-B will have to access two different eMandates (not necessarily from the same eMandate Registry or EU MS).

3.9. Use Case 2 – Creation of an eMandate

"**A Person in MS-A wants to create an eMandate to empower one or more Persons that is in MS-B to access one or more Services on her behalf**".

Some preliminary considerations

- All EU citizens and EU residents should have the Power to empower a natural or legal person to act on his/her behalf through an eMandate in any EU MS.

[30] Remember that the SP and the "owner" of the service may be different organisations.

- The creation of an eMandate should be a "harmonised public service", which implies the need for a legal instrument that currently does not exist.
- The user will access the system as the Mandator; all EU MS have one or more eMandate Registries for public and private services.
- Section "2.4 Definitions" and Use Cases 0 and 1 establish the differences between ePower and eMandate. Both are eDocuments that can be stored in an eMandate Registry, thus becoming "records", i.e. evidence containers. The main difference between them is the following:
    - ePowers:
        - An ePower does not specify Mandatees, but only Powers assigned always to a natural person, thus is given the categorisation of Personal Power in the proposal of the EU Power Taxonomy (see section "3.4 The EU Powers taxonomy").
        - The empowered person could be seen as a Mandator acting on behalf of him/herself.
        - In principle, the Powers emerge from the fact that the empowered natural person is in a EU MS, i.e. s/he is a EU citizen or a EU resident. Therefore, Personal Powers cannot be explicitly constrained in an ePower. Any possible constraint on a Personal Power should be explicitly defined in a legal instrument.
        - The situation in which an authority invests a natural person with a Power and it is necessary to create an ePower could be treated as an eMandate where the Mandator is the authority (a natural or legal person) and the Mandatee is the natural person being empowered. However, this Power would not be considered a "Representation Power", but a "Personal Power". In this case, the Power could be constrained by the authority.
    - eMandates:
        - An eMandate should carry information about the Mandator, the Mandatee, the Powers of the Mandator, the Powers being assigned to the Mandatee (this is the notion of empowerment), possible constraints related to each Power, possible references to sources of evidences, and additional information.
        - In an eMandate, the Powers assigned to a Mandatee can be constrained at the time of creation (e.g. validity period, delegation/non-delegation flag, maximum level of delegation, financial thresholds, etc.); see Use Cases 2 and 3 for further details on this.

The example below covers only the creation of an eMandate. Use Case 0 – Cross-border user eAuthorisation – provides insight on how the creation of an ePower can be approached. The analysis made throughout this document suggests that the Data Model for eMandates (to be developed in Task 2) can be also applied to the instantiation of ePowers.

Example

A user that is a citizen of EU MS-A and resides in MS-A wants to receive an unemployment benefit from MS-B. This user lived and worked for a period of time in MS-B and has the right to apply for that benefit using SP-B (i.e. a service supplied by a public administration of the MS-B).

SP-B is a non-harmonised service that expects the use of an eMandate containing data required for that Member State and for that service (i.e. similar services in other MS would require different data and could have different constraints).

The figure below illustrates the information that would be required by this SP in the eMandate:

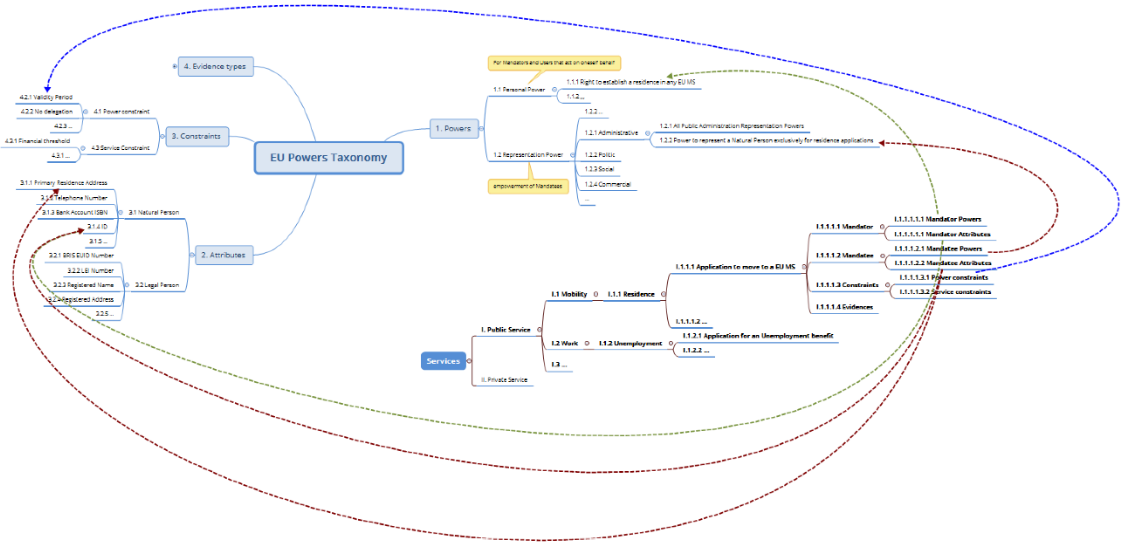


FIGURE 6: EXAMPLE OF DATA REQUESTED BY A NON-HARMONISED PUBLIC SERVICE

Pre-conditions

- The user (Mandator, in this case) is in a EU MS.
- The EU Powers Taxonomy is accessible online.
- The eMandate Registry is able to download or interact with the online EU Powers Taxonomy.
- The user knows how to access the MS-B National Service Catalogue where this specific service has been defined (because when trying to access the service, SP-B supplied the user with its URL). Alternative: it has been included in the EU Service Catalogue.

(See section “3.4 The EU Powers taxonomy”).

Possible flow

- The user (the Mandator) enters the eMandate Registry of a EU MS.
- The user uses an electronic device to identify him/herself and chooses to create an eMandate.
- The eMandate Registry identifies and authenticates the user and recognises his/her Power to create eMandates. Hence, it allows the user to access this specific service (creation of eMandates).
- The user selects the type of service s/he wants to access. This action provides the eMandate Registry System with the set of Powers, Constraints and Attributes that are required for the service (based on the National Service Catalogue and on the EU Powers Taxonomy).
- The user introduces the data about him/herself in the section about the Mandator. Following the example, these data would be:

    - EU Attribute code ("2.14") and data values for the type of Identification document and ID number (as defined in the EU Powers Taxonomy);
    - EU Power code ("1.1.1") and data value for the Mandator Power (right to establish residence in a EU MS, as defined in the EU Powers Taxonomy).

- The user introduces the data about the Mandatee. Following the example, these data would be:

    - EU Power code ("1.2.2") for the power assigned to the Mandatee (as defined in the EU Powers Taxonomy). This empowers the Mandatee to represent the Mandator exclusively for the purpose of applying for a residence (see figure above);
        - When assigning this Power code, the user specifies Power constraints. For example:
            - The user introduces the code ("4.2.1") and data value for the period of validity of the representation power (as defined in the EU Powers Taxonomy). Notice that this specific service requires the specification of the Power validity period (as defined in the National Service Catalogue, arc in blue colour from the service node "I.1.1.1.3.1 Power constraints" to the EU Powers Taxonomy node "4.2.1 Validity Period").
            - The user sets whether this Power can be delegated or not by the Mandatee onto another Mandatee in subsequent eMandates (see Use Case 3 – Delegation of Powers). For this, the user specifies the Service Catalogue Power Constraint code "I.1.1.1.3.1.1 No delegation possible" and the value "true" or "false" [31] . The user could also specify the depth of the delegation: "I.1.1.1.3.1.2 Max delegation level".
    - EU Attribute code ("2.1.4") and data values for the type of Identification document and ID number of the Mandatee (as defined in the EU Powers Taxonomy);
    - EU Attribute code ("2.1.2") and data value of the primary residence address (as defined in the EU Powers Taxonomy).

- Service-related constraints: some services may need special constraints; e.g. financial constraints of the type "The Mandatee can represent the Mandator in financial operations involving amounts below a threshold". In this case, the user would indicate the Service Constraint code "4.3.1 Financial threshold" followed by the threshold amount value.
- The user saves and signs electronically the eMandate.
- The eMandate Registry communicates with the Mandatee inviting him/her to sign the eMandate (this can be done in many different ways; one way could be an email containing a URL that, after identification and authentication of the Mandatee, redirects the Mandatee to the signature facility).
- Optionally (to be further analysed), the eMandate Registry seals the eMandate (the eMandate thus becomes a "record").

GDPR-related note:

[31] From the data modelling experience, one good practice is to define this as a "compulsory non-nillable Indicator" element. If so, the element is always present in the eMandate and cannot be left empty.

The Mandator and the Mandatee will need to explicitly consent in front of the eMandate Registry that their personal data can be shared for the purposes of the service(s) indicated in the eMandate.

ePower: summary, conclusions and further implications

The flow described above could also be used for harmonised services, both public and private. The difference would be that the Powers, Attributes and Constraints would be common for a given service in all EU MS or for all the organisations of a partnership (see Use Case 1 for more details about private partners).

3.10. Use Case 2.1 – Update of an eMandate

"**A Person in MS-A wants to modify or revoke an existing eMandate that is registered in MS-B**".

In principle, there should be little or no reason for the modification of an ePower, especially if we adhere to the principle that ePowers reflect the inherent rights of a natural person.

Nevertheless, updating an eMandate may imply one or more of the following operations:

- The modification of the value of certain data contained in an existing eMandate. The revocation of an eMandate can be seen as a subcase of this operation, as the "status" of an eMandate is one of these possible data.
- The addition of new Power Attributes, Constraints or references to sources of evidences.
- The removal of Power Attributes, Constraints or references to sources of evidences.
- The modification of an eMandate implies the creation of a new eMandate. "Temporal" eMandates should not exist. If they do, they cannot be used for eAuthorisation purposes. Therefore, if an SP succeeds in retrieving a temporal eMandate from a EU MS eMandate Registry (which should never happen), its validation should fail and the user access to the SP system should be rejected.
- One way of determining whether the eMandate is a record (i.e. not a temporal eDocument) is to verify whether it has been signed by all the parties involved in the empowerment. Additionally (or alternatively), the eMandate could contain a "status" code, and even a "content version identifier" [32].
- The modification of an eMandate does not necessarily deactivate the previous version of the eMandate. This is an easy way of creating "copies" of the Mandates for different purposes[33].

Example

[32] An "ePower/eMandate Status Type" Code List should be prepared in Task 2. Possible candidate codes could be: "Active", "Revoked", "Working version". Be aware that "Expired" would not be an appropriate choice, as the expiration due to time limitation is an attribute applicable to each Power, not to the eDocument. Whilst modelling the ePower/eMandate, consider also: 1) versioning the content (current version ID); and 2) referring to the previous version (previous version ID) plus the previous version eDocument URL or identifier. This facilitates the "historification" and tracking of families of eDocuments.

[33] This suggests that the Data Model should facilitate the possibility of describing these purposes, e.g. with Title and Description fields. This would facilitate the management of the eMandates by the user when creating or updating eMandates in the eMandate Registry.

A natural person (the Mandator) wants to retrieve an existing eMandate and extend the period of validity of one of the Powers assigned to one Mandatee (an eMandate could carry more than one Mandatee).

Pre-conditions

- The user (Mandator in this case) is in a EU MS.
- The EU Powers Taxonomy is accessible online.
- The eMandate Registry is able to download or interact with the online EU Powers Taxonomy.

(See section "3.4 The EU Powers taxonomy").

Possible flow

- The user (the Mandator) enters the eMandate Registry of a EU MS.
- The user uses an electronic device to identify him/herself and chooses to update an eMandate.
- The eMandate Registry identifies and authenticates the user and recognises his/her Power to modify and create eMandates. Hence, it allows the user to access this specific service (updating of eMandates). This suggests that many of the features used for the creation of the eMandate can be reused for its update.
- The eMandate Registry presents the user with the existing eMandates that s/he can modify.
- The user modifies, removes or adds the data values s/he is interested in.
- The user saves and signs electronically the new version of the eMandate[34].
- The eMandate Registry communicates with the Mandatee, inviting him/her to sign the new eMandate.
- Optionally (to be further analysed), the eMandate Registry seals the new eMandate (the eMandate thus becomes a new "record").

GDPR-related note:

Same as for Use Case 2 – Creation of an eMandate.

ePower: summary, conclusions and further implications

None beyond those already described in previous Use Cases.

3.11. Use Case 3 – Delegation of Powers

"**A Mandatee, with the Power to delegate[35], assigns the Power of the Mandator to another Mandatee**".

[34] In relation to the versioning, different strategies may be applied by eMandate Registry System. Thus, the version ID, status and link to the previous eMandate could be assigned automatically by the eMandate Registry System, thereby avoiding possible human errors. However, the user should have the option of deciding whether the new eMandate is an evolution of the previous one (and therefore needs to be re-versioned and linked) or if it needs to be considered a totally new eMandate (in which case it would be statused and versioned as a totally new eMandate, not linked to any previous eMandates). In any case, the Data Model must allow all these variants.

[35] The "Power to delegate" can be defined as a type of Representation Power (i.e. for Mandatees) that needs to be defined in the EU Powers Taxonomy.

This use case implies that:

- There is no exchange of information between an SP and an eMandate Registry. Therefore, this is not a true "cross-border interoperability" scenario (according to the definition convened in this document, see section "3.1 Cross-border interoperability").
- The data regarding the Mandator at the origin of the first empowerment should be referred to in the eMandate. This would facilitate the discovery of linked eMandates and the cross-checking of the data regarding the Mandator and all the Mandatees.

Example

A legal person (the Mandatee) that was previously empowered with the EU Power code "1.2.1 All Public Administration Representation Power" wants to delegate this power to a third legal person (the sub-Mandatee[36]).

Pre-conditions

- All EU MS have one or more eMandate Registries for public and private services.
- The user is a Mandatee for which an eMandate exists, in at least one EU MS eMandate Registry. As the user is a Mandatee, this also implies that the user is in a EU MS (see previous Use Cases).
- The EU Powers Taxonomy exists and is available online (See section "3.4 The EU Powers taxonomy").
- A Service Catalogue also exists and is available online (EU or national, see section "3.4 The EU Powers taxonomy").
- The Power Constraint "No delegation possible" exists in the Service Catalogue; e.g.:

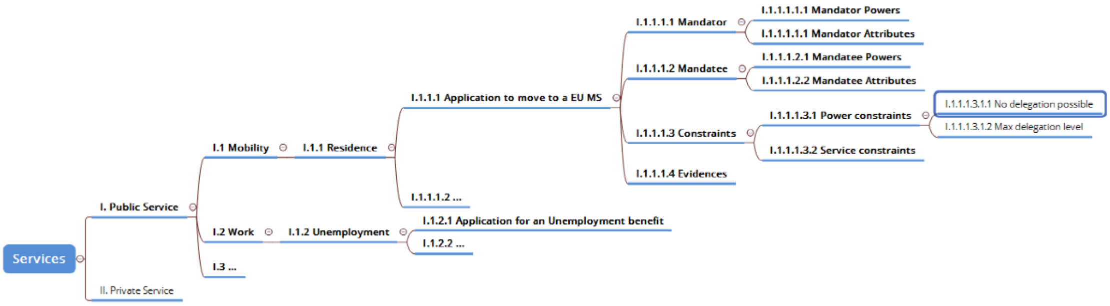

Services
I. Public Service
II. Private Service
I.1 Mobility
I.1.1 Residence
I.2 Work
I.1.2 Unemployment
I.3 ...
I.1.1.1 Application to move to a EU MS
I.1.1.1.2 ...
I.1.2.1 Application for an Unemployment benefit
I.1.2.2 ...
I.1.1.1.1 Mandator
I.1.1.1.2 Mandatee
I.1.1.1.3 Constraints
I.1.1.1.4 Evidences
I.1.1.1.1.1 Mandator Powers
I.1.1.1.1.1 Mandator Attributes
I.1.1.1.2.1 Mandatee Powers
I.1.1.1.2.2 Mandatee Attributes
I.1.1.1.3.1 Power constraints
I.1.1.1.3.2 Service constraints
I.1.1.1.3.1.1 No delegation possible
I.1.1.1.3.1.2 Max delegation level

FIGURE 7: NO DELEGATION POSSIBLE (POWER CONSTRAINT, IN THE SERVICE CATALOGUE)

- The data needed to access the original eMandate and the subsequent delegation eMandates is accessible online.

Possible flow

- The user enters the eMandate Registry System and identifies him/herself.
- The eMandate Registry identifies and authenticates the user; eIDAS infrastructure could be used for this purpose.
- The user selects the eMandate Registry feature "Delegation of Powers".

[36] This suggests that, in the Data Model, Mandatees can be characterised by a quality such as "Power Delegation Level" (or similar, to be analysed) to indicate whether the Mandatee obtained the Power directly from the Mandator (Level 0, for example, meaning "no delegation") or from another Mandatee (Level 1 → empowered by a Mandatee, Level 2 → empowered by a sub-Mandatee of Level 1). This could facilitate the systems to obtain all the eMandates that need to be validated.

- The user is required to supply the following data:
    - The identifier of the eMandate that empowers him/her to represent the Mandator;
    - Data about the Mandatee that will be assigned all or part of the Powers originally assigned to the user (e.g. the type of ID document and ID number. Specific non-harmonised services may require other Attributes about the Mandatee; see Use Case 2 – Creation of an eMandate for details on how a national non-harmonised service can define service-specific Attributes);
    - The Powers that have to be assigned to the sub-Mandatee (Mandatee of Level 1);
    - Per each Power, the user may specify constraints; e.g.: period of validity of the Power; whether it can be re-delegated or not; Maximum number of delegation levels; etc. For this, the user specifies the Service Catalogue Power Constraint codes "I.1.1.1.3.1.1 No delegation possible", "I.1.1.1.3.1.2 Max delegation level" and values (e.g. true and 3 levels max.)[37].
- The user saves and signs electronically the eMandate.
- The eMandate Registry communicates with the original Mandator and the new sub-Mandatee (of Level 1), inviting them to sign the eMandate (this can be done in many different ways; one way could be an email containing a URL that, after identification and authentication, redirects the Mandator and sub-Mandatee to the signature facility).
- Optionally (to be further analysed), the eMandate Registry seals the eMandate (the eMandate thus becomes a "record").

GDPR-related note

There would be the need for all natural persons involved in the delegation to explicitly consent in front of the eMandate Register[38] in order for the eMandate Register to share their personal data with the SPs.

ePower: summary, conclusions and further implications

It is debatable whether the Service Constraints exist or not. It may be that what is it named here "Service Constraint" in both taxonomies (Powers Taxonomy and Service Catalogue) does not actually exist and all constraints are "Power Constraints". The "financial threshold", for example, could be expressed in both taxonomies as sub-nodes of the nodes "EU Powers Taxonomy/3. Constraints" and "Service Catalogue/ I.1.1.1.3 Constraints". This shall be re-analysed in Task 2.

3.12. Architecture

This section analyses the architectural approaches adopted by several trans-European systems and recapitulates on the MS national solutions. Based on these experiences and other solutions

[37] This already offers several insights for the data modelling task: 1) the taxonomies need to be identified in the metadata of each code; which is a common practice in XML standards and ontologies (e.g. use of ISO 15000 ebXML CCT); and 2) the combination of "No delegation possible" and "Max delegation level" casts several business rules: "if no delegation possible → max delegation level is not present or max delegation equals 0; else → max delegation level compulsory and max delegation > 0".

[38] The authority responsible for the information being registered, may not be the same organisation as the one that manages the Registry System. See section "2.4 Definitions".

not directly related to the objectives of this project, a proposal is put forward for the federation of the sources of information on eMandates.

For further details, please refer to the original source of these works, cited in the footnotes of the present document.

The architecture depends on the assurance that the business capabilities are available and well-coordinated. Its functioning also depends on the expected implementation and the reliability of the stakeholders' business capabilities, as well as the correct use of the generic and specific enablers and business processes, workflows and artefacts.

The understanding of how the architectural approach supports the business processes helps clarify (and elicit) the information requirements and business rules necessary to incept the data model; i.e. to ensure the **semantic interoperability**[39].

In the end, the architectural approach and solutions have to face one important challenge: to prove that it effectively and efficiently supports the **organisational interoperability**.

Several architectural approaches directly or indirectly related to eMandates were studied. The following sub-sections briefly describe these approaches.

3.12.1. Solutions analysed

3.12.1.1. STORK 2

At the core of the STORK 2 architecture lie two main systems, the PEPS (Pan-European Proxy Servers) and the V-IDP (Virtual ID Provider)[40].

[39] Hence the UN/CEFACT UMM (Universal Modelling Methodology) takes the domain processes as the basis for the identification of the requirements for the transactional information (https://www.unece.org/cefact/umm/umm_index.html).

[40] See "D4.10 Final version of Technical Design" (https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=71:d410-final-version-of-technical-design&Itemid=174&start=5) and "D4.11 Final Version of Technical Specifications for the cross-border interface" (https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=64:d411-final-version-of-technical-specifications-for-the-cross-border-interface&Itemid=174&start=5).

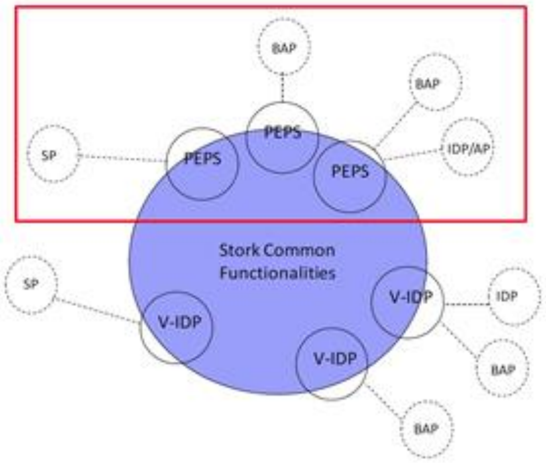


FIGURE 8: STORK 2 GENERIC ARCHITECTURAL APPROACH

In each instance of PEPS, there are three roles: one that attends to SP[41] requests, one in the country that issued the ID that the citizen wants to use, and one in another country where the user may have domain-specific Attributes.

For each request received, the first role (S-PEPS) forwards the request to his/her colleague PEPS or V-IDP, and the second role (C-PEPS) resolves the request received from his/her colleague PEPS or V-IDP. If in this request any domain-specific Attributes (BA) are included, the user is prompted to indicate the Attribute Provider (AP), or alternatively the country in which they can be found. In the latter case, the user is redirected to the A-PEPS of that country, which will allow him/her to indicate from which APs those Attributes can be retrieved.

A V-IDP fulfils the same basic objectives as the PEPS:

- They both form anchors of trust, which elevate the national circles of trust to European level; and
- They both hide country-specific aspects like organisation, available ID providers and national and domain-specific Attribute providers, offering only standardised data through a standardised interface.

In the context of eMandates, the national eMandate Registries would fulfil a similar role to the one played by the STORK 2 V-IDPs.

There are four use cases offered by the STORK 2.0 system, and they are closely related to the use of eMandates:

[41] E.g. a public administration asking for identification and authorisation to access one of its online public services.

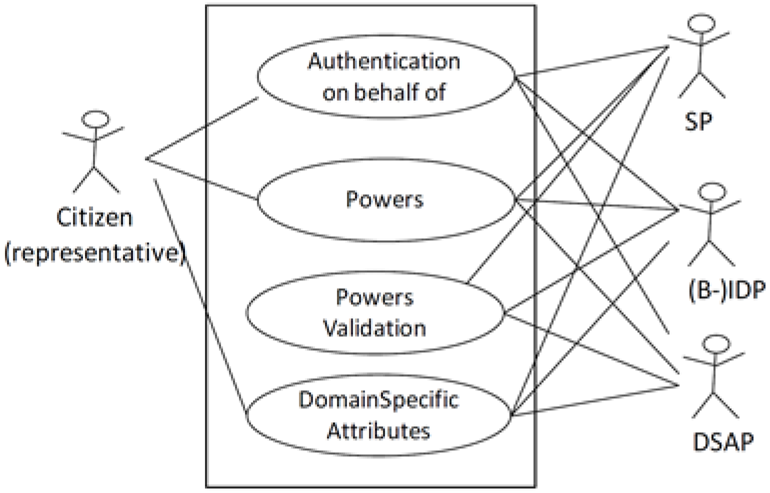
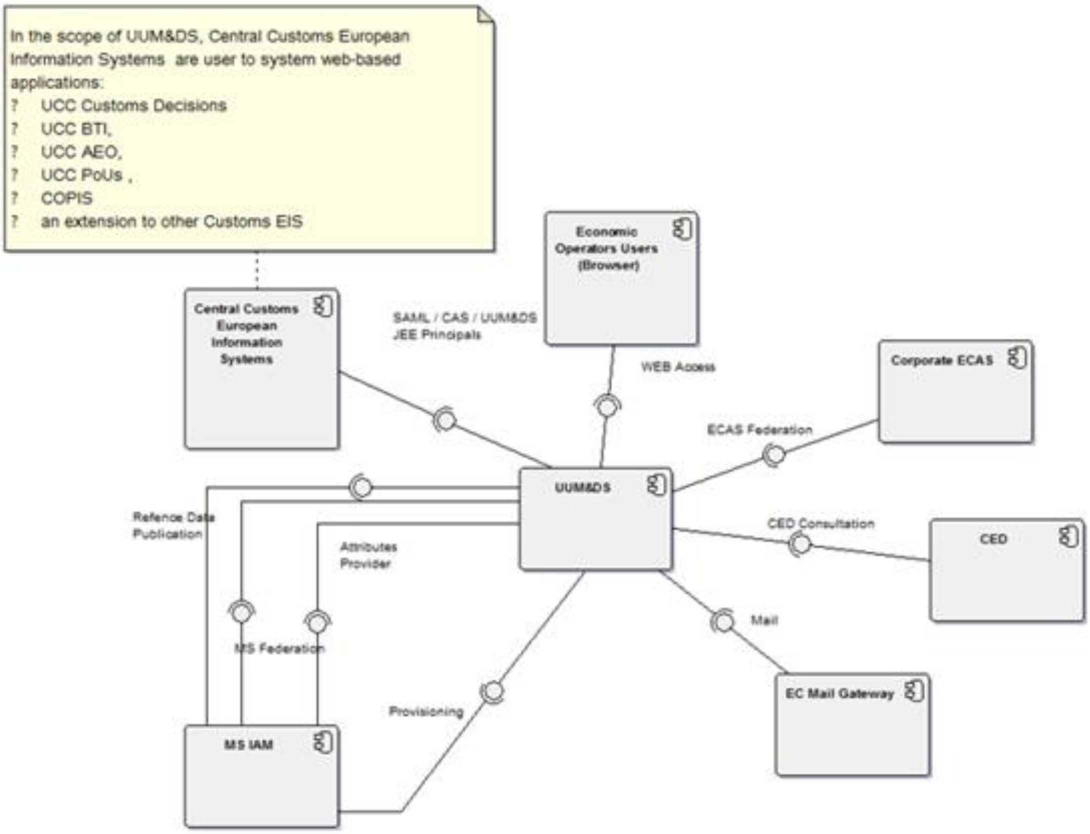


FIGURE 9: USE CASEUSE CASEUSE CASEUSE CASE VIEW OF THE STORK 2.0 CORE

3.12.1.2. UUM&DS

TAXUD's Uniform User Management and Digital Signatures (UUM&DS) Project enables the provision of a single trader interface by implementing secure authorised access for Economic Operators and their representatives to Customs European Information Systems (EIS).

The figure below presents the IT systems and applications with which the UUM&DS system interacts and exchanges information:


In the scope of UUM&DS, Central Customs European Information Systems are user to system web-based applications:

? UCC Customs Decisions
? UCC BTI,
? UCC AEO,
? UCC PoUs ,
? COPIS
? an extension to other Customs EIS

FIGURE 10: UMM&DS SYSTEM INTERACTIONS WITH IT SYSTEMS AND APPLICATIONS

- **Economic operators as users**: Economic operators access UUM&DS web-based services and Central Customs EIS (UCC Customs Decisions, UCC BTI, UCC AEO, UCC PoUs, COPIS and other future Central Customs EIS) using a browser, through the web access interface.
- **Central Customs European Information Systems (EIS)**: UUM&DS enables secure authorised access for economic operators and their users to the Central Customs EIS as defined in the Multi-Annual Strategic Plan (MASP) of DG TAXUD and in the Union Customs Code (UCC) Work Programme.
- **ECAS**: ECAS is the European Commission Authentication Service. This portal will be used and federated by UUM&DS to authenticate EC officials through the ECAS Federation interface.
- **CED**: CED is the Commission Enterprise Directory and it is consulted by UUM&DS to obtain information about EC officials and existing ECAS accounts through the CED consultation interface.
- **EC Mail Gateway**: EC Mail Gateway provides mail facilities used by UUM&DS to send notifications through the Mail interface.
- **MS IAM**: MS IAM is the group of components of the national domain that perform the integration with UUM&DS. The details of this component and the interfaces used with UUM&DS may vary based on the situation of the Member States.
    - The **Reference Data Publication** is an interface that allows the Member State to retrieve UUM&DS reference data, needed to create the proper authentication assertion or to provision the proper data into UUM&DS.
    - The **Provisioning** interface is used by MS that don't have an IAM and that choose to provision their users into UUM&DS.
    - The **Federation** interface is used to federate the MS IAM with UUM&DS. It is used both for the authentication, and optionally for the user's information (Attributes).
    - The **Attributes Provider** interface is used to provide user information separately from the Federation interface. It represents the technical means to provide this information.

UUM&DS integrates with three types of MS Identity and Access Management Systems:

- **Type A**: MS with one consolidated IAM for the authentication and authorisation of economic operators that can directly integrate with the UUM&DS system. They will use the **MS Federation** and **Reference Data Publication** interfaces to integrate with UUM&DS.

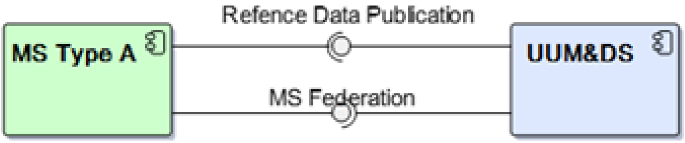


FIGURE 11: TYPE A MS INTEGRATION

- **Type B**: MS with one IAM for authentication only (e.g. National IAM for authentication) and a complementary authorisation system that can integrate with the UUM&DS system. This type will use the MS Federation interface combined with the Attributes Provider interfaces.

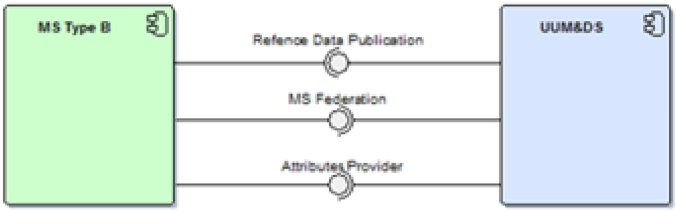


FIGURE 12: TYPE B MS INTEGRATION

- **Type C**: MS with multiple IAMs for the authentication and the authorisation of users. MS shall provide a unified IAM with a common authentication portal in order to integrate with the UUM&DS system. They integrate to UUM&DS using the same interfaces as in Type A: MS Federation and Reference Data Publication.

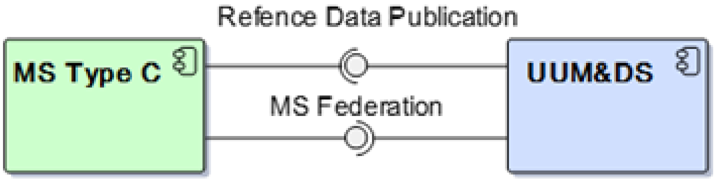


FIGURE 13: TYPE C MS INTEGRATION

3.12.1.3. TOOP

The Once - Only Principle Project (TOOP)[42] is an initiative of 50 organisations from the EU and associated countries to explore and demonstrate the once-only principle on a cross-border scale with the aim to reduce the administrative burden of businesses and public administrations.

The once-only principle (OOP) needs to be seen in the context of public sector digitalisation. It means that citizens and businesses provide diverse data only once in contact with public administrations, while public administration bodies take actions to internally share and reuse these data – even across borders – always respecting data protection regulations and other constraints.

The OOP concept focuses on reducing the administrative burden for individuals and businesses by re-organising public sector internal processes, instead of making citizens and business users adjust to existing procedures.

One of the main technical principles for the development of OOP architecture is the reuse of existing frameworks and building blocks provided by CEF, e-SENS, and other initiatives. The TOOP generic federated OOP architecture relies on frameworks such as the European Interoperability Reference Architecture (EIRA)[43], the CEF Building Blocks[44], and the e-SENS deliverable "D6.6 e-SENS European Interoperability Reference Architecture"[45], among others.

[42] http://toop.eu
[43] https://joinup.ec.europa.eu/catalogue/distribution/eira_v1_1_0_overviewpdf
[44] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home
[45] https://www.esens.eu/deliverables?page=3

For the architectural approach, TOOP reuses the eDelivery n-Corner Model[46]. The high-level architecture diagram below depicts the scope of the main building blocks for a general OOP architecture - eDelivery 4 Corner Model. It is highly scalable and eliminates the risks of a single point of failure and service provider lock-in.

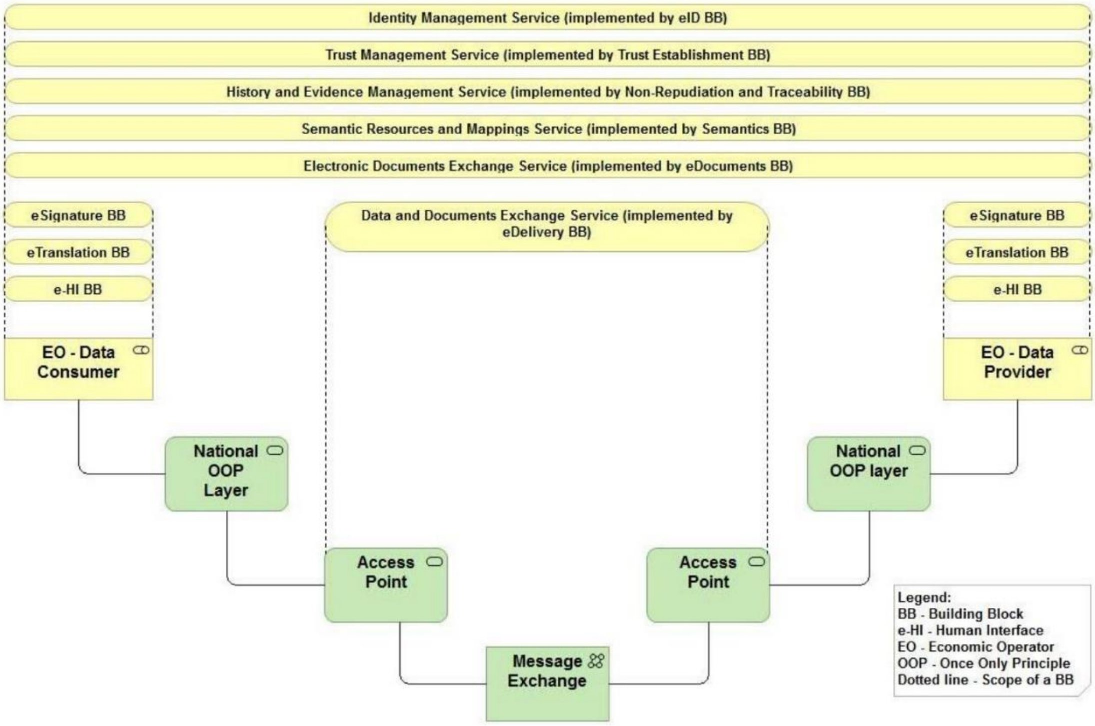

Identity Management Service (implemented by eID BB)
Trust Management Service (implemented by Trust Establishment BB)
History and Evidence Management Service (implemented by Non-Repudiation and Traceability BB)
Semantic Resources and Mappings Service (implemented by Semantics BB)
Electronic Documents Exchange Service (implemented by eDocuments BB)
eSignature BB
eTranslation BB
e-HI BB
Data and Documents Exchange Service (implemented by eDelivery BB)
eSignature BB
eTranslation BB
e-HI BB
EO - Data Consumer
EO - Data Provider
National OOP Layer
National OOP layer
Access Point
Access Point
Message Exchange
Legend:
BB - Building Block
e-HI - Human Interface
EO - Economic Operator
OOP - Once Only Principle
Dotted line - Scope of a BB

FIGURE 14: HIGH-LEVEL VIEW OF OOP ARCHITECTURE (EDELIVERY 4 CORNER MODEL)

In this architecture, each national OOP layer would provide transparent access to the eMandates Provider System.

In CEF eDelivery, Message Exchange is the main use case that is implemented by an access point software component that supports the standards and profiles which message exchange defines and endorses for generic use. The main goal is to promote interoperability, security, scalability, legal assurance and accountability for exchanging of documents and/or data. The endorsed standards are the e-SENS profile OASIS AS4 and the OpenPEPPOL profile of AS2 IETF36. A CEF eDelivery AP (Application Profile) is an implementation of the AS4 Profile developed by e-SENS or of the AS2 Profile developed by OpenPEPPOL. AS4 is an open technical specification for the secure and **payload-agnostic exchange of data** using web services.

From the backend perspective, the actors are the end entities (EEs) which connect to the gateway of the 4-Corner Model used in e-SENS. The Backend Integration ABB facilitates the connection between the national infrastructure and the e-SENS infrastructure.

[46] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/What+is+eDelivery+-+Overview

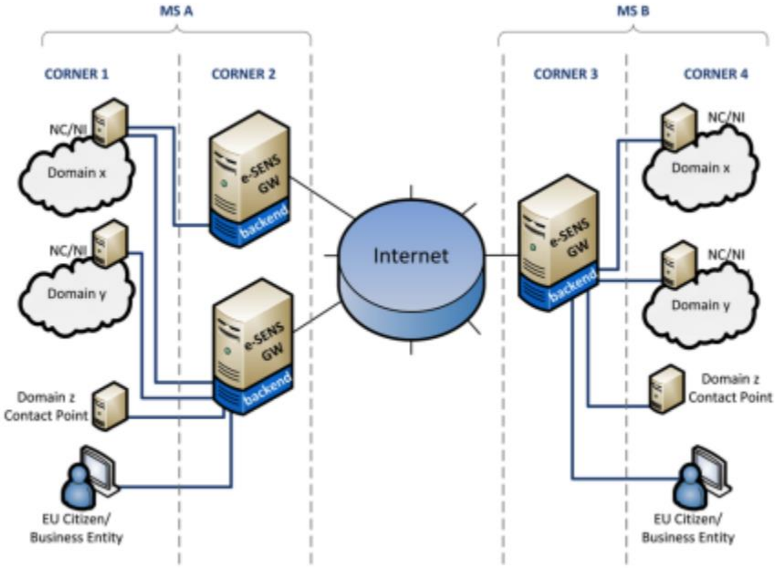


FIGURE 15: TOOP BACKEND INTEGRATION TOPOLOGY

3.12.1.4. eIDAS

The components necessary to achieve the interoperability of notified eID schemes are defined in the document "eIDAS – Interoperability Architecture". This document specifies the requirements laid out in the eIDAS Implementing Act[47].

In eIDAS, interoperability of different eID-schemes is achieved via the technical interfaces between eIDAS-Connectors and eIDAS-Services, collectively eIDAS-Nodes. The interfaces between the eIDAS-Connector and the relying parties, and between the eIDAS-Services and the eID-scheme are part of the national system of the Receiving MS and the Sending MS, respectively.

Sending MS can choose between two integration scenarios for their eID-scheme:

a) **Proxy-based**: The Sending MS operates an eIDAS-Proxy-Service, relaying authentication requests and authentication assertions between an eIDAS-Connector operated by the Receiving MS and the eID scheme of the Sending MS.
b) **Middleware-based**: In this scenario, the Sending MS does not operate a proxy for the purpose of authentication of persons to relying parties of other MS. The Sending MS provides a middleware to other MS, which is operated by the operator(s) of the eID-Connector(s) of the Receiving MS. A MS notifying their eID scheme as a middleware-based scheme MUST provide the necessary middleware to the Receiving MS

Each Receiving MS operates one or more eIDAS-Connectors. It is up to the Receiving MS to decide on the national deployment of Connectors. Connectors do not need to be operated by the MS itself, but can also be operated by public and/or private relying parties established in that MS. MS operating exactly one Connector are called Centralised MS, while those operating several Connectors are called Decentralised MS. An eIDAS-Connector is operated together with eIDAS-Middleware-Services for communication with middleware-based eID schemes.

[47] eIDAS IF: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002

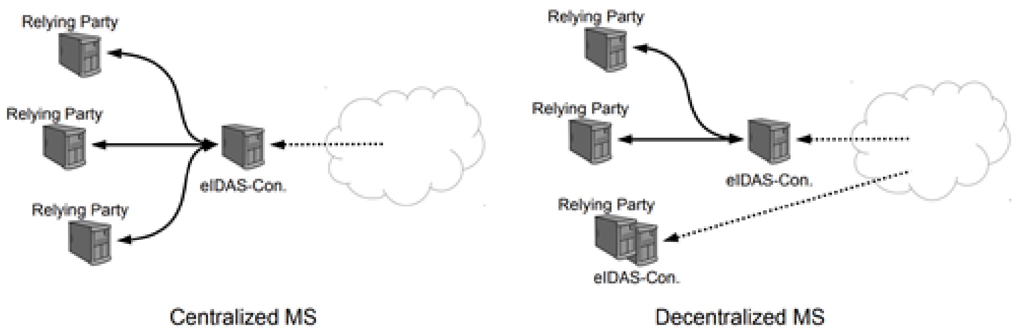


FIGURE 16: EIDAS CENTRALISED AND DECENTRALISED DEPLOYMENT OF EIDAS NODES

An eIDAS-Connector MAY provide additional services, (e.g. signature services). Centralised MS notifying their own eID-scheme as a proxy-based scheme MAY operate their eIDAS-Connector and their eIDAS-Proxy-Service as an integrated deployment. Receiving MS MUST ensure that personal identification data received via an eIDAS-Connector is processed according to applicable data protection legislation. This means that data MUST NOT be forwarded to unidentified peers.

Centralised MS notifying their own eID-scheme as a proxy-based scheme MAY operate their eIDAS-Connector and their eIDAS-Proxy-Service as an integrated deployment.

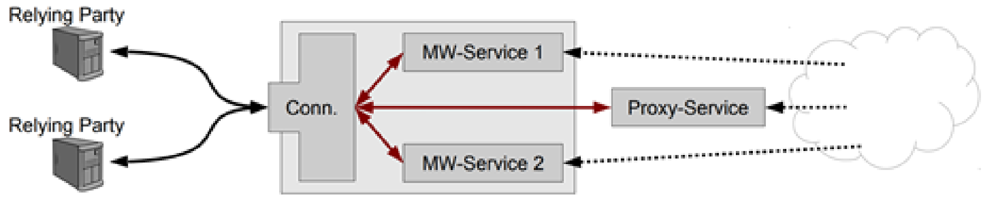


FIGURE 17: EIDAS COMPONENTS

The eIDAS interoperability framework including its national entities (eIDAS-Connector and eIDAS-Service) is able to exchange personal and technical Attributes to support cross-border identification and authentication processes. For the exchange of messages, it uses the SAML 2.0 specification.

During the interviews with the MS, they all stated that the natural way forward to the development of a cross-border eMandates exchange should be the extension of the current eIDAS infrastructure. Some of them said that they would eagerly support the promotion of a specific EU legal framework oriented to enforce this approach.

3.12.1.5. Member States

The current situation is that, except for a few cases[48], the Member States do not authorise other MS users into their systems and do not exchange information about empowerments.

[48] E.g. Finland and Estonia through X-Road, the Netherlands and Belgium for specific sectorial needs (farming and agriculture).

Nonetheless, they recognise the convenience and need for a cross-border exchange of Mandates.

As they do not have to exchange this information, they tend to centralise the management of eMandates. Under legally controlled environments, this is not only possible but also convenient.

There are a few exceptions to this centralised paradigm, like Spain. The reason for these exceptions lies precisely in the decentralised model of their competencies in different governments and their respective public administrations.

The section below graphically summarises the architectural approaches developed for the European initiatives and MS analysed. The document "RPaM-State-of-affairs of EU eMandate Systems-v2 0" presents a more detailed explanation on how the analysed MS are legally and administratively organised and which architectural solutions they have developed.

3.12.2. Comparative analysis

3.12.2.1. EU initiatives

	STORK	UMM&DS	TOOP	eIDAS
	Federative architecture?			
	YES	YES	YES	YES

3.12.2.2. MS eMandate Registries

	AT	BE	FI	NL	ES
One centralised eMandate Registry?					
	YES	NO	YES	YES	NO
National eMandate Registries interoperate amongst themselves?					
	NO	NO	NO	NO	YES

- Belgium does not have one central eMandate Registry, it has developed up to three sector-specific eMandate Registries, which do not exchange information between themselves.
- Spain has three different sectorial independent eMandate Registries (Administrative, Judicial and Notaries). For administrative purposes, different governments (regional and central) are interconnected (via web-services) to the central eMandates repository (@Podera) and exchange eMandates using a common vocabulary.

3.12.3. Proposals

3.12.3.1. Ad-hoc architecture

An ad-hoc architectural approach and development is **NOT recommended**. By "*ad-hoc*" we mean:

- An architectural solution developed from scratch (even if reusing existing building blocks (BB) and digital service infrastructures (DSI)); and
- Exclusively dedicated to implement the authorisation to the SP.

The reasons are many and obvious, and include the following:

- Legally unviable (and politically incorrect), very difficult to defend;
- Too costly in terms of organisational interoperability and economic investment;
- Operational solutions exist that are totally aligned with the objectives of this project.

It could be tempting to consider a centralised architectural approach. However, given the political, legal and organisational complexities of the European Union environment, such a solution would be **impossible to implement in practice**. By “*centralised”* we mean essentially two things:

- A platform that would store all the e-Mandates issued in all MS (legally impossible and technically complex);
- All services related to the creation, modification, validation, revocation of the eMandates would fall under the responsibility of the European Commission (violation of the principles of subsidiarity and proportionality).

3.12.3.2. Federated solution

All the solutions studied, that took into account the need for eMandates, approached the architectural solution as a federation of cross-border systems.

Except for TOOP, all these solutions were based on STORK 2 achievements.

Our proposal is to **reuse and extend the eIDAS infrastructure**. Even TOOP integrates eIDAS as an alternative service, which would mean that if eIDAS were used to implement the cross-border federation of eMandates, TOOP would immediately benefit from it.

The extension to which we refer would affect two main aspects of the eIDAS solution:

a) **The eIDAS SAML Attribute profile**: For sectorial specific needs, the eIDAS specification invites experts to “develop additional Attribute schemata describing the type and usage of these Attributes for inclusion in Member State eIDAS Node metadata[49]”. However, it also specifies that some principles should be observed for the development of specific Attribute schema. Amongst them:

   - The principle of data minimisation shall be observed;
   - Complex data structures should be avoided;
   - Other, up to five including an indication on the governance of the inclusion of new Attributes[50].

   This invitation to extend the set of Attributes and the five general principles could both be taken as a paradigm of what could be done for the extension the eIDAS Attribute profile with two SML-based eIDAS Attributes:

TABLE 2: NEW EIDAS ATTRIBUTE ISUSERMANDATEE

```
<saml:Attribute    FriendlyName="IsUserMandatee"
            Name="http://eidas.europa.eu/Attributes/Mandates/IsUserMandatee"
            NameFormat="urn:osis:names:tc:SAML:2.0:attrname-format:uri">
```

[49] eIDAS SAML Attribute Profile, p. 23:
https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Profile

[50] See point 5 about the publication of a new Attribute schema and the role of the CEF eIDAS Technical Subgroup (eIDAS SAML Attribute Profile, op.cit. p. 23).

```
            <saml:AttributeValue xsi:type=”eidas:IsUserMandatee”>true</saml: AttributeValue >

</saml:Attribute>
```

TABLE 3: NEW EIDAS ATTRIBUTE MANDATE

```
<saml:Attribute    FriendlyName=”Mandate”
Name=”http://eidas.europa.eu/Attributes/Mandates/Mandate”
NameFormat=”urn:osis:names:tc:SAML:2.0:attrname-format:uri”>

            <saml:AttributeValue
xsi:type=”eidas:Mandate>PGVpZGFzOkxvY2F0b3JEZXNpZ25hdG9yPjIyPC9laWRhczpMb2N
hdG9yRGVzaWduYX
Rvcj48ZWlkYXM6VGhvcm91Z2hmYXJlPkFyY2FjaWEgQXZlbnVlPC9laWRhczpUaG9y
b3VnaGZhcmU+DQo8ZWlkYXM6UG9zdE5hbWU+TG9uZG9uPC9laWRhczpQb3N0TmFtZT
4NCjxlaWRhczpQb3N0Q29kZT5TVzFBIDFBQTwvZWlkYXM6UG9zdENvZGU+
Rvcj48ZWlkYXM6VGhvcm91Z2hmYXJlPkFyY2FjaWEgQXZlbnVlPC9laWRhczpUaG9y
b3VnaGZhcmU+DQo8ZWlkYXM6UG9zdE5hbWU+TG9uZG9uPC9laWRhczpQb3N0TmFtZT
Rvcj48ZWlkYXM6VGhvcm91Z2hmYXJlPkFyY2FjaWEgQXZlbnVlPC9laWRhczpUaG9y
b3VnaGZhcmU+DQo8ZWlkYXM6UG9zdE5hbWU+TG9uZG9uPC9laWRhczpQb3N0TmFtZT
4NCjxlaWRhczpQb3N0Q29kZT5TVzFBIDFBQTwvZWlkYXM6UG9zdENvZGU-
Rvcj48ZWlkYXM6VGhvcm91Z2hmYXJlPkFyY2FjaWEgQXZlbnVlPC9laWRhczpUaG9y
b3VnaGZhcmU+DQo8ZWlkYXM6UG9zdE5hbWU+TG9uZG9uPC9laWRhczpQb3N0TmFtZT
4NCjxlaWRhczpQb3N0Q29kZT5TVzFBIDFBQTwvZWlkYXM6UG9zdENvZGU+ </saml:
AttributeValue >

</saml:Attribute>
```

Notice that:

- The first Attribute (“IsUserMandatee”) could be considered unnecessary: if the response to the Attribute “Mandate” is null then the Relying Party may infer that the user is a person acting on behalf of him/herself, and vice-versa;
- The value of the Attribute “Mandate” is a B64 coded string. This is an eIDAS requirement for non-simple structured data[51]. All **the content of the eMandate should be modelled separately and bound (or not) to a syntax different to SAML** 2.0. See section “3.14 Data model”.
- The Attribute “Mandate” was already identified as a need[52] in STORK 2: `<stork:RequestedAttribute Name=http://www.stork.gov.eu/1.0/Mandate>`
- Other Attributes of the eIDAS `<saml2p:Extensions>` can be also necessary in the case of eMandates, e.g. the `<eidas:SPType>` element to identify whether the SP requester is from the private or the public sector.

[51] See Section “2.2.3 Responding Attributes” of the eIDAS Message Format specification, https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_message_format_v1.0.pdf

[52] See “D4.11 Final version of Technical Specifications for the cross border Interface”: https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=64:d411-final-version-of-technical-specifications-for-the-cross-border-interface&Itemid=174

b) **The process flow**: the eIDAS Interoperability Architecture specification[53] lists up to six steps for the user authentication in front of an SPsystem. To this list, some additional steps should be considered, e.g.:

- The eIDAS-Connector (interfaced to the Relying Party System) would request whether the user is acting on behalf of another person or his/her own behalf;
- If the user is acting on behalf of another person the eIDAS-Connector would assume that the user is the Mandatee.
- If the user is acting on behalf of another person, the eIDAS-Connector would need to request from the selected MS either the user's eMandate or a certification that the person behind the user fulfils all the criteria necessary to access the Relying Party Service (see section "3.13 Recognition" for a detailed explanation of these two approaches);
- In principle, the eIDAS-Service (interfaced to the eMandates System) would not need to verify the authenticity of the request, as this is already done during the authentication phase;
- In principle, the eIDAS-Service would not need to verify the authenticity of the persons referred to in the eMandate, as this is done upon eMandate creation, on the side of the eMandate Registry;
- However, the eIDAS-Connector may want to cross-authenticate the persons referred to in the eMandate or in information associated to the response. For this, a separate workflow could be designed.

The technological infrastructure proposal – based on eIDAS-Nodes, eIDAS-Connectors and eIDAS-Middleware-Services, plus the interfaces between eIDAS-Connector and Relying Parties and eIDAS-Services – could be used as it is now and would not be impacted whatsoever for the purposes of the cross-border exchange of eMandates or eMandates-related evidences.

However, it may be necessary to review some minor technical restrictions, like the limitations related to the size of the SAML2 request and response messages.

Something to consider is whether the eIDAS federative solution, namely the SAML Attribute Profile, should be used to handle all the use cases related to cross-border eMandate management or not.

3.12.3.3. Centralised architectural approach

The SWOT analysis below, inspired by the analysis performed in TAXUD's UUM&DS project, illustrates why **a centralised approach is not viable**:

TABLE 4: SWOT ANALYSIS OF AN EMANDATE CENTRALISED ARCHITECTURE

Strengths	Weaknesses
• Central implementation: maximum control; facilitates the development of the organisational, semantic and technical interoperability.	• Central system would have to be newly implemented: it would require an ad-hoc development.

[53] See the documentation available on Joinup, e.g. https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_interoperability_architecture_v1.00.pdf

	• MS would not benefit from investments already made. • MS would need to adapt the way they work to the new central solution→ high resistance from the MS. • Doubled replication and maintenance of the eMandates and national services. • High implementation cost. • Would need to implement a special integration with the European eIdentification solution.
Opportunities	**Threats**
• Secure environment, especially for specific domain area purposes where security may be relevant, such as taxation or health.	• Slow adoption from MS. • Additional stress to the central systems in regards to performance and security (Single Point of Failure).

3.12.3.4. Federated architectural approach

The SWOT analysis below lists the main strengths and opportunities of the federated approach and also of some of its challenges (weaknesses and threats):

TABLE 5: SWOT ANALYSIS OF THE FEDERATED ARCHITECTURAL APPROACH

Strengths	Weaknesses
• Redundancy (no Single Point of Failure). • Additional level of data security. • MS keep their existing investments. • Administration is limited to a minimum. Only one registration of eMandates and related information is needed, at the MS side.	• In order to guarantee the new functionality and quality of services, implementation effort is required.
Opportunities	**Threats**

• Enhances currently offered, proved and accepted solutions. • Ability to incorporate further federated services. • MS are eager to adopt the extension of eIDAS for eMandates and would not mind adapting their systems if that option was offered to them[54]. All the interviewed MS are already aligned to the eIDAS Regulation and infrastructure or are about to become aligned.	• Requires coordination of multiple involved stakeholders. • No EU legal support at the present time.

3.13. Recognition

In terms of business processes related to the use of cross-border and cross-sector eMandates, a fundamental question needs to be answered upfront: where should the recognition of the eMandate happen, and how? Is it for the specific SP to impose the authorisation criteria and evaluate the eMandate or, instead, should the SP rely on the cross-border eMandate system on the basis of commonly agreed criteria? Depending on the answers, the proposal of the eMandates Data Model may be different.

Where the "recognition" occurs has been examined in the sub-sections 3.6 and 3.7 of Use Cases 0 and 1 (Cross-border User eAuthorisation, and Cross-border Mandatee eAuthorisation).

Aiming to come up with an architectural proposal, let us presume that the eIDAS infrastructure is adopted. In this case, at least three scenarios can be considered:

1. **A data-oriented recognition** performed by the SP. Harmonised services (both public and private) would be solved via this architectural approach.
2. **A trust-oriented recognition** where the SP does not perform any verification of the data and authorises the access upon the positive answer issued by the cross-border eMandate Registry[55]. Non-harmonised services would be solved via this architectural approach.
3. **A hybrid** solution that would admit both orientations depending on the SP and the sector. The architectural solution is able to handle both types of recognition.

3.13.1. Data-oriented solution

In this scenario, the SP performs any task necessary to unlock the access to its system. For any request for an eMandate, the SP will have to evaluate each data value contained in the eMandate and decide whether to authorise the access or not. This implies that:

[54] During the interviews with the MS (AT, NL, BE, FI and ES), the idea of reusing eIDAS infrastructure for eAuthorisation was repeatedly expressed.

[55] In the TOOP architecture, the eMandate Registry would be accessed through the TOOP national layer.

- The eMandate Registry has to know the exact information requirements of the service. One solution for this is to use a single Service Catalogue, such as the ones proposed in previous sections (see sections about the use cases above);
- The eMandate Registry has to send high quality data (authentic and up-to-the-date);
- As described in the use cases, a central platform needs to be put in place in order to 1) discover the eMandate Registries all across Europe; and 2) maintain the taxonomies of Powers and Services, Code Lists, and other common artefacts (meaning that they are shared and equally used by all the stakeholders on agreed principles, policies, contracts, etc.).

One inconvenience of this approach is that MS are not eager to share data with other MS, especially personal data. Thus, when possible, non-harmonised services (such as those related to complex sectors) should not define in their Service Catalogue specific Power Attributes (e.g. “Date of birth”), but more abstract ones (e.g. “Above 16 years”).

Another problem is that specific sectors (e.g. agriculture, health, other) require such rich sets of Power Attributes, Constraints, and eventually types of Evidences, that they are difficult to map amongst MS, which have different and heterogeneous legislations on the sector. An effort towards standardisation could be made, which in time could lead to a single EU Service Catalogue that includes both non-harmonised and harmonised services. Both taxonomies would use the EU Powers Taxonomy to specify the particular service’s Power Attributes, Constraints and Evidence Types (see sections above on the EU Powers Taxonomy and Uses Cases 0 to 5).

The Services Taxonomy should be based on functional principles, and not on organic criteria. In other words, services should not be linked to organisations. Mapping services to organisations is expensive to maintain: organisations vary too frequently, sometimes unpredictably. Functions, especially administrative ones, rarely change.

The problem with service taxonomies is that they are not truly “controlled vocabularies” (contrary to the Power Taxonomy) but “structured lists of identifiers”. As such, they can grow indefinitely.

In the end, it could result that the specific information that a Mandator needs to provide for each possible cross-border online service becomes too much of a burden. Therefore, an effort to keep the taxonomy as simple as possible is needed. This responsibility could lie with the MS or, in a worse scenario, with the SP.

Some MS have resolved this scenario in different ways, from adopting a relatively lax perspective (Austria and Finland are “user-centric”) to setting up a detailed legislative and administrative-based approach (Spain, which is very “SP-centric").

In our architectural vision, the setup of the central platform mentioned above could be the responsibility of the European Commission. EU institutions, MS and public and private stakeholders could all be involved in the governance and support of the platform, its functionalities and content.

3.13.2. Trust-oriented solution

In this scenario, the SP relies on the response provided by the cross-border eMandate Registry.

This implies that:

- The SP does not need to validate the eMandate. It is for the eMandate Registry to execute the validation and communicate back to the SP with the message “OK, you can let the user in". The main advantage of this is that only a reduced subset of data about the natural persons is transferred between the SP and the eMandate Registry. However, it also implies that all the conditions necessary to create trust are in place, soundly proven and accepted; e.g. the data provided by the Registry is of high quality, the responsibilities and liabilities have been well established in a legal framework, the business and technical capabilities exist and have been well piloted and deployed, etc;

- In a trust-oriented solution, a request for validation of the eMandate by the SP could also be done by the eMandate Registry. If the eMandate is not (or is no longer) valid, the eMandate Registry could respond with a non-authorisation signal and a code representing the reason for the authorisation denial (e.g. "eMandate revoked", "eMandate time-limit expired", etc.).

3.13.3. Hybrid solution

The experiences of other trans-European systems present a frequent lesson: making all MS agree on the adoption of one single solution is a political and organisational challenge.

Whilst some MS would not care much about cross-border sharing or centralising data on their national persons – always under the adequate legal and technical protection measures, of course – others refuse to share the same data, regardless of the protection measures.

The other problem is trust, namely for sensitive authorisations in specific sectors (e.g. health, criminal records, etc.). Some of these SPs usually want to keep a tight control of who accesses their systems, under which conditions, and for what reasons. The only way for them to provide access is to receive an adequate set of data, for which they define their own Power Attributes, Constraints and Evidence Types.

When situations like these occur, other trans-European systems provide "hybrid" solutions, where the MS SPs are free to choose the approach that best suits them.

A hybrid solution would imply that both connectors and services are able to cope with data-oriented and trusted-oriented approaches. Both the workflows and the data model would have to support both situations.

The hybrid solution could also imply that services that could be considered as harmonised need to be treated as non-harmonised; e.g. due to specific criteria of criticality or sensitivity similar to the examples cited above in this same section. The EU Service Catalogue could be used to identify and define these services and to link them to their particular Power Attributes, Constraints and Evidence Types.

3.13.4. Solutions analysed

3.13.4.1. STORK 2

The functionality of STORK 2 is defined by the following processes.

a) "Authentication on behalf of and Powers (for digital signatures)" arethe process of verifying the identity of a particular representative (user), representing another person. This is achieved by requesting information that proves his/her identity, as well as the data about the represented persons and the Mandate for representation. As a result of this process, the user is allowed to access privileged data. This process usually ends with a fully identified representative (Mandatee), represented person (Mandator), and eMandate for representation. This means that eIdentifier of the Mandatee, and the identifier of the Mandator are transferred to the SP, and the SP recognises the Mandatee as a known customer, partner, patient, etc., and recognises the empowerment of the Mandatee[56].

b) "Domain-specific Attributes" is the process of verifying the identity of a particular user, and (possibly) collecting additional domain-specific Attributes. The standard authentication is achieved by requesting information that proves his/her identity. As a result of this process, the user is allowed to access privileged data. This process usually ends with a fully identified user, which means that his/her eIdentifier and any collection of other personal Attributes is transferred to the SP, and this SP recognises the user as a known customer, student, partner, etc.

c) "Powers Validation" is the process of verifying that an eMandate is still valid. This process is designed for SPs which maintain a database with the eMandates, and its users often represent several persons. The process is designed not to include any user interaction, not even for consent, as all personal data have already been sent to the SP. However, whether or not consent is to be requested is configurable.

Conclusion: The STORK 2 solution is a data-oriented approach that tried to put forward an extended harmonised set of Attributes protocol based on a standard (OASIS SAML2) and the possibility of exchanging eMandate content (for which a specific model was not provided).

3.13.4.2. UUM&DS

In TAXUD's solution, the Central Customs EIS receive all the UUM&DS information (authenticated user information and permissions) through a SAML assertion, a CAS assertion, or a set of classes, UUM&DS JEE Principals. UUM&DS allows a variety of integration protocols, which come out of the box with ECAS.

Different integrations are provided according to the needs of the services. Central services can select the most appropriate protocol, but ECAS client and CAS protocol is strongly recommended as they provide all the functionalities needed for the central services and this is a standard way and protocol for all European Commission applications.

The Attributes required in UUM&DS are part of a very well specified and harmonised data model. See section 3.14 "Data model" below for more details on these Attributes.

Conclusion: The UUM&DS solution is a data-based approach. As it is a specific-domain controlled environment, it was possible for them to define a federated architecture that works on the basis of harmonised protocols and vocabularies for eAuthorisation.

3.13.4.3. TOOP

One important aspect of TOOP is that it integrates the CEF eID Building Block for its pilots and for OOP applications in general. This implies that the eIDAS infrastructure can be interconnected to the TOOP eDelivery infrastructure. Once-Only-Principle applications using the TOOP approach could therefore leverage the benefits of the eIDAS infrastructure for eIdentification, eAuthentication and eAuthorisation via eMandates.

[56] I.e. the SP takes the eMandate (and the authenticity of the eIdentifiers) as evidences of the fact that the Mandate has actually been empowered by the Mandator.

The interviews of the selected MS revealed that the interviewees had never considered using TOOP as the infrastructure for the exchange of eMandates. All of them knew the project, but only related it to the once-only-principle goal and never to the facts that:

- The TOOP project approached the need of exchanging eMandates, and took that possibility into consideration when designing the authentication and authorisation data model;
- The TOOP infrastructure is perfectly able to ensure the exchange of eMandates and related information (as it is a payload-agnostic eDelivery system);
- The TOOP infrastructure is based on eDelivery, where **trust establishment is mandatory** for the provision of reliable and guaranteed message exchange. It uses the CEF PKI Service for publishing certificates both for access points and SMPs, as an enablement service for easy/early deployment of an eDelivery network of nodes[57].

TOOP is aligned to the eIDAS Regulation and can interoperate with the eIDAS Infrastructure.

Conclusion: The TOOP solution is based on a trust-oriented approach. It provides alternative protocols and technical solutions for the development of trust.

3.13.4.4. eIDAS

The eIDAS infrastructure is implemented on the basis of the eIDAS Regulation, which *"[…] seeks to **enhance trust** in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities […]."*[58]

The subject matter of the Regulation is to:

- Lay down the conditions under which Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State;
- Lay down **rules for trust services**, in particular for electronic transactions; and
- Establish a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

The eIDAS Regulation is further developed in several Implementing Acts on electronic identification and trust services that endorse the development of an eIDAS-Network Infrastructure[59].

The interoperability components of the eIDAS-Network are mainly based on the requirements laid down in the Implementing Act "eIDAS IF" (Interoperability Framework")[60].

The stakeholders of the eIDAS network are:

[57] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service

[58] eIDAS Regulation (REGULATION (EU) No 910/2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[59] https://ec.europa.eu/futurium/en/content/eidas-implementing-acts

[60] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0001

- The relying party:
  - Requires authenticity/integrity of the received personal identification data in order to fulfil his/her data protection obligations, and also requires the confidentiality of the received personal identification data.
- The citizen:
  - Expects confidentiality of his/her personal identification data;
  - Expects that the eIDAS-Network will respect his/her privacy.
- The operators of components of the eIDAS-Network:
  - Requirements derived from the requirements of the relying party and the citizen.

To fulfil these requirements, and to provide accountability / liability mandated by the regulation, **a chain of responsibility / trust is needed throughout the complete authentication process**.

Therefore, the framework for cross-border interoperability provides:

- Confidentiality of the personal identification data;
- Authenticity/integrity of the personal identification data;
- Secure identification/authentication of communication end-points.

Conclusion: eIDAS is a trust-oriented approach where the recognition of the eIdentification and eAuthentication relies on the cross-border service.

3.13.4.5. Member States

The solutions implemented in all the MS studied are all data-oriented and the recognition always happens at the SP side. See document "RPaM-State-of-affairs of EU eMandate Systems-v2 0" for details on their legal and administrative organisation.

One very interesting case is Spain, where the decentralisation of competencies in different governments and public administrations could be compared to the macro-European environment.

In Spain, the eMandates used to access the central public administration services contain the precise identification of what actions can be undertaken ("actuaciones"), before which authorities ("ante quién"), and for what specific administrative procedures.

This is possible because the central eMandate Registry (@Podera) defines and maintains each type of Power and links it to the identifier of the concrete administrations (supplied by the central registry DIR3[61]) and to the identifier of the administrative procedure (supplied by the SIA, Administrative Information Management System[62]). In this system, the Powers are perfectly identified and the eMandate always carries the exact data expected by the SP.

Conclusion: All MS systems are data-oriented and the recognition of the eMandates happens at the SP side. None of the approaches studied in the MS could be transposed into a pan-European model.

[61] https://administracionelectronica.gob.es/ctt/dir3/abstract#.W0o5Q9L7SUk

[62] https://administracionelectronica.gob.es/ctt/sia/abstract#.W0o5ZNL7SUk

3.13.5. Comparative analysis: commonalities and differences

The table below presents which of the EU initiatives studied are data-oriented and which ones are trust-oriented. This is an over-simplification. For additional details, please read the specifications of each initiative provided in footnotes.

The MS are not compared, as they do not yet exchange cross-border eMandates.

TABLE 6: COMPARATIVE ANALYSIS LEGAL FRAMEWORK IMPACTING EMANDATES SYSTEMS

	STORK	UUM&DS	TOOP	eIDAS
	Trust-oriented?			
	NO	NO	YES	YES

3.13.6. Proposal

Our proposal is to use the eIDAS infrastructure to offer the hybrid approach.

3.13.6.1. Trust-oriented proposal

For the trust-oriented proposal some principles and initiatives should be developed:

Principles

a) The SP shall request from the eMandate Registry whether a person should be authorised to access the SP system. The SP system shall rely on the answer of the cross-border eMandate Registry to authorise the user.

b) Trust should not preclude the possibility of accompanying the response by the eMandate Registry with references to the source of additional electronic evidences and information.

It would be for the eIDAS-Connector and eIDAS-Service nodes to resolve the communication between the SP and the eMandate Registry and to interpret the content of the messages exchanged.

Initiatives

The experience of previous pan-European initiatives and trans-European systems shows that trust is built progressively.

In this sense, the proposal would consist of starting with the definition of a reduced set of Powers, to be agreed with all Member States. The definition of Powers for actions in front of private sector SPs should be postponed to a later stage.

3.13.6.2. Data-oriented proposal

Principles

- The data is validated at the SP side;
- The SP should only request the data it needs in order to verify the eAuthorisation;
- Power Attributes shall be designed in an “abstract” manner; e.g. instead of asking the date of birth, asking whether the represented person (the Mandator) is over a certain age.

Initiatives

This scenario is more complex than the trust-oriented one. The cross-border eMandate Registry would have to know which exact Attributes will be requested by the SP for a given Power.

- **Development of the EU Registry of Registries, the EU Powers Taxonomy and EU Services Taxonomy**: Other trans-European initiatives solved this problem by means of a **legal instrument** and a **technical solution**. Thus, in the domain of procurement, the Directive 2014/24/EU introduces three articles, Art. 59, 60 and 61 where the rights of the economic operators and the obligations of the contracting authorities and MS are laid down regarding the request and responses of **formal statements** (ESPD Request and Response, Article 59) and for the setup of a European Central Repository (eCertis-2) where the MS shall ensure the **constant update by the MS** of the types of information concerning certificates and other forms of evidence.
  If we consider that each Power Attribute is a criterion that contributes to authorising access into an SP system, the solution could be similar to the one laid down in Directive 2014/24/EU: Member States shall contribute to the development of the Registry of Registries and the definition of Powers and Services;
- **Domain Area Harmonisation**: Two lessons learned from eCertis-1 were that (i) evaluation cannot be based on documents, but must be based on very specific criteria, otherwise the cross-border mapping becomes too complex; and (ii) national criteria need to be associated to a European commonly-agreed parent criterion.
  If we translate this situation to the eMandates-based eAuthorisation, the following two principles are to be set:
  - The evaluation at the SP side cannot be based on "types of eMandates" but on very specific Attributes associated to a concrete Power; and
  - Any national or sectorial service needs to be associated to one or more European commonly agreed Powers: in the end, Powers Attributes, Constraints and Evidence Types (as we have defined them) can be seen as criteria for the eAuthorisation.

3.13.7. Development timeline

When considering the introduction of a hybrid solution that permits the coexistence of the trust-oriented and data-oriented approaches, one reflection comes to mind: a project of this complexity should be planned as a long-term development and divided in clear progressive phases. In the initial phase, only the trust-oriented approach should be implemented.

That first phase could already take leverage of a first implementation of the EU Powers Taxonomy and the EU Services Taxonomy.

Subsequent phases should plan how to introduce public sector sectorial-specific Powers and services in both taxonomies.

3.13.8. SWOT analysis

3.13.8.1. Trust-oriented approach only

TABLE 7: SWOT ANALYSIS OF THE TRUST-ORIENTED APPROACH PROPOSAL

Strengths	Weaknesses

• No exchange of sensitive data. • No need for validation of eMandates. • The technical infrastructure is already available (eIDAS).	• The SP does not have full control of the details upon which the eAuthorisation is decided.
Opportunities	**Threats**
• Initial construction of a core European Powers Taxonomy. • eIDAS could be extended (e.g. with new eIDAS Implementing Acts and eMandate Interoperability Framework) to enforce the use of eMandates through the eIDAS network.	• Trust needs to be built progressively. • Delays in the developments due to the lack of specific legal enforcement. • Reluctance by the MS to agree on the common Powers and services.

3.13.8.2. Data-oriented approach only

Table 8: SWOT analysis of the Data-Oriented approach proposal

Strengths	Weaknesses
• The SP has full control of the details upon which the eAuthorisation is decided. • The technical infrastructure is already available (eIDAS).	• The connector has to execute more actions, and more in particular to each Power, on behalf of the SP.
Opportunities	**Threats**
• Extension of the EU Powers Taxonomy.	• Delays in the developments due to the lack of specific legal enforcement. • Complexities imposed on the eMandate Registry at eMandate creation time.

3.13.8.3. Hybrid approach

Table 9: SWOT analysis of the [Trust] + [Data]-Oriented hybrid approach proposal

Strengths	Weaknesses

• Great flexibility on the SP side (can choose one approach or the other, but not both simultaneously). • The technical infrastructure is already available (eIDAS).	• More complexity on the connector side.
Opportunities	**Threats**
• Extension of the EU Powers Taxonomy and the EU Service Catalogue covering both approaches. • Burden Reduction Observatory: good occasion to put in place KPI to monitor the burden reduction for all the actors intervening in the process of the eIdentification, eAuthentication and eAuthorisation, especially for the citizen, but also the SPs and eMandate Registries. • Integration into the Once-Only-Principle (OOP) solutions. One natural environment to disseminate the benefits of eMandates, especially the trust-oriented approach, is all the initiatives related to the implementation and deployment of the OOP.	• The adoption of common Power definitions and Attributes for specific sectors, especially those with strong restrictive national legislations may not happen unless a strong political will, promotion policy and legal instruments are put in place. • SPs may not be interested in moving towards the trust-oriented approach. • A double maintenance of centralised repositories could be asked in case the goal of pursuing a harmonised taxonomy of Powers and related Attributes is not accepted by one or more MS. • Development pitfalls, e.g. extremely complex approaches (see example below).

Development pitfall: One challenge to overcome is the possibility of falling into extreme complexities. An example of this could be the temptation of copying models that, at the national level, may work well. For example, the solution implemented in Spain may function perfectly well at the national level, but could end up in a very complex solution at the European level. The dependence of the Power and the Attributes on a dual organic and functional identification system would impose a huge burden on the user, the SP and the eMandate Registries; the governance and maintenance of the entire system could become unmanageable.

3.14. Data model

The recognition of the eMandate triggers the authorisation to access the SP's system and use it for the purposes stated in the eMandate. Therefore, the data model shall need (i) to express all the concepts and properties of the two axes upon which the authorisation is based: the identification of which actions can be performed (the "Power"); and (ii) to provide access to the evidence that the person acting on behalf of another person was indeed transferred that Power (i.e. to the eMandate content).

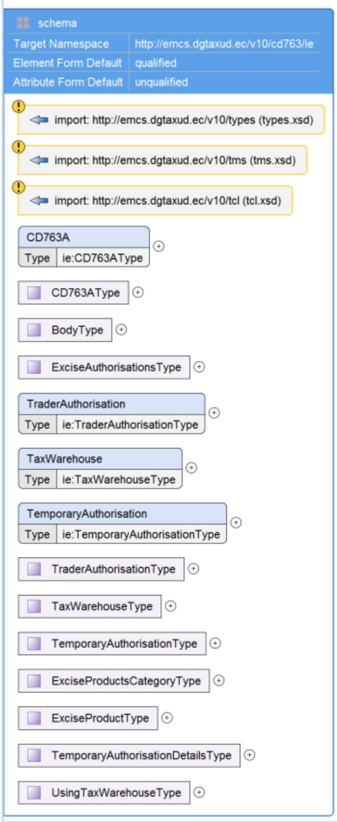
3.14.1. Solutions analysed

3.14.1.1. STORK 2

Stork does not define a data model for eMandates. Instead, it defines the type of Attribute “Mandate” and allows any type of content for that attribute (contrary to eIDAS that requires expressing the content of structured data as a Base 64 coded string).

3.14.1.2. UUM&DS

TAXUD defines a common vocabulary used by all the UUM&DS stakeholders. It is a very rich data model that covers all the needs of data, reference data and eMandate metadata needed for each of their business cases and use cases. The figures below show how complete and particular to the customs domain this model is:



schema

Target Namespace	http://emcs.dgtaxud.ec/v10/cd763/ie
Element Form Default	qualified
Attribute Form Default	unqualified

import: http://emcs.dgtaxud.ec/v10/types (types.xsd)

import: http://emcs.dgtaxud.ec/v10/tms (tms.xsd)

import: http://emcs.dgtaxud.ec/v10/tcl (tcl.xsd)

FIGURE 18: UUM&DS COMMON VOCABULARY, OVERVIEW

Each of the main entities is composed of different nested levels of sub-elements, e.g.:

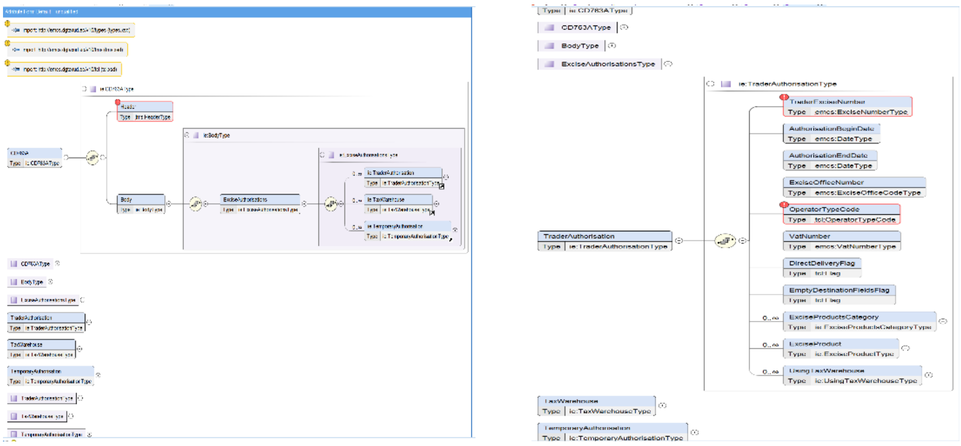


FIGURE 19: EXAMPLES OF A COUPLE OF ELEMENTS FROM THE UMM&DS COMMON VOCABULARY

3.14.1.3. TOOP

TOOP only foresees one type of Power: ALL Powers for a natural person to represent a legal person. For this, they proposed the reuse of the ISA2 Business Core Vocabulary (rov:RegisteredOrganization). They saw that it was not their mission to model Powers and eMandates, as their focus is the implementation of the Once-Only-Principle.

The figure below shows this model, which is an extension of the W3C Organisation ontology:

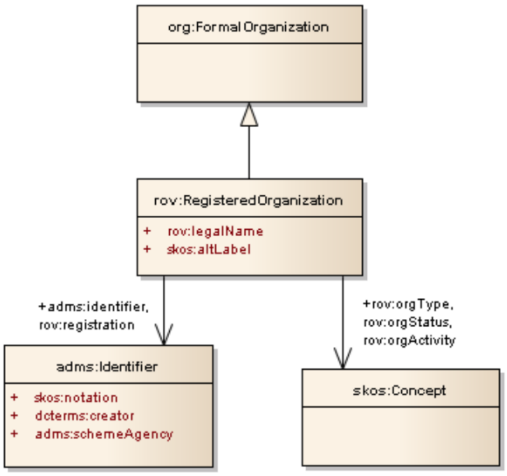


FIGURE 20: W3C REGISTERED ORGANIZATION DATA MODEL

The W3C Organization Ontology, in turn, looks like this[63]:

[63] https://www.w3.org/TR/vocab-org/

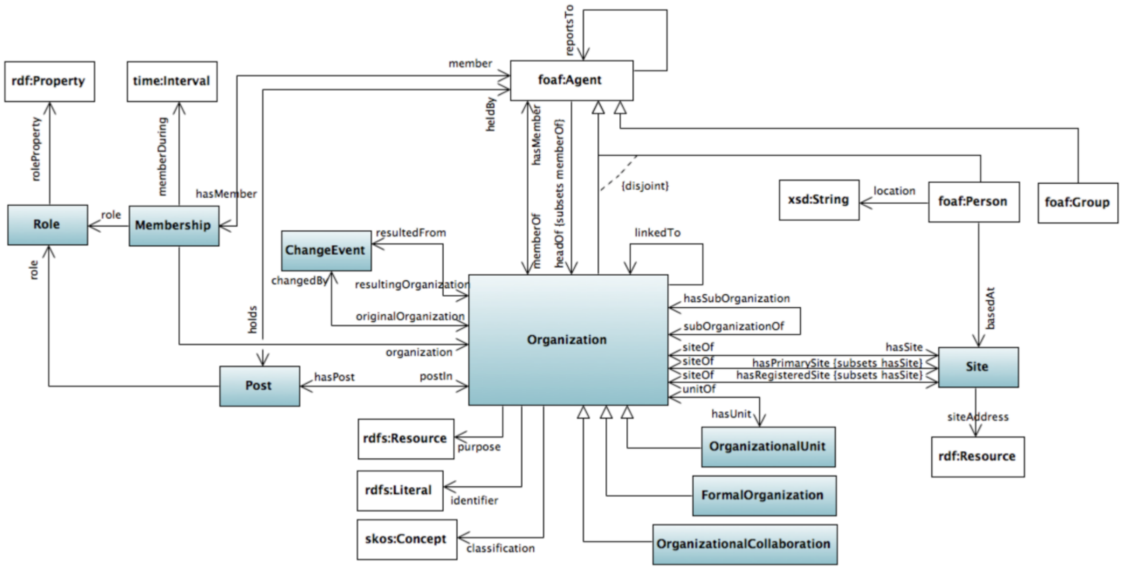


FIGURE 21: W3C ORGANISATION ONTOLOGY

ISA2 produced a merged version of the Core Person and the Core Business (legal entity) Vocabularies[64]:

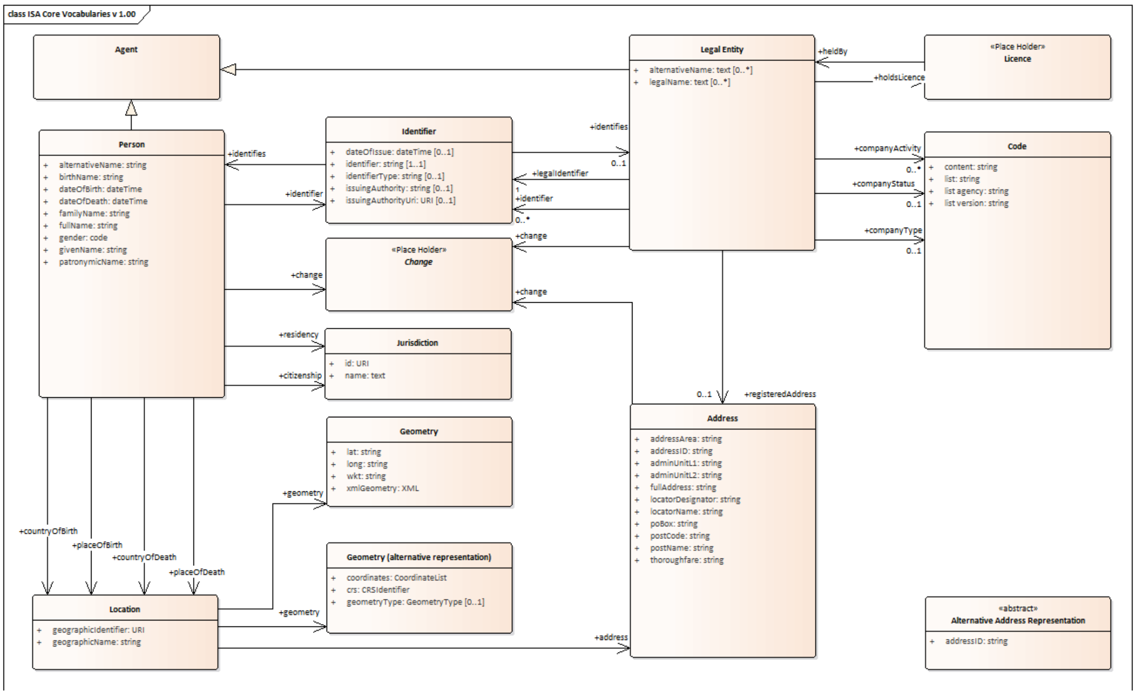


FIGURE 22: ISA2 CORE BUSINESS VOCABULARY AND CORE PERSON VOCABULARY

[64] See eGovernment Core Vocabularies, op. cit.

3.14.1.4. eIDAS

eIDAS is focused on the Attributes related to the eIdentification /eAuthentication. It does not provide specific Attributes for eMandates. However, it allows for structured content as values of certain Attributes, e.g. for “Address”.

As explained previously, this approach of eIDAS would facilitate the specification of a new Attribute named “Mandate”, which could convey instances of eMandates based on the proposed Core eMandate Vocabulary.

3.14.1.5. Member States

Austria

Austria defined its own data model used for the expression of eMandates. The figure below shows the XSD schema of that data model:

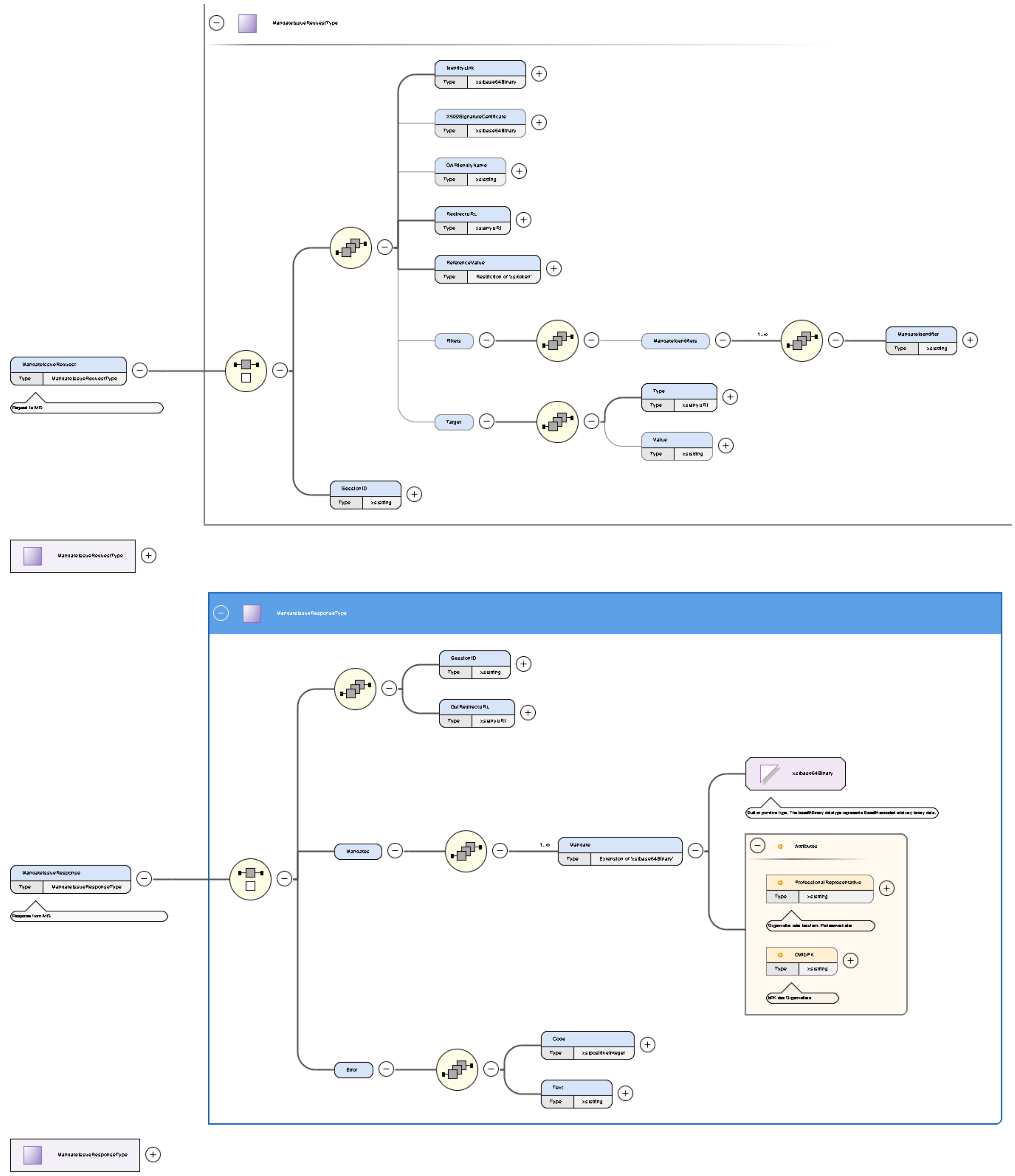


FIGURE 23: THE AUSTRIAN DATA MODEL TO ENVELOP EMANDATES

Notice that this is the model developed by the Austrian Central eMandate Registry and it aims at "enveloping" any format of eMandate as Base 64 encoded content (the particular modelling of eMandate is placed on the SP side). Therefore, there is no unique harmonised vocabulary for all types of eMandates:

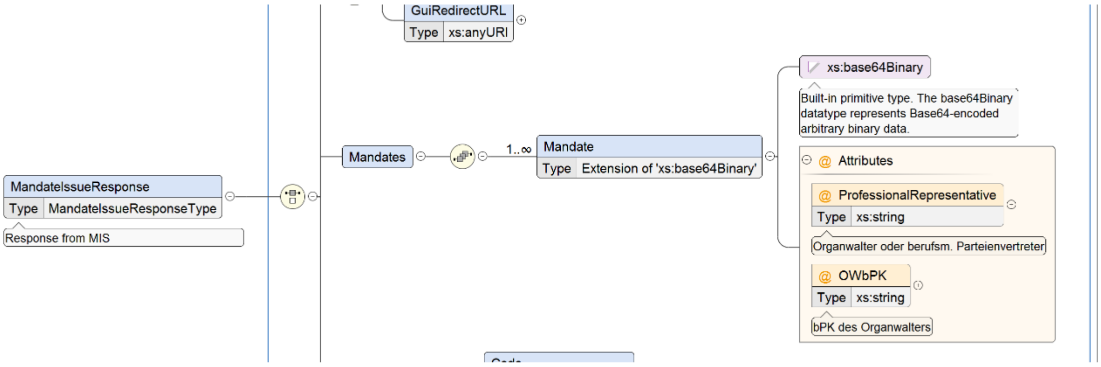

GuiRedirectURL
Type xs:anyURI
xs:base64Binary
Built-in primitive type. The base64Binary datatype represents Base64-encoded arbitrary binary data.
Mandates
1..∞
Mandate
Type Extension of 'xs:base64Binary'
Attributes
ProfessionalRepresentative
Type xs:string
Organwalter oder berufsm. Parteienvertreter
OWbPK
Type xs:string
bPK des Organwalters
MandateIssueResponse
Type MandateIssueResponseType
Response from MIS

FIGURE 24: AT EMANDATE EMBEDDED AS BASE 64 BINARY CONTENT

Belgium

Belgium does not have a common eMandate-related vocabulary. Each eMandate system existing in Belgium acts as a silo and does not interoperate.

The Netherlands

The two existing Netherlands models for eMandates is not documented as publicly available specifications.

Finland

Finland defines different concepts related to Power and eMandate as components of a larger “YSO - General Finnish ontology”, a compound of small taxonomies expressed in three different bindings (a SKOS-XML and Turtle Concept Scheme, and equivalent JSON mapping).

Each one of these taxonomies approaches the eMandate from a different perspective:

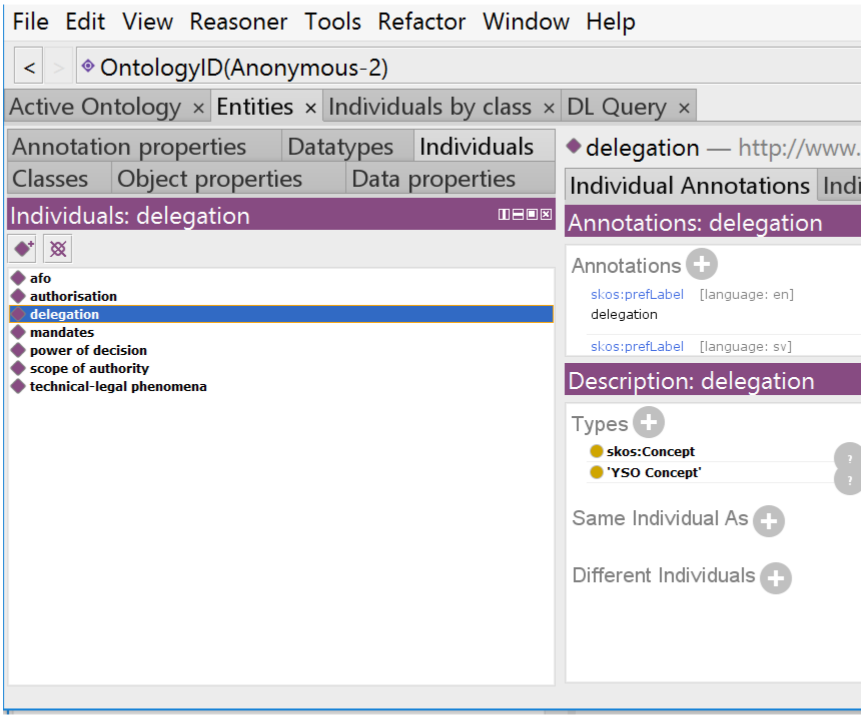
- As a legal phenomenon (Powers)[65];
- As a social object (abilities)[66];
- As an authorisation means (societal object)[67];

The figure below, for example, shows the SKOS individuals (i.e. class instances) of one of these small taxonomies as SKOS concepts labelled as “scope of authority”, “delegation”, “Mandates”, “Power of decision”:

[65] http://finto.fi/afo/en/page/?clang=fi&uri=http%3A%2F%2Fwww.yso.fi%2Fonto%2Fyso%2Fp5623

[66] http://finto.fi/yso/en/page/p5623?clang=fi

[67] http://finto.fi/yso/en/page/p5621



- afo
- authorisation
- delegation
- mandates
- power of decision
- scope of authority
- technical-legal phenomena

skos:prefLabel [language: en]
delegation

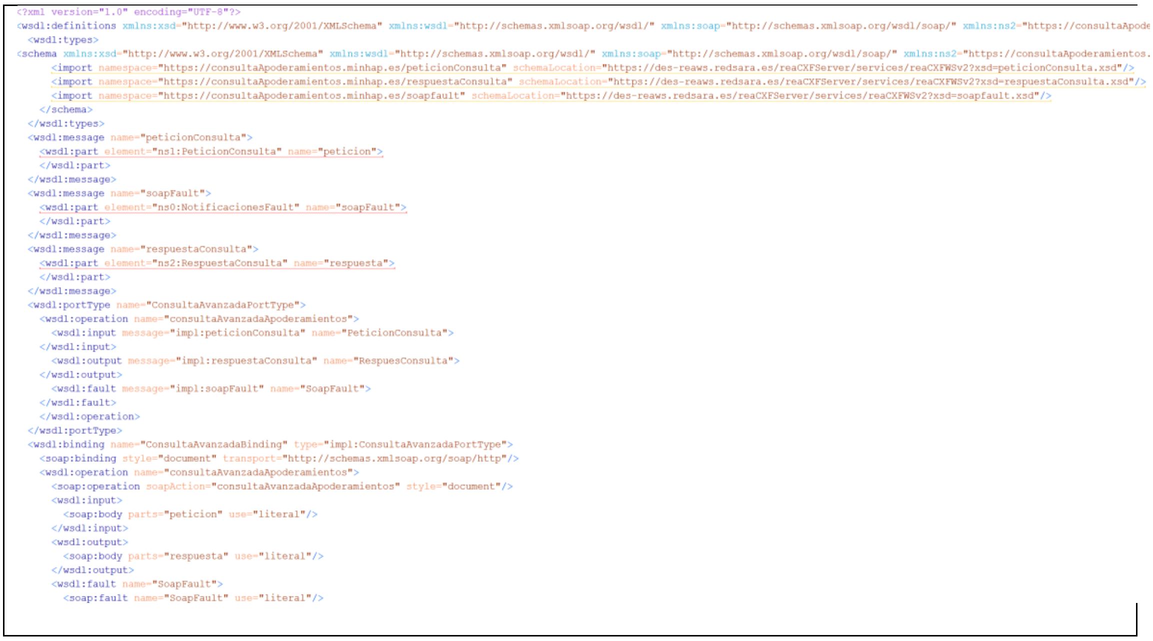
skos:prefLabel [language: sv]

skos:Concept
'YSO Concept'

FIGURE 25: FI – DEFINITION OF POWERS AND MANDATES-RELATED CONCEPTS AS SKOS TAXONOMIES

Spain

The Spanish approach is based on the consultation of data for validation by the SP. The Central eMandate Registry, @Podera, defined a WSDL specification, common for all the SPs that want to get information related to eMandates for actions in front of public administrations. The web service WSDL schema imports two other XSD schemas, one for the request and one for the response (and a third one for the format of the SOAP faults). The fragment of code below shows the header of the common WSDL:



```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:ns2="https://consultaApode
  <wsdl:types>
<schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:ns2="https://consultaApoderamientos.
      <import namespace="https://consultaApoderamientos.minhap.es/peticionConsulta" schemaLocation="https://des-reaws.redsara.es/reaCXFServer/services/reaCXFWSv2?xsd=peticionConsulta.xsd"/>
      <import namespace="https://consultaApoderamientos.minhap.es/respuestaConsulta" schemaLocation="https://des-reaws.redsara.es/reaCXFServer/services/reaCXFWSv2?xsd=respuestaConsulta.xsd"/>
      <import namespace="https://consultaApoderamientos.minhap.es/soapfault" schemaLocation="https://des-reaws.redsara.es/reaCXFServer/services/reaCXFWSv2?xsd=soapfault.xsd"/>
    </schema>
  </wsdl:types>
  <wsdl:message name="peticionConsulta">
    <wsdl:part element="ns1:PeticionConsulta" name="peticion">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="soapFault">
    <wsdl:part element="ns0:NotificacionesFault" name="soapFault">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="respuestaConsulta">
    <wsdl:part element="ns2:RespuestaConsulta" name="respuesta">
    </wsdl:part>
  </wsdl:message>
  <wsdl:portType name="ConsultaAvanzadaPortType">
    <wsdl:operation name="consultaAvanzadaApoderamientos">
      <wsdl:input message="impl:peticionConsulta" name="PeticionConsulta">
    </wsdl:input>
      <wsdl:output message="impl:respuestaConsulta" name="RespuesConsulta">
    </wsdl:output>
      <wsdl:fault message="impl:soapFault" name="SoapFault">
    </wsdl:fault>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="ConsultaAvanzadaBinding" type="impl:ConsultaAvanzadaPortType">
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="consultaAvanzadaApoderamientos">
      <soap:operation soapAction="consultaAvanzadaApoderamientos" style="document"/>
      <wsdl:input>
        <soap:body parts="peticion" use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap:body parts="respuesta" use="literal"/>
      </wsdl:output>
      <wsdl:fault name="SoapFault">
        <soap:fault name="SoapFault" use="literal"/>
```

FIGURE 26: ES WSDL SPECIFICATION FOR THE REQUEST AND RESPONSE OF DATA ABOUT EMANDATES

The figure below shows the XSD schema corresponding to the request:

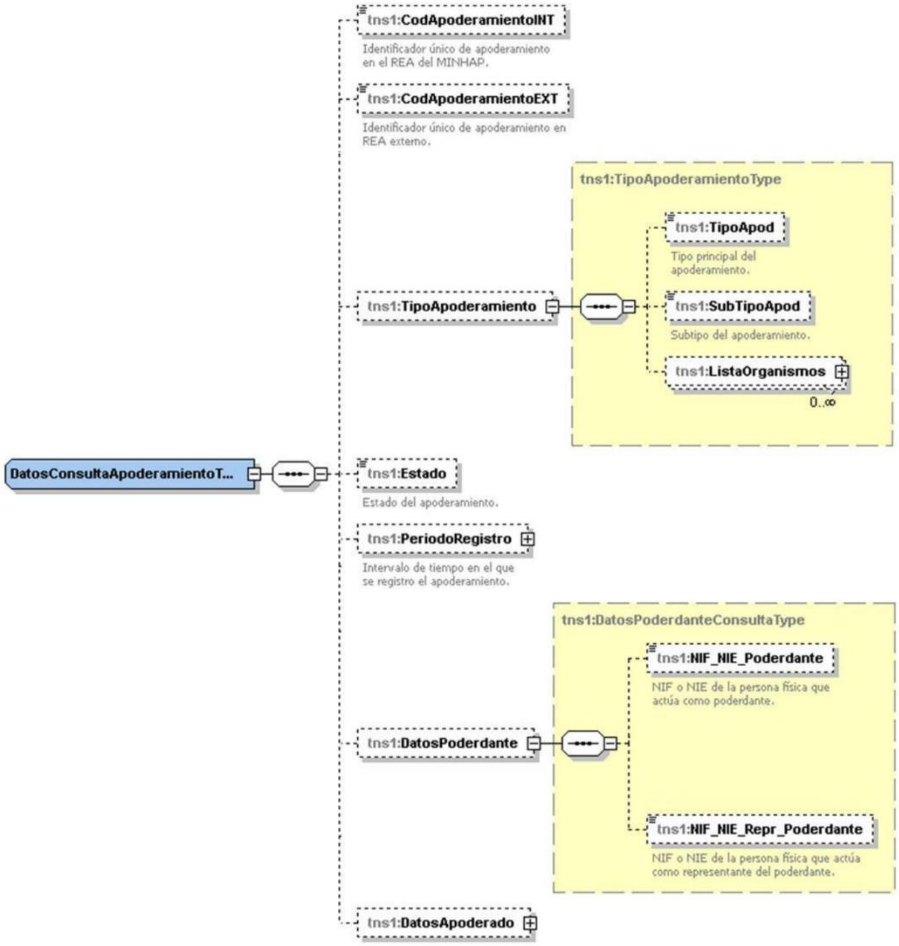

DatosConsultaApoderamientoT...
tns1:CodApoderamientoINT
Identificador único de apoderamiento en el REA del MINHAP.
tns1:CodApoderamientoEXT
Identificador único de apoderamiento en REA externo.
tns1:TipoApoderamientoType
tns1:TipoApoderamiento
tns1:TipoApod
Tipo principal del apoderamiento.
tns1:SubTipoApod
Subtipo del apoderamiento.
tns1:ListaOrganismos
0..∞
tns1:Estado
Estado del apoderamiento.
tns1:PeriodoRegistro
Intervalo de tiempo en el que se registro el apoderamiento.
tns1:DatosPoderdanteConsultaType
tns1:DatosPoderdante
tns1:NIF_NIE_Poderdante
NIF o NIE de la persona física que actúa como poderdante.
tns1:NIF_NIE_Repr_Poderdante
NIF o NIE de la persona física que actúa como representante del poderdante.
tns1:DatosApoderado

Figure 27: ES data model (XSD) for the Request of information on an eMandate

The figure below shows the schema for the response:

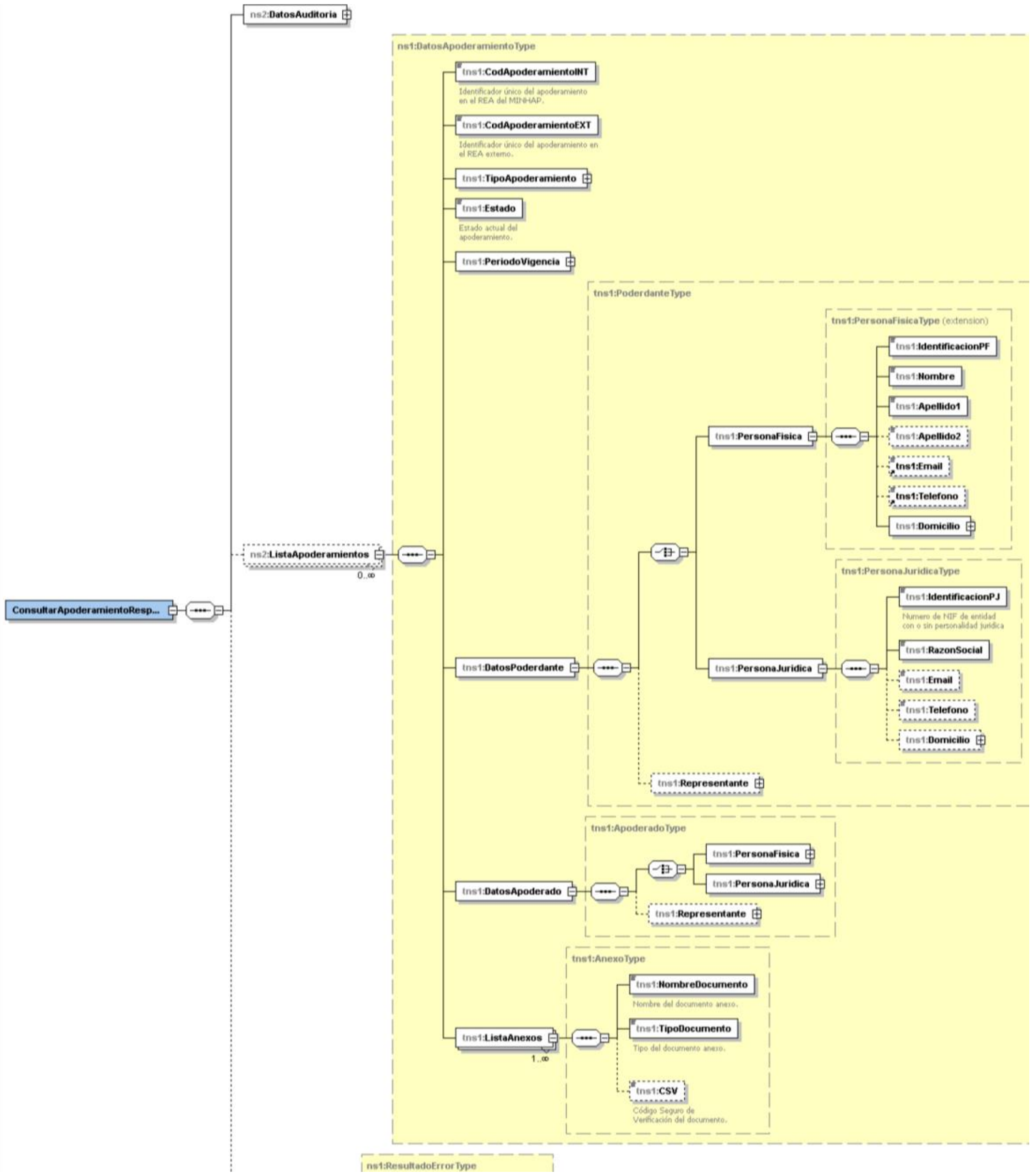


FIGURE 28: ES DATA MODEL (XSD) FOR THE REQUEST OF INFORMATION ON AN EMANDATE

This model exhaustively defines structures, data elements, reference data and eMandate metadata for the identification of the Mandator, the Mandate, the Power, and eMandate restrictions (e.g. the time limitation of the eMandate).

3.14.2. Comparative analysis

3.14.2.1. EU common initiatives

	STORK	UMM&DS	TOOP	eIDAS
Did the initiative define a common eMandate Data Model?				
	NO	YES	NO	NO

3.14.2.2. Member States

	AT	BE	FI	NL	ES
Did the MS define a common eMandate Data Model?					
	NO	NO	NO	NO	YES

3.14.3. Proposals

3.14.3.1. The eMandate vocabulary

We propose that a new "eMandate vocabulary" be designed. This vocabulary would be used to implement data structures to be shared between systems embedded or referenced into the SAML 2 Attribute of type "`eidas:Mandate`" (See Section "3.12 Architecture / 3.12.3 Proposals /Federated solution" for further details).

For the development of a new vocabulary, a large variety of methodologies and techniques exist. We propose using the ISA2 "eGovernment Core Vocabularies Handbook"[68].

Information requirements

The very first step for the design of a vocabulary is to clearly identify the information requirements. When examining the existing data models about eMandates, one can observe that they aggregate a common set of data groups, reference data and metadata:

- **Data** on the Mandator, Mandatee: Names, addresses, Identifiers, Attribute values, etc.;
- **Reference data**: Type of Powers, e.g. the identifier of the Power as specified in the European Powers Taxonomy;

[68] https://joinup.ec.europa.eu/site/core_vocabularies/Core_Vocabularies_user_handbook/ISA%20Hanbook%20for%20using%20Core%20Vocabularies.pdf

- **Metadata**: Data about the eMandate, e.g. date of expiration of the eMandate (or period of validity of the eMandate).

The use case "eAuthorisation" and the request-response protocol implemented also provide insight on how the eMandate can be structured. Both imply the following requirements:

- Both the Mandator and the Mandatee (the person behind the user) MUST be identified. The minimum set of data for the natural person and the legal person MUST be the ones specified in the eIDAS SAML Attribute Profile[69]. Optional additional data can be added upon common consent by the MS.
- The Power MUST be unequivocally identified; access to its definition in a machine-readable way MAY be provided, but not necessarily, as each Attribute has to be defined in the European Powers Taxonomy. If the identifier is a Persistent URL (PURL[70]) leading to the metadata about the Power in the European Powers Taxonomy, both needs would be satisfied (identification and access to the Power metadata).
- All the Attributes related to the Power(s) MUST be unequivocally identified; access to the definition in a machine-readable way MAY be provided, but not necessarily if the identifier is a PURL leading to the metadata on the Attribute. Each Attribute MAY specify its link to the Power(s), but this could be optional as the definition of the Attribute in the European Powers Taxonomy already MUST do this.

Another important requirement on the source of information is the outcome of previous efforts by the ISA2 programme regarding the domain of Powers and Mandates. Thus, previous deliverables of the "ISA Action 2016.2 – Semantic interoperability for representation Powers and Mandates"[71] identified the following sets of data elements and candidates for reference data:

- As already explained in STORK 2.0, there is a difference between general and specific types of Mandates (for all MS)[72]. While general Mandates encompass all affairs of the Mandator (i.e. a universal right to represent the Mandator for all legal acts), specific Mandates are required for specific legal acts that the Mandator wants to delegate to the Mandatee. Depending on the countries, the specific Mandates can be special Mandates that limit the Mandatee's rights to a certain type of act, or individual Mandates, that limit the Mandate to one or more individual acts.
- It must be noted that the Mandate types defined here are **conceptual models** that the end user (Mandator or Mandatee) doesn't necessarily see as such when creating or using a Mandate. During the Mandate creation or Mandate usage processes, the end user does not choose a type of Mandate such as the ones described below. The Mandate type is automatically set up and on a case-by-case basis during the creation of the eMandate, depending on the nature of the end user (natural or legal person), his/her representation capacities, the public service s/he is using, the parameters s/he selects, etc.

[69] https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_saml_attribute_profile_v1.0_2.pdf

[70] https://en.wikipedia.org/wiki/Persistent_uniform_resource_locator

[71] https://joinup.ec.europa.eu/collection/isa-action-201612-semantic-interoperability-representation-Powers-and-Mandates-0

[72] STORK 2.0., D3.5. "Legal Entities Identification Report": https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=8:d35-legal-entities-identification-report&Itemid=175&start=5

TABLE 10: MANDATE TYPES

STORK 2.0.	AT	BE	FI	NL	ES
General Mandate	**General PoR (Generalvollmacht):** Encompasses the Mandatee's authorisation to conclude all actions that may be subject to representation. For example, the Mandator empowers the Mandatee to manage his/her bank accounts, submit her/his taxes, open a business, etc.		**Open PoR**: It is a 'carte blanche' authorisation which allows the Mandatee to conclude all actions required in the name of the Mandator/principal. It is the most inclusive authorisation and is often given to professional Mandatees/representatives (e.g. lawyers or accountants to act in the name of the Mandator) for the treatment of administrative matters.	**General PoR**: Authority granted for representation covering all affairs of the Mandator and all juridical acts, except those that have been unequivocally excluded.	**General Power (public administration):** General Power so that the Mandatee can act in the name of the Mandator in any administrative action and before any public administration **General Power (administration or concrete organism)** Special Power so that the Mandatee can act on behalf of the Mandator in any administrative action before the General State Administration, before a local entity or before any of its bodies or linked entities or dependents.
Specific / Special Mandate	**Generic PoR (Gattungsvollmacht):** Authorises the Mandatee to conclude all actions of a specific type, or within a certain financial value. For example, the Mandator empowers the Mandatee to manage all his/her bank accounts (in Bank A, B, C,		**General PoR**: The General Mandate enables the Mandatee/representative to not only conclude the primary action, but also to conclude any other actions that may be necessary to accomplish the primary one. It is used to conclude precisely the defined actions	**Special PoR**: Granted authority that is limited to a specific act, and thus covers the Power to perform only that act. Even if it is granted for the purpose of completing a specific act, it also covers all of the linked administrative acts and potential Mandate transfers	Special Power so that the Mandatee can act on behalf of the Mandator to carry out the procedures specified in Power.

	etc.) or to conclude transactions that do not exceed XXX euros.		on behalf of the Mandator. Both the Mandatee and the object of the Mandate must be clearly denoted and defined.	that may be useful to complete the initial act.	
Individual Mandate	**Single PoR (Einzelvollmacht):** Authorises the Mandatee to conclude a single, specific action. For example, the Mandator empowers the Mandatee to manage her/his bank account in Bank A. When creating this type of Mandate, the Mandator should take care to ensure that it is limited in time.		**Identified PoR**: It is used to conclude precisely defined actions on behalf of the Mandator. Both the Mandatee and the object of the Mandate must be clearly denoted and defined.	**Limited PoR**: Granted authority to cover the Power to act on another's behalf for a limited period of time. As soon as the indicated period has ended, the Mandate is voided of its validity.	
X	**Precautionary/Enduring PoR (Vorsorgevollmacht):** A representative is appointed in the case of loss of the decision-making capacity of the Mandator. A medical certificate must be obtained to determine the extent of the loss of the Mandator's decision-making capacity.		**Continuing PoR**: In this Mandate, a representative is appointed in the case of loss of the decision making capacity of the Mandator. The continuing Mandate ceases to be valid when the authorisation is withdrawn, when the Mandator dies or when notice of the Mandatee's resignation is presented.	**Irrevocable PoR:** The effects of this Mandate do not cease upon the death of the principle, nor upon her/his placement under guardianship. It is transferable unless agreed otherwise, and the acts it covers must always be completed in the best interest of the Mandator.	

Mandate business rules

The following information was collected in STORK 2.0[73] as well as from the first phase of the ISA^2 Action 2016.12[74]. It must be noted that it concerns the RPaM in general in each MS, and not electronic Mandates specifically.

TABLE 11: MANDATE BUSINESS RULES

	AT	BE	FI	NL	ES
Conditions	The Mandator and Mandatee must both be of legal age and possess adequate mental capacity for legal decision making A person cannot delegate a Power that s/he does not have him/herself. A person cannot grant a Mandate with a broader scope than the Powers the Mandator actually has.	Idem.	Idem.	Idem.	Idem.
Oral vs. written Mandates?	Both.	Both but mostly written.			Spanish law allows the possibility of Mandates formalised with a written document other than a

[73] STORK 2.0. D3.5. "Legal Entities Identification Report": https://www.eid-stork2.eu/index.php?option=com_phocadownload&view=file&id=8:d35-legal-entities-identification-report&Itemid=175&start=5

74 ISA2 Action "Study about cross-border interoperability of Powers and Mandates", p.28: https://joinup.ec.europa.eu/document/study-about-cross-border-interoperability-Powers-and-Mandates

					notary deed, as well as oral Mandates.
Unilateral vs bilateral/ contractual	Both unilateral and bilateral Mandates exist. Unilateral: the Mandatee may simply act based on the Mandate with no formal acceptance.	The acceptance by the Mandatee is necessary, however this acceptance can be tacit (silent) and result from the execution of the Mandate without any formal acceptance.	Mandatee must explicitly accept the Mandate if it is a continuing one.	Mandatee must activate the authorisation code by logging in to the DigiD Machtigen Portal. Mandatee must explicitly accept the Mandate if it is an Irrevocable one.	
Requires handwritten signature?	Not mandatory.	Mandatory for written Mandates.			Mandatory.
Requires qualified electronic signature?					
Necessary to have intervention of a notary or other public officer? Requires validation by an authority?	Every eMandate must be signed by the issuing SourcePIN Register Authority, bilateral Mandates too.	For acts concerning real estate and for acts of incorporation of public companies, limited companies and cooperative companies.	No.	No.	General Mandates should be formalised through a notary deed, although typically all Mandates are done by notary deed to assure legal security.

Obligation to act vs. right to act under the Mandate	Right to act.			Right and obligation to act.	Obligation to act: in case of contractual Mandates, the Mandatee is obliged to fulfil the Mandate and is responsible for any harm done to the Mandator that is caused by his/her omission to exercise the Mandate at all, or to exercise the Mandate according to the Mandator's instruction. Furthermore, the Mandatee is obliged to report on his/her acting and to transfer to the Mandator whatever s/he has received in virtue of the Mandate, even if the received payment was not at the credit of the Mandator. The obligation is an obligation of means (best effort commitment). In case of unilaterally-given Mandates, the Mandatee has no obligation to act.
Compensation for the Mandatee?	Deemed to be free.	Deemed to be free unless the parties expressly agree that a fee is due.			Deemed to be free unless the parties expressly agree that a fee is due.
Number of Mandatees that can act jointly?	There exists the possibility to empower several persons at once. In such cases, if some of these have been given express full authority			A PoR in the Netherlands may be granted to two or more persons jointly, where	

	to act upon a certain matter, they may do so. However, in the case where none of the Mandatees have been granted full authority, the chosen representatives must act jointly and unanimously.			each is empowered to act individually.	
Mandate can be transferred?	The transfer of PoR from one Mandatee to another is allowed. Nevertheless, this is only the case when disposition/transfer is expressly provided for in the PoR or if it is considered inevitable due to surrounding circumstances.	SSM accepts transfer of Mandates, for example in case of a merging of companies.	Generally not. However, the Mandatee/representative may transfer the PoR only if transfer by the Mandatee/ representative is explicitly mentioned in the initial PoR or if the Mandator/principal agrees with the delegation.	Yes, if unequivocally provided for in the PoR and only: • To the extent that the transfer is a necessary consequence of the juridical acts to be performed; • To the extent that the transfer is necessary in the interest of the Mandator who is unable to act him/herself; • To the extent that the PoR concerns assets located outside the country in which the current representative is residing; An Irrevocable PoR is transferable unless agreed otherwise.	
Mandate can be used for acts of disposition?	Yes			Generally not, unless explicit in the PoR.	

eMandate ceases to produce effects when…	• Death of Mandator/principal; • Death of Mandatee/representative; • Declaration of insolvency by the Mandator/principal; • Revocation of PoR by Mandator/principal; • Completion of the requested duties.		A PoR's validity does not end with the death of the Mandator/principal, unless special circumstances require its revocation. The PoR ceases its effects in cases of: • Revocation of the PoR by the Mandator; • Bankruptcy of the Mandator/principal; • Declaration of void PoR by the Mandator; • Forbidding the Mandatee to act on PoR by the Mandator; • Loss of employment of an employee whose PoR is linked to his/her title/position.	• Upon the death of the Mandator; • Upon the Mandator being placed under adult guardianship; • Upon the Mandator's bankruptcy; • Upon revocation of the PoR by the Mandator; • Upon renunciation of the PoR by the Mandatee; • Upon the Mandatee's completion of all requested duties.	• 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.

Other specificities?		For the MAHIS system: • MAHIS Mandates can only be given for a period of one trimester. The reason for this time limit is historical, it comes from the requirements in the law regulating the most widely used MAHIS service, the declaration of employees by employers to social security, since this must be done every trimester. • It is possible for a current MAHIS Mandate holder to give a delegation to someone who was a Mandate holder in the past. For example, if a declaration that was submitted the year before by another Mandate holder has to be modified, and the current Mandate holder has no right to access and modify it, then the past Mandate holder can give a delegation.	A Mandate can be granted for a pre-set period (one, five, 10 or 25 years) or a custom period (from-to) defined by the user. A permanent Mandate cannot be granted.		

TABLE 12: ATTRIBUTES

	AT	BE	FI	NL	ES
Identity of the Mandator	• Natural person: first name, last name, date of birth • Legal person: full legal name • For both NP and LP: the person's unique identifier (i.e. the sourcePIN in the event of natural persons)		• Natural person: first name, last name, date of birth, social security number • Legal person: current registered name and unique electronic identifier	• Natural person: first name, last name, prefix associated with name, date of birth • Legal person: current registered name	
Identity of the Mandatee	• Natural person: first name, last name, date of birth • Legal person: full legal name • For both NP and LP: the person's unique identifier (i.e. the sourcePIN in the event of natural persons)		• Natural person: first name, last name, date of birth, social security number • Legal person: current registered name and unique electronic identifier	• Natural person: first name, last name, prefix associated with name, date of birth • Legal person: current registered name	
Identity of intermediary (optional)	• Natural person: first name, last name, date of birth • Legal person: full legal name • For both NP and LP: the person's unique identifier (i.e. the sourcePIN in the event of natural persons)				

Scope of empowerment	One or several text blocks are used to describe the scope of empowerment. Although arbitrary text blocks are possible, typical electronic Mandates are built by using standardised text blocks. This eases Mandate verification. However, in order to be able to create any kind of Mandate, arbitrary text is allowed.		When using electronic PoR services for citizens, the details of the Mandate pertaining to its scope and object are entered in free text	When using electronic PoR services for citizens in the Netherlands, the details of the Mandate pertaining to its scope and object are entered in free text and the Mandatee/representative does not need to sign or confirm the received Mandate.	
Constraints	Constraints [optional]: Additional to the scope of empowerment, arbitrary restrictions can be formulated (optionally). Currently, the specification defines three concrete types of restrictions by using specialised XML elements: • Time constraint (i.e. a Mandate is effective within a given time frame only: start date and expiry date) • Collective constraint (i.e. a Mandatee cannot act alone; further proxies are required) • Financial constraint (i.e. actions taken based on the given Mandate are limited		Minimum required Mandate attributes for natural persons are: • Scope of empowerment for open, general and identified Mandates • Object of empowerment for general and identified Mandates • Time constraint (start date and expiry date) for identified Mandates • Financial constraint for identified Mandates	Minimum required Mandate attributes for natural persons are: • Scope of empowerment for general, special and limited Mandates • Object of empowerment for special Mandates • Time constraint (start date and expiry date) for limited Mandates	

	with a financial transaction limit).				
Other?	• Unique serial number: each electronic Mandate is assigned a unique serial number. This is required for revocation purposes. • Link to a revocation service [optional]: If a link to an electronic Mandate revocation service is given, the verifier of the Mandate is asked to contact this service in order to verify the revocation status of the Mandate. For requesting the revocation status, an HTTP-based protocol has been developed. Currently, the SourcePIN Register Authority runs a Mandate revocation service; all existing electronic Mandates are registered with this service by default. • Electronic signature of the issuing Authority: due to Austrian law, every electronic Mandate has to be signed by the issuing SourcePIN Register Authority. This also applies to bilateral Mandates.				

Data model design

For the design of the data model, we propose the following:

- Use the Core Person Vocabulary (CPV) for the expression of data on the natural person;
- Use the Core Business Vocabulary (CBV) for the expression of data on the legal person;
- Use the Core Criterion and Evidence Vocabulary (CCEV) for the expression of Attributes;
- Use SKOS-XL for the expression of the European Powers Taxonomy.

A complete design of the data model is beyond the scope of this deliverable (but within the scope of Task 2 of this project). However, for a better understanding of the proposal, a recent version of the CCEV is presented below:

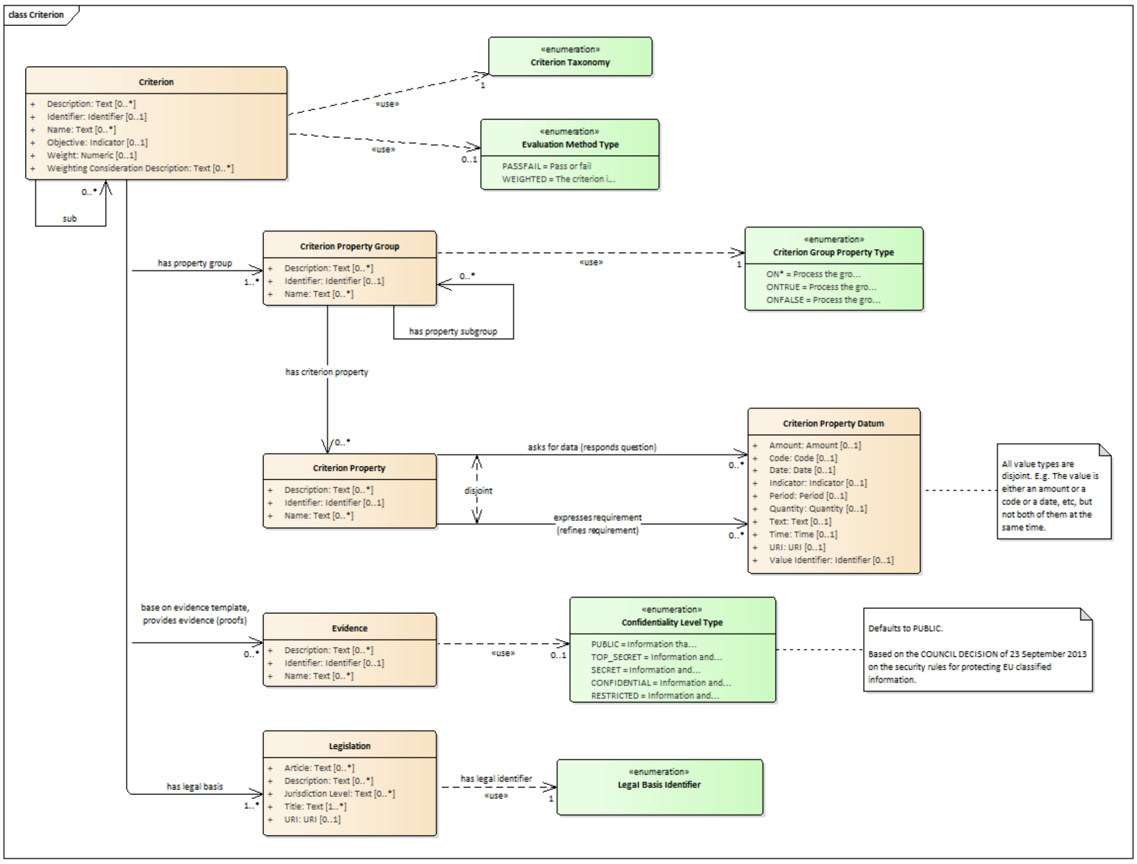

class Criterion
«enumeration»
Criterion Taxonomy
Criterion
+ Description: Text [0..*]
+ Identifier: Identifier [0..1]
+ Name: Text [0..*]
+ Objective: Indicator [0..1]
+ Weight: Numeric [0..1]
+ Weighting Consideration Description: Text [0..*]
«use»
1
«use»
0..1
«enumeration»
Evaluation Method Type
PASSFAIL = Pass or fail
WEIGHTED = The criterion i...
0..*
sub
Criterion Property Group
+ Description: Text [0..*]
+ Identifier: Identifier [0..1]
+ Name: Text [0..*]
has property group
1..*
«use»
1
0..*
has property subgroup
«enumeration»
Criterion Group Property Type
ON* = Process the gro...
ONTRUE = Process the gro...
ONFALSE = Process the gro...
has criterion property
0..*
Criterion Property
+ Description: Text [0..*]
+ Identifier: Identifier [0..1]
+ Name: Text [0..*]
asks for data (responds question)
0..*
disjoint
expresses requirement
(refines requirement)
0..*
Criterion Property Datum
+ Amount: Amount [0..1]
+ Code: Code [0..1]
+ Date: Date [0..1]
+ Indicator: Indicator [0..1]
+ Period: Period [0..1]
+ Quantity: Quantity [0..1]
+ Text: Text [0..1]
+ Time: Time [0..1]
+ URI: URI [0..1]
+ Value Identifier: Identifier [0..1]
All value types are disjoint. E.g. The value is either an amount or a code or a date, etc, but not both of them at the same time.
base on evidence template,
provides evidence (proofs)
0..*
Evidence
+ Description: Text [0..*]
+ Identifier: Identifier [0..1]
+ Name: Text [0..*]
«use»
0..1
«enumeration»
Confidentiality Level Type
PUBLIC = Information tha...
TOP_SECRET = Information and...
SECRET = Information and...
CONFIDENTIAL = Information and...
RESTRICTED = Information and...
Defaults to PUBLIC.
Based on the COUNCIL DECISION of 23 September 2013 on the security rules for protecting EU classified information.
has legal basis
1..*
Legislation
+ Article: Text [0..*]
+ Description: Text [0..*]
+ Jurisdiction Level: Text [0..*]
+ Title: Text [1..*]
+ URI: URI [0..1]
has legal identifier
«use»
1
«enumeration»
Legal Basis Identifier

FIGURE 29: CORE CRITERION AND EVIDENCE CONCEPTUAL DATA MODEL

This version of the CCEV is the one being proposed for the ePO (eProcurement Ontology for the Publications Office), and was based on the ESPD Criterion Vocabulary, which in turn was based on the ISA2 CCEV. Both the ePO and the ESPD extend the CCEV to add specialised classes and properties.

The concepts present in this vocabulary have been defined in the ePO as follows[75]:

[75] These definitions are not final, they are currently being discussed with the ePO Working Group members. Other concepts, terms and definitions related to this vocabulary can be found in the ePO. Working Group (WG) GitHub Repository: https://github.com/eprocurementontology/eprocurementontology/wiki/eProcurement-Glossary.

- **Criterion**: a condition that needs to be answered for evaluation purposes;
- **Criterion Property**: specific information needed to measure a criterion;
- **Criterion Property Group**: an organised structure of related criterion properties;
- **Criterion Property Datum**: the value provided for a criterion property.

Note that the CCEV is completely business-agnostic. The concepts represented therein do not carry semantics related to any domain. This makes the CCEV a very flexible and highly reusable vocabulary, but also a very abstract one that needs thorough documentation on how to be implemented[76].

Note also that this CCEV model uses two different properties regarding the Evidences that may be attached to the Criterion:

- At Request-time, a type of Evidence may be suggested or requested by the SP (e.g. a specific type of template);
- At Response-time, the actual proof can be attached (i.e. referred to).

This extensibility of the Core Vocabularies is needed also for the proposal of a Core eMandate Vocabulary. In the case of the CCEV, we propose extending it to meet the information requirements of the Power Attributes as depicted below:

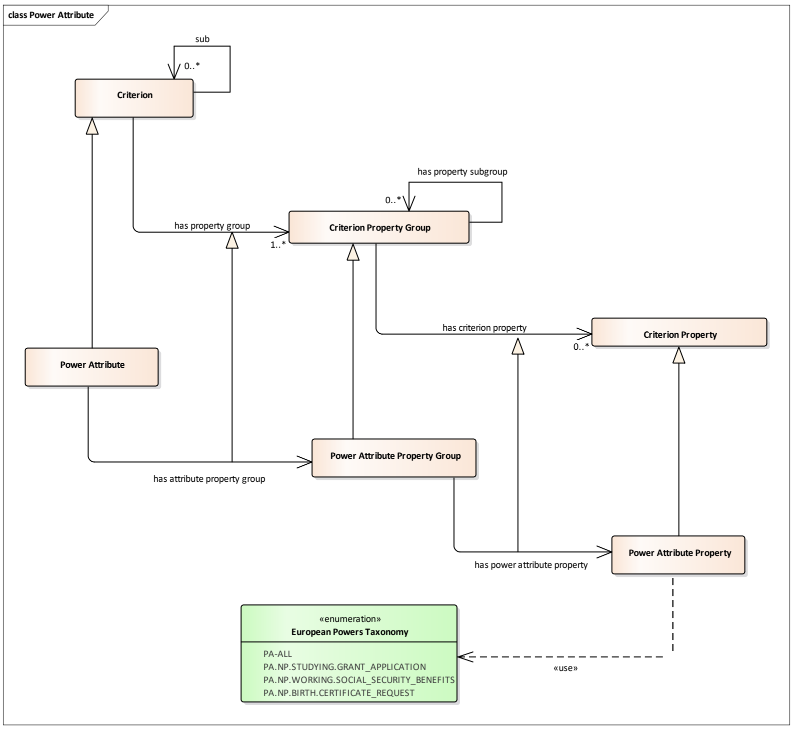


FIGURE 30: POWER ATTRIBUTE AS A SUBCLASS OF THE CCEV CRITERION

One additional convenient extension would be that the Power Attribute Property is also linked to the Evidence (the current version of the CCEV only links Evidences to Criterion, which may be an inconvenient/incomplete design).

[76] For an example, see the ESPD-Exchange Data Model and how it implements the CCEV: https://github.com/ESPD (click on the ESP-EDM repository).

A possible data model for the complete eMandate is presented in the diagram below. The following points must be taken into account:

- This is only a representation for illustration purposes, as the modelling of the Powers and of the eMandate (or other possible data structures) are the goal of Task 2 of this project;
- This diagram represents only the core elements for the Request and the Response. Many details that belong to the Response are supported by the parent CCEV, e.g. the “Datum” holding the value responded for a requested Attribute. Other elements will have to be added to the Request and the Response, e.g. metadata about the Request and the Response, error codification in the Response, etc.;
- Axioms and coherent representation of classes and properties; e.g. representation of the disjointedness between natural person and legal person individuals.

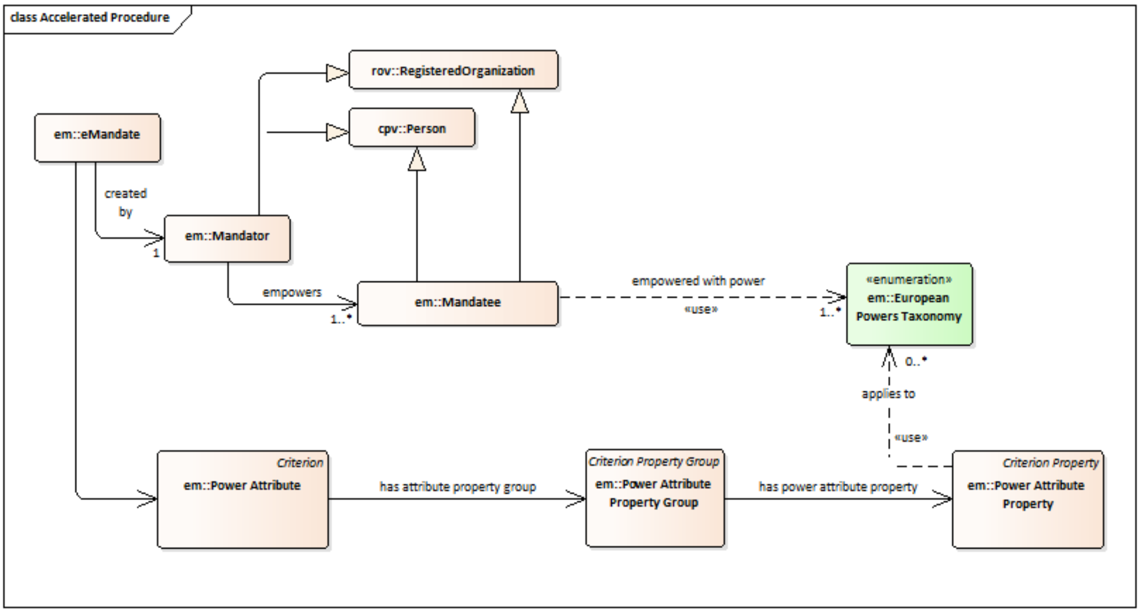


FIGURE 31: EMANDATE CONCEPTUAL DATA MODEL, POSSIBLE DRAFT APPROACH

In this design, the Mandator and the Mandatee can either be natural persons (CPV stands for Core Person Vocabulary) or legal persons (ROV stands for Registered Organisation Vocabulary, which is the vocabulary used in the ISA Core Business Vocabulary).

The Powers are assigned to the Mandatee by the Mandator, thus expressing the actual transfer of Power as the core fact that the eMandate expresses.

One interesting aspect of this design is that the Attributes of the Mandator and the Mandatee are decoupled. This facilitates offering responses where the SP is not interested in the Mandatee nor the Mandator, but only in the values of the Attributes specified in the response. Provided that the Attribute and the Attribute property are correctly identified, the Attribute property does not have to compulsorily point at the Powers it is associated to, as the European Taxonomy also contains that information.

Syntax bindings

The eMandate Conceptual Data Model can be expressed in different syntaxes, XML (e.g. UBL-2.2-based, as for some of the ISA2 Core Vocabularies[77]), or RDF-based (XML, Turtle, other), as in the OWL ontology, JSON or even better JSON-LD, etc.

We propose that in Task 2, at least one version of the Core eMandate Vocabulary is provided as an OWL-DL Turtle (or XML) syntax.

The proposal of expressing the European Powers Taxonomy as a SKOS-XL syntax is easy to justify:

- Each Power can be represented as a Concept, to be identified preferably with a PURL leading to the definition of the Power and associated attributes;
- Each Power can be assigned as many metadata as necessary, if the SKOS-XL (eXtension for Labels) specification is used;
- Every element, included the metadata, is machine-readable;
- It is a well-known and widely used specification.

All these semantic assets – the Core eMandate Vocabulary, the European Powers Taxonomy, any related validation artefact (e.g. Schematron schemas, SHACL developments, etc.) – should be publicly available in Joinup. As an alternative, the possibility of maintaining the European Powers Taxonomy in the Publications Office of the European Union MDR (Metadata Registry) should be considered, too.

Self-containment

One recurrent debate in projects similar to this is whether all the information in the eMandate should be embedded in the message transferred between systems. In our proposal, the transfer would occur between the cross-border service (interfaced to the eMandate Registry) and the Connector (interfaced to the SP system), or instead, part of it can simply be referred to (e.g. via a URL).

In the trust-oriented approach, only the attribute values that confirm that the user is authorised should be sufficient. These could be fully replaced by a very simple certificate by the eMandate Registry stating “yes, authorise”, or “no, reject authorisation” (plus a code indicating the reason for the denial).

In the data-oriented approach, the data that is used by the SP should be embedded. Evidences associated to Attributes should be referred to as URLs. To consider that the reference to data via URL is also a self-contained approach, at least the following conditions should be met:

- The SP WILL be able to access the evidence from that URL freely and in a timely manner;
- The eMandate Registry MUST provide official “sources of truth” in the eMandate, e.g. official evidences associated to the Power Attribute property that are the URLs of national base registries or databases.

SWOT analysis

The table below presents the strengths, weaknesses, opportunities and threats of reusing the CCEV as a basis for the modelling and expression of Power Attributes. For a similar analysis of for the Core Person Vocabulary and Core Business Vocabulary designs, please search the Joinup

[77] http://docs.oasis-open.org/ubl/UBL-2.2.html

community SEMIC (Semantic Interoperability Community) for the "eGovernment Core Vocabularies" collection[78].

TABLE 13: SWOT ANALYSIS OF THE MODELLING OF POWER ATTRIBUTES AS AN EXTENSION OF THE ISA2 CCEV

Strengths	**Weaknesses**
• Great flexibility for the expression of any type of Power Attribute for both public sector and private sector, notably in sectors with rich Attribute-related requirements; • Links to legal basis and evidences supporting the Power Attribute at the level of the Attribute, group of Attribute properties or singular Attribute properties; • Great flexibility for the extension of the Power Attribute to link the Attribute to other entities; • Permits adjusting the granularity of the Attribute properties; e.g. very atomic (similar to the SAML2 attributes) or highly structured (less semantics).	• Poor eMandate-related semantics (the semantics are moved from the data element level (the Attribute property) to the "Attribute data shape"; • Needs tight control and efficient maintenance of the existing data shapes (e.g. in the central European Powers Taxonomy repository); • Each Attribute will need a thorough documentation, both human and machine-readable.
Opportunities	**Threats**
• Enabler for the production and harmonised set of unique and well-structured Attributes linked to the European Powers Taxonomy.	• May be considered excessively abstract; a 100%-semantic terminology is proposed instead.

3.15. Legal interoperability instruments

One challenge to the possibility of reaching agreements on harmonised processes and common data models is the lack or dearth of European and national legislation specific to Mandates (and eMandates) and the heterogeneity of the national laws. Very important legal measures have already been undertaken regarding matters closely related to the eMandates, most notably related to the eIdentification, e.g. the eIDAS Regulation and the associated Implementing Framework Acts. Two relevant benefits of this legal framework are that: (i) it has endorsed and enforced efficient solutions that ensure **technical interoperability** (e.g. the use of the SAML2

[78] https://joinup.ec.europa.eu/solution/e-government-core-vocabularies

protocol for the exchange of eID Attributes); and (ii) it gave place to the implementation of an infrastructure that is seen as a good "reference" duly supported by a **legal interoperability** framework.

The eIDAS Regulation is relevant to the topic of eMandates because, while it doesn't regulate Mandates directly, it does govern the cross-border recognition of electronic identification schemes, both for natural persons and for legal persons. Identification of legal persons is particularly relevant in this context, since legal persons can only act through a natural person who is representing them. It is of course possible for representation to be chained – one legal person is represented by another legal person, who is represented by another legal person and so forth – but ultimately a natural person must act on their behalf.

As such, the eIDAS Regulation by necessity introduces the concept of 'person identification data' in Article 3 (3), meaning "a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established". Furthermore, Article 12.2 of the Regulation calls for the creation of an interoperability framework to facilitate cross-border recognition of electronic identities, which consists (among other elements) of "a reference to a minimum set of person identification data uniquely representing a natural or legal person, which is available from electronic identification schemes".

This interoperability framework was created via the Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market[79]. Article 11.2 of this Implementing Regulation states that "a minimum data set for a natural person representing a legal person shall contain the combination of the Attributes listed in the Annex for natural persons and legal persons when used in a cross-border context"; and the Annex lists the following elements:

"1. The minimum data set for a natural person

The minimum data set for a natural person shall contain all of the following Mandatory Attributes:

(a) Current family name(s);

(b) Current first name(s);

(c) Date of birth;

(d) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time

[…]

2. The minimum data set for a legal person

The minimum data set for a legal person shall contain all of the following Mandatory Attributes:

(a) Current legal name;

[79] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1441782373783&uri=OJ:JOL_2015_235_R_0001

(b) A unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time".

The fact that, under the Implementing Regulation, "the combination of the Attributes" mentioned above should be included implies that it must be possible to establish a link between that natural person and the legal person it claims to be representing. What the Implementing Regulation does not specify, is any obligation for Member States to be capable of explicitly stating the nature of that link, i.e. the title or competences of the natural person towards the legal entity. Doing so would also be challenging, given that company law within the EU is largely unharmonised, and that types and names of legal entities, types and names of their representatives, and the competences of the representatives can differ from Member State to Member State, without even considering the complexity that may be added to this picture when taking into account that articles of association of an individual company can expand or limit competences.

This complexity would be mitigated to some extent with a future adoption of the Company Law Package[80] at EU level, which would more effectively harmonise the use of digital tools and processes in company law. This would include an obligation for Member States to lay down detailed rules for the online registration of companies, which must provide for procedures to ensure the legal capacity of the applicant and his/her authority to represent the company; and the means to verify the identity of the person or persons registering the company or their representatives. The Company Law Package builds on the eIDAS Regulation on this point. Therefore, at least for the narrow case of eMandates in relation to the Power to represent companies or other legal entities, the eIDAS Regulation already provides some of the legal underpinnings required to support cross-border recognition and validation of eMandates.

[80] https://ec.europa.eu/info/publications/company-law-package_en

4. CONCLUSIONS

4.1. Cross-border interoperability

Recommendations

- The phased development of a hybrid architectural approach, aiming towards a fully trust-oriented e-authorisation environment.
- Not to invent new vocabularies, but to re-use, extend and customise the existing ones (Core Person Vocabulary, Core Business Vocabulary, Core Criterion and Evidence Vocabulary).

Legal challenges

- Putting in place a legal or several legal instruments, and/or evolving some of the existing ones – eg. eIDAS, SDGR, etc.
- Making it possible for citizens to act with eMandates before each and any MS public administration (only public administration services available online).
- Putting in place an instrument that enforces the obligations of the Member States to support a taxonomy of Powers and related Attributes in a central repository at EU level.

Organisational challenge

- Managing the change from a data-oriented approach to a fully trust-oriented approach.

Semantic challenge

- Coming up with a common model that everyone can share and use, for both public and private sector, and for the hybrid architecture proposed. The outcome should be a flexible and expressive vocabulary able to represent any type of question in the Attributes and providing any type of data in the response.

Technical challenge

- The current systems being used by the MS will have to be adapted to include the features related to eMandates, namely the eIDAS nodes and the Once-Only Principle national layers.

Interoperability governance challenge

- Setting up a governance model, body and policy to ensure the functioning and evolution of the solutions implemented, which will require strong regulatory support.

4.2. Development challenges

- The complete development of a project like this may take a **very long period of time** due to great legal, organisational and technical complexities.
- Such a development will need a long-term strategic approach, a multi-phased implementation plan and a very progressive implementation schedule. In this sense, some high-level proposals would be:
    1. Start with the public sector, leaving private sector to the end. Private sector services will benefit from the experience, resources and solutions developed by the public sector administrations.
    2. Start preparing the legal instruments to support the implementation and deployment of the project.

3. In parallel, start developing the ePowers Taxonomy for public harmonised services only. Do not begin other phases until this is soundly approved.
4. Come up with an eMandate model that is sufficiently generic so it can be used by any public or private service. Do not begin other phases until this is soundly approved.
5. Pilot the first phase before deploying it to all harmonised public services in all MS.
6. Plan and execute a revision period for the pilots before starting the deployment.
7. Plan and execute a revision period before starting the development of the second phase.