

# SEMPER

---

## Report on mandate attributes and solutions for cross-border mandate attributes

---

**Deliverable :** M3  
**Deliverable Name :** Report on mandate attributes and solutions for  
cross-border mandate attributes  
**Status :** Final  
**Version:** 1.0  
**Lead for this deliverable :** RVO.NL  
**Authors:** Ivar Vennekens  
Bart van Bekkum  
Edona Faslija  
**Reviewers** TUG  
**Partner(s) contributing :** TUG, MIHFP, SI-MPA  
**Dissemination Level :** SEMPER project



Co-financed by the Connecting Europe  
Facility of the European Union

This project has received funding from the European Union's CEF programme with action No 2018-EU-IA-0032 under grant agreement No INEA/CEF/ICT/A2018/1633489. This document reflects the view of SEMPER's participants. INEA shall not be held responsible for any use that may be made of the information it contains.

## Executive summary

The new European Commission's Digital Europe program boosts digitalization of public administration and public services and their EU-wide interoperability. With an overall budget of €9,2 billion, the program shapes and supports the digital transformation of Europe's societies and economies: 1. The Single Digital Gateway Regulation is pioneering this transformation: "The single digital gateway will facilitate online access to the information, administrative procedures and assistance services that citizens and businesses need to get active in another EU country. By the end of 2020, citizens and companies moving across EU borders will easily be able to find out what rules and assistance services apply in their new residency. By the end of 2023 at the latest, they will be able to perform a number of procedures in all EU member states without any physical paperwork, like registering a car or claiming pension benefits." 2. Moreover, projects like TOOP pioneer in implementing the once only principle (OOP) cross-border in which natural and legal persons have to provide information to public authorities just once. Authorities need to retrieve available information directly from the source, even if this source is hosted by another member state. An example of this is the retrieval of company information from a business register to open a company branch in another member state. Without proper cross-border solutions for (1) identification & authentication and (2) powers validation, it is not possible (or responsible) to open up digital services to persons from other member states. Identification & authentication are crucial for confirmation of the identity of the person that applies for the digital service, powers validation for confirming the person has the right to act on behalf of the other person.

With eIDAS the European Union adopted a cross-border solution for identifying & authenticating natural and legal persons cross-member state, breaking the first barrier for digitalization of cross-border services. Nowadays, persons can digitally apply for services cross-border on their own behalf in a reliable and easy way. The second barrier to break is cross-border powers validation for persons representing others, e.g. an employee representing its company, an accounting firm representing a client and a parent representing a child. Cross-border powers validation is much less straight forward as it might seem due to differences in national legal frameworks, semantics, governance and organization and technologies deployed. The ISA2 2016.12 (representation powers and mandates) initiative touches a lot of these topics and brings to light the complexity of the matter. It is unlikely that cross-border powers validation can be tackled at once EU-wide. Controlled steps are needed in designing, implementing, and validating a cross-border solution for powers validation.

Building on the results of ISA2 2016.12 and other projects like STORK2.0, the SEMPER project focusses on hands-on cross-border powers validation. SEMPER extends on eIDAS to provide mandate attributes to service providers cross-border and pilots this extension with real services. The project sets an important step forward in making digital Europe happen by transforming abstract concepts into a working software solution.

This milestone 3 deliverable introduces the basics of cross-border mandate management in chapter 1 and describes the eServices (and their requirements) and mandate management systems (and their capabilities) of the project partners in chapter 2 and 3. Furthermore, it defines the semantic model for cross-border mandate attributes in chapter 4 and 5. Finally, in chapter 6, it specifies the eIDAS SAML extension needed for cross-border information flow on mandates.

---

<sup>1</sup> Fact sheet "investing in the future digital transformation 2012-2017", 6 June 2018.

<sup>2</sup> [https://ec.europa.eu/growth/single-market/single-digital-gateway\\_en](https://ec.europa.eu/growth/single-market/single-digital-gateway_en).

## Table of contents

---

<b>Executive summary</b> .....	<b>2</b>
<b>Table of contents</b> .....	<b>3</b>
<b>1. Introduction to cross-border use of mandates</b> .....	<b>5</b>
1.1. Objective.....	5
1.2. Context .....	6
1.3. Member state involvement.....	6
1.4. Actors.....	7
1.5. Systems.....	7
1.6. Baseline scenario .....	8
<b>2. eServices</b> .....	<b>10</b>
2.1. Austria: Business Service Portal .....	10
2.2. Slovenia: Slovenian business point.....	11
2.3. The Netherlands: Message box for Businesses .....	11
2.4. Requirements .....	12
<b>3. Mandate management systems</b> .....	<b>13</b>
3.1. Austria: Online mandate system .....	13
3.2. Slovenia: Central eMandate platform (CeP).....	14
3.3. Spain: Public administration Registry of e-Mandates (REA-AGE).....	15
3.4. The Netherlands: eHerkenning .....	17
3.5. Capabilities .....	18
<b>4. Concepts</b> .....	<b>20</b>
4.1. Introduction.....	20
4.2. Validation and access policy.....	21
4.3. Person.....	22
4.4. Power of Representation (PoR).....	22
4.5. Scope of Power.....	23
4.6. Power use constraint.....	25
<b>5. Mandate attributes</b> .....	<b>26</b>
5.1. Overview.....	26
5.2. Request.....	26
5.3. Request processing rules.....	30
5.4. Response .....	31
5.5. Response processing rules .....	34
<b>6. eIDAS SAML extension</b> .....	<b>36</b>
6.1. Design principles.....	36

6.2.	SAML Extensibility .....	37
6.2.1.	Current eIDAS SAML extension .....	37
6.3.	Extending the eIDAS SAML Authentication Request .....	38
6.3.1.	Powers of Representation Requirements .....	38
6.3.2.	Represented .....	42
6.3.3.	Representative.....	42
6.3.4.	Intermediary .....	43
6.3.5.	Additional Representation Attributes .....	44
6.4.	Extending the eIDAS SAML Authentication Response .....	45
6.4.1.	Powers of Representations, Status, Error Code .....	45
6.4.2.	Represented .....	47
6.4.3.	Representative.....	48
6.4.4.	Intermediary .....	48
6.5.	Extending the eIDAS SAML Metadata Objects .....	48
<b>Annex I:</b>	<b>pilots.....</b>	<b>50</b>
<b>Annex II:</b>	<b>definitions .....</b>	<b>51</b>
<b>Annex III:</b>	<b>structure and examples of scope .....</b>	<b>56</b>
<b>Annex IV:</b>	<b>legal.....</b>	<b>59</b>
<b>Annex V:</b>	<b>process .....</b>	<b>60</b>
<b>Annex VI:</b>	<b>ISA2 2016.12 RPaM .....</b>	<b>61</b>
<b>Annex VII:</b>	<b>STORK 2.0 .....</b>	<b>64</b>
<b>Annex VIII:</b>	<b>SDGR.....</b>	<b>66</b>
<b>Annex IX:</b>	<b>TOOP .....</b>	<b>69</b>

## 1. Introduction to cross-border use of mandates

SEMPER aims to provide solutions for cross-border powers of representation and e-mandates. The project will construct the semantic definitions of mandate attributes and enhance the eIDAS Interoperability Framework with appropriate elements on protocol-level and integration modules for connecting national mandate management infrastructures. This will support Service Providers in enabling representation of legal or natural persons within their eIDAS enabled services as well as the eIDAS node operators to access national mandate infrastructures as Attribute Providers. Specifically, SEMPER will enhance eIDAS node implementation of the project's beneficiaries in the piloting infrastructure.

### 1.1. Objective

*This document specifies the core concepts and mandate attributes for cross-border use ('the semantic model'). It harmonises the cross-border information flow on powers of representation. The focus of this document is on the requirements of the SEMPER pilots. Although concepts and attributes have been defined in a generic way, its usability beyond SEMPER has not been assessed.*

This model does not:

1. Harmonise the way national mandate management systems register and validate mandates, the concepts by which the systems have been designed, the structure of the registries, the technology by which they are implemented, etc. The mandate management systems *as is* will be connected to the national eIDAS services. For interoperability, member states have to implement 'national-to-SEMPER' translation of mandate attributes.
2. Harmonise the way service providers grant people access to their electronic services. Service providers can still have their own access policy by which they decide upon granting access in specific situations. Service providers should be able to handle cross-border mandate attributes though.
3. Deal with the process of service fulfilment. Access is a precondition for the service provider to start service fulfilment. For service fulfilment, there will be additional interaction between the person and the service provider to validate compliance with service criteria.

## 1.2. Context

With the introduction of eIDAS, authentication can be handled cross-border and communicated to the service provider in another member state. eIDAS does not specify the powers of representation though. SEMPER extends on eIDAS to provide the service provider with proper information on the powers a (natural or legal) person has to represent another (natural or legal) person. The SEMPER model specifies the information flow between mandate attribute providers and service providers through the eIDAS network in order to provide access to electronic services in another member state. Furthermore, SEMPER extends eIDAS nodes to perform semantic translation of powers of representation from formats that are specific to member states to SEMPER's format.

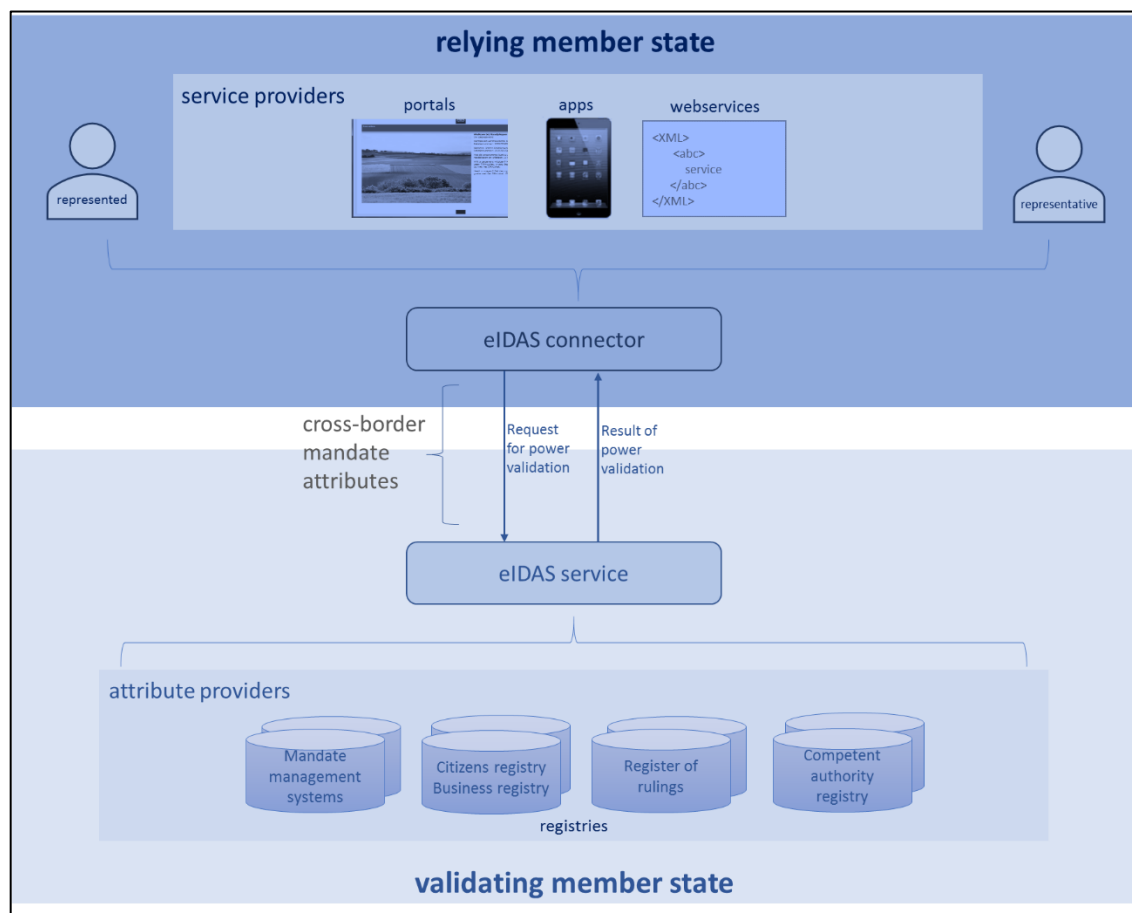


Figure 1 context

## 1.3. Member state involvement

The SEMPER model supports bilateral communication between member states. One member state authenticates the user and validates powers. The other member state relies on the mandate attributes to provide the service to the user. In this bilateral communication, a member state can be a:

- **Validating member state**

The country responsible for retrieval and assessment of mandate attributes as well as providing mandate attributes to relying member states. In SEMPER, the validating member state is the country in which the mandate management attribute provider is located. The validating member state is the 'sending country of mandate attributes'.

- **Relying member state**

The country of the service provider that is responsible for granting access and fulfilling the service. The relying member state is the 'receiving country of mandate attributes'.

#### 1.4. Actors

In the SEMPER use cases, several actors are involved. The main actors in the relying member state are the service providers, in the validating member states the (mandate) attribute providers. The representative and represented are persons from the validating member state that act (or being acted on behalf of) in the relying member state. "From" in the SEMPER use cases means: "have their eIDs issued by and have their mandates registered in".

- **Service providers**

Service providers are responsible for the interpretation of mandate attributes in electronic service fulfilment. In order to do so, persons have to be authenticated and – in case of representation – powers have to be validated. Nowadays, this is nationally done in a federated way by identity providers and mandate management systems. With the responses from these systems, the service provider grants people access to their electronic services (or denies access in case powers are not sufficient or could not be assessed properly).

- **Attribute providers**

The attribute providers are the organisations that handle and provide information on the powers of a person to represent another person. The attribute providers need to connect their systems to the eIDAS service to provide cross-border information on powers.

- **Representatives**

Representatives are persons authenticating to the service of the service provider in order to act on behalf of another person. The representative is the person with the powers to act.

- **Represented persons**

The represented person is the person on whose behalf the representative acts. The roles representative and represented are not fixed. In one case, a person can be a representative, and in another case, the person can be represented person.

#### 1.5. Systems

The main systems involved are:

- **Portals, apps, web services (eServices)**

These refer to the systems the service provider uses to grant a person access to its services as well as to fulfil the service. These systems include (federated) identity and access management suites on a national or service provider level.

- **Registries**

The registries take care of the registration, validation, and issuance of information on powers. These systems are to a large extent already in place in the participating member states and have been tailored for national law, regulations, and policy. The systems have common elements with regard to the mandator, the mandate, the mandatee, supported sources of powers and scope of powers. Within SEMPER, these registries are integrated 'as is'. This project aims at cross-border use of already available information instead of harmonising and redesigning national mandate solutions. Furthermore, all components processing (registering, updating, extracting, combining, validating, deleting) powers information nationally are considered part of the registries.

- **eIDAS connectors**

The receiving part of the eIDAS node, to be used by relying member states. eIDAS connectors need to be connected to the eIDAS services of other participating member states. This entails an exchange of certificates and metadata.

- **eIDAS services**

The sending part of the eIDAS node. To be used by validating member states. The eIDAS services can be proxy services and middleware services. Within the SEMPER consortium, all member states have implemented proxy services.

1.6. Baseline scenario

The SEMPER scenario supports authenticating and validating powers of a person in one member state and accessing the electronic service in another member state. This corresponds with RPAM<sup>3</sup> scenario 1.12 of the ISA<sup>2</sup> 2016.12 action. This SEMPER baseline scenario is eIDAS-driven: powers will be validated as part of the online eIDAS authentication flow.

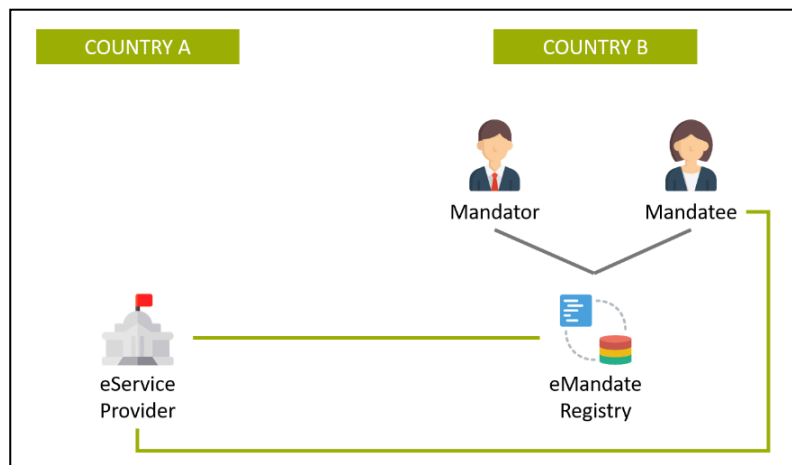


Figure 2 RPAM scenario 1.12

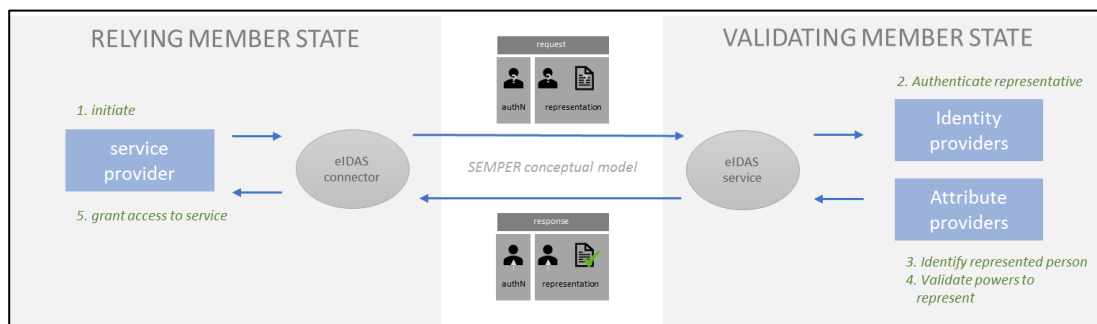


Figure 3 baseline SEMPER scenario

The process flow of this scenario is:

**1. relying member state - initiate:**

A person browses to the website of a service provider and chooses to log in on behalf of another person from another member state. The service provider initiates a cross-border authentication by sending a request to the (central or decentral) eIDAS connector. The service provider specifies the person attributes it wants to receive and the powers that

<sup>3</sup> ISA<sup>2</sup> 2016.12: Semantic interoperability of the representation of powers and mandates, RPAM\_Description of cross-border scenarios for eMandates\_v2.0.



need to be validated. This request is validated and forwarded to the eIDAS service of the member state the person has an eID of (the validating member state).

**2. validating member state - authenticate representative:**

(One of) the identity providers of the validating member state authenticates the person at (at least) the requested level of assurance (LoA).

**3. validating member state - identify represented person:**

The mandate management system of the validating member state identifies the represented person. This can be done by the mandate management system in several ways, e.g. by requesting the representative to enter the identifier of the represented person or by presenting a list of mandators he may represent. As an alternative, the mandate management system may require the representative to select the mandate to use directly.

**4. validating member state - validate powers to represent:**

The mandate management system validates the powers of the representative to act on behalf of the represented person. The powers should be sufficient to access the service defined by the service provider: the scope of powers. Note that the scope of powers as registered in the mandate management system may be broader than needed for this service. E.g. full powers will be sufficient to apply for any service. After validation of powers, the response will be sent to the eIDAS connector of the relying member state via the eIDAS service of the validating member state. The response contains the scope requested and the outcome of the validation of the powers (the powers are either sufficient or insufficient for the requested scope).

**5. relying member state - grant access to service:**

The relying member state uses the response to decide upon granting access to the representative to apply for the requested service on behalf of the represented person (eAuthorisation). Therefore, it assesses the authentication of the representative as well as the powers. Both need to provide enough assurance<sup>4</sup>.

As SEMPER is eIDAS-driven, powers will only be validated as part of (or directly following) the authentication process. Service providers might want to validate powers again later on in the service fulfilment process, e.g. when user interaction takes place by phone or paper. This is out of scope for SEMPER although there might be a need to add this in the future.

---

<sup>4</sup> In validating powers, the mandate management system has to validate the assurance level of the mandate as well. In compliance to STORK 2.0 this model uses the same eIDAS LoA's for expressing assurance for authentication and mandates. E.g. a service requiring LoA substantial needs a mandate that provides LoA substantial as well. A mandate that has been registered on LoA low must not lead to a successful powers validation on a service requiring substantial.

## 2. eServices

SEMPER will pilot with several eServices that integrate cross-border electronic mandates. This chapter will briefly introduce these eServices and summarise the service's main requirements.

### 2.1. Austria: Business Service Portal

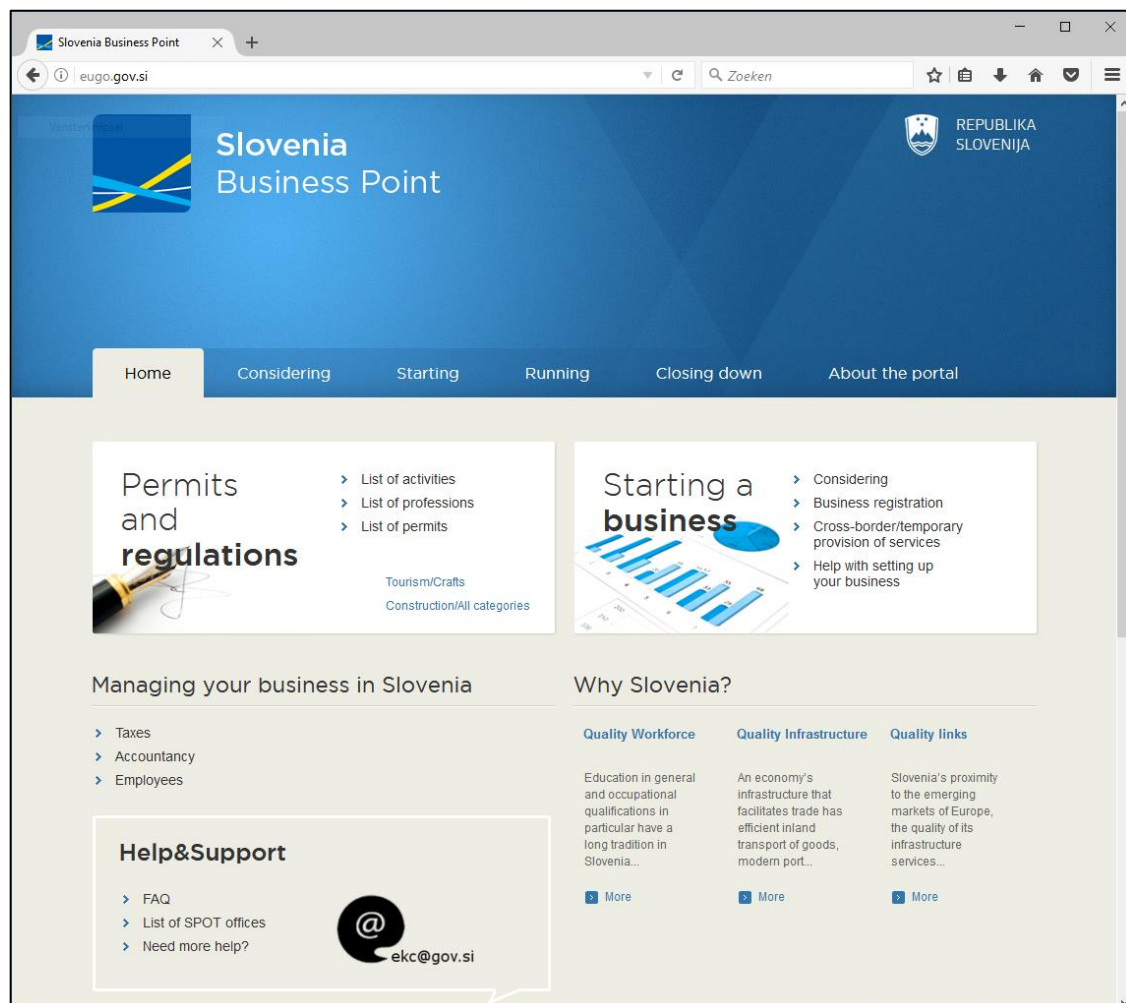
The Business Service Portal, called 'Unternehmensserviceportal (USP)' in German, has been launched with the aim to serve as single entry point for businesses when interacting with public administration. This portal offers access to information as well as various online services that allow businesses to efficiently fulfill their legal obligations.

A typical use case for representation is the reporting of various aspects (e.g. financial) to the public administration. A general manager, authorized officer or other employees may have a mandate to be allowed to submit reports for a company or other legal person.

The screenshot shows the 'Unternehmensserviceportal - Chromium' browser window. The address bar displays 'https://www.usp.gv.at/Portal.Node/usp/public'. The page layout includes a top navigation bar with links for 'Formulare', 'Gesetzliche Neuerungen', 'Alle Themen', and 'Lexikon'. A search bar is located below the navigation. The main content area is divided into several sections: 'Über das Unternehmensserviceportal - USP', 'Neu im USP: Ausschreibungssuche', 'News', and 'Aktuelles Thema: Umsatzsteuersenkung auf Nächtigungen'. The right sidebar contains 'Anmelden', 'Registrieren', 'RSS-Feeds', and 'Gebärdensprache' options.

## 2.2. Slovenia: Slovenian business point

The SEMPER e-mandates solution will be integrated into the Slovenian business point (<http://eugo.gov.si/>) as the service provider.

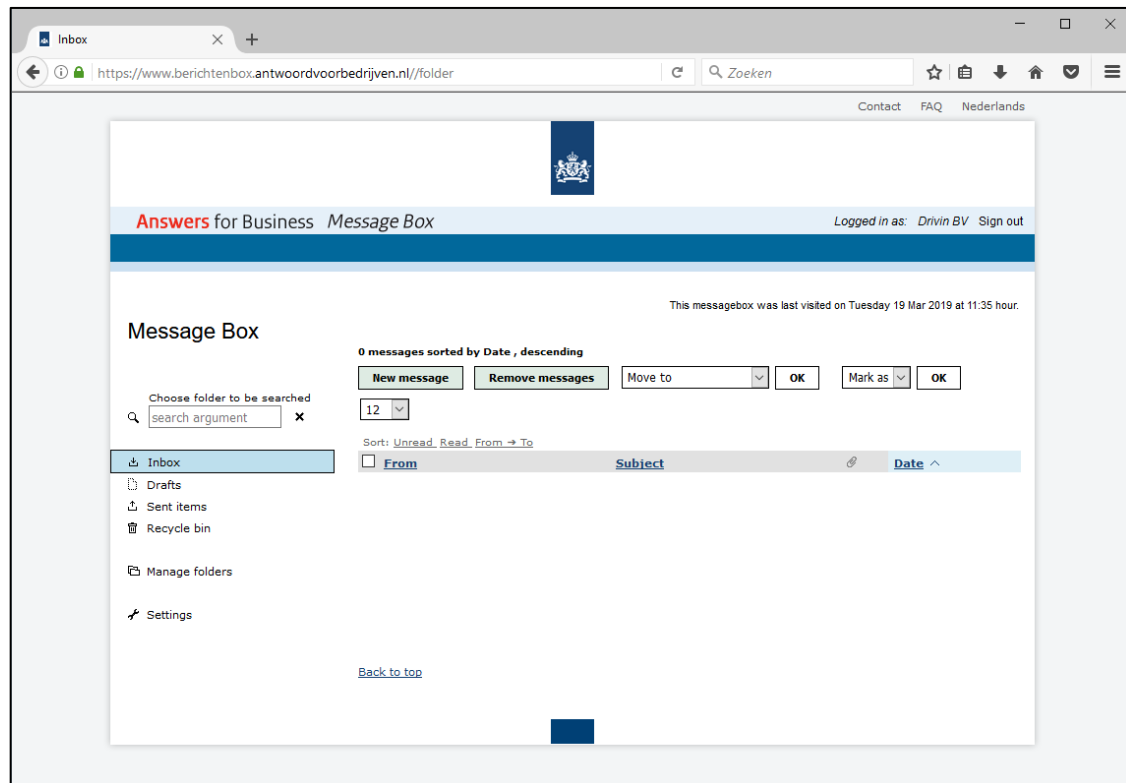


## 2.3. The Netherlands: Message box for Businesses

The Message box for businesses is a secure email environment for the exchange of messages between entrepreneurs and the government. The system can also be used for the exchange of messages between governmental organisations. The Message box enables the safe and easy exchange of (sensitive) information. For example, license application decisions. But also notifications, subscriptions, objections, and registrations. The Message box replaces traditional, classified, and normal mail with secure digital messaging. It is part of the Single Point of Contact under the Service Directive.

NL intends to pilot the use of the message box as a representative of a cross-border organisation: (a) employee representing the company and (b) intermediary company representing the company.

For accessing the message box of a company, the Dutch person needs to have the powers on the eHerkenning service 'Berichtenbox voor bedrijven'. In SEMPER there should be a cross-border equivalent.



## 2.4. Requirements

Analysis of the SEMPER eServices leads to some requirements for cross-border eMandate attributes. The SEMPER model should:

- support representing legal persons and natural persons (but in SEMPER participants will only pilot with natural persons representing legal persons);
- in all cases start with authenticating a natural person via eIDAS (there are no use cases in SEMPER where a legal person authenticates without a natural person present);
- in all cases have the represented person selected at the validating member state;
- (at least) support powers by mandate, by professional representation (regulated profession) and by company executive (as defined in company law);
- support chained mandates in which a representative of a company acts on behalf of another company (Dutch service);
- include harmonisation on services;
- allow for another mechanism of specifying services in the absence of harmonisation;
- allow for differentiation in access policy of the service provider (e.g. allow specific types of powers and not others).

There is no SEMPER use case for:

- standalone powers validation afterward (first authenticating and later on - maybe days later – validate powers while the user is not online);
- multilateral cross-border interactions (person from MS A representing a legal person from MS B applying for a service in MS C).

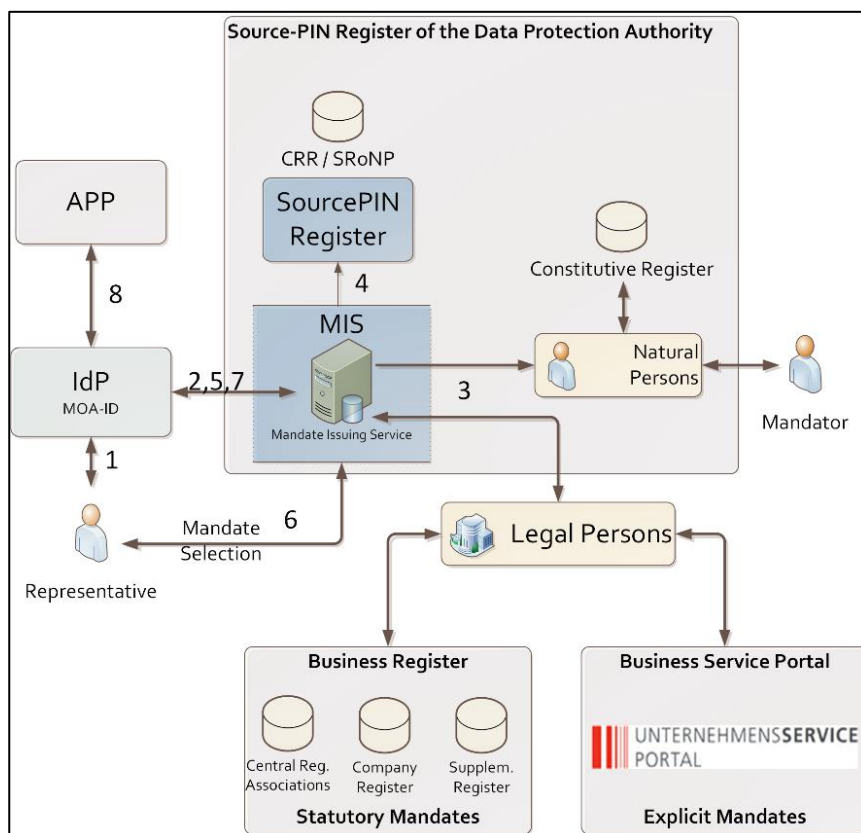
### 3. Mandate management systems

SEMPER will pilot with mandate management systems of the participating countries. This chapter briefly describes these national mandate management systems and presents the common capabilities.

#### 3.1. Austria: Online mandate system

The Austrian eID<sup>5</sup> (Mobile Phone Signature or Citizen Card) can also be used to conduct procedures with authorities on someone else's behalf, provided that proper mandate authority has been granted for that person. The use of representatives as it is common in conventional business, is also available in eGovernment.

Electronic mandates are especially interesting for businesses since the eID with both the card-based Citizen Card and Mobile Phone Signature options can automatically depict legal representation, whether for lawyers or business managers in a company. The only prerequisite is that a conventional mandate for the business or public authority already exists. This means that the existing mandate will simply be represented in electronic form. It allows the representative to carry out procedures electronically on behalf of the principal (the one who grants the mandate). The Austrian approach uses so-called "online mandates" where the assertion of a representation is created just in time (JIT) when it is needed by the application. This gives fresh assertions, improves usability, and better fits an increasing demand for mobility.



<sup>5</sup> <https://www.buergerkarte.at/en/index.html>

The concept of online mandates involves the following entities, which are illustrated in the figure:

- The APP is the (eGovernment) application, at which the representative authenticates and acts on behalf of the mandator.
- MOA-ID is an open source identity provider middleware of the Austrian eGovernment initiative, which bundles several authentication and identification functionalities for the Austrian Mobile Phone Signature and Citizen Card.
- The Mandate Issuing Service (MIS) is the core component, which handles the communication with all involved entities and generates online mandates on demand. The MIS is operated by the SourcePIN Register Authority (SPRA).
- The SourcePIN Register (SPR) is the interface between the MIS and the Central Residents Register (CRR) and the Supplementary Register for Natural Persons (SRoNP). It is used by the MIS to request a mandator's sourcePIN on demand. The sourcePIN is a citizen's unique identifier, which, however, cannot be directly used in eGovernment procedures. A sector-specific PIN (ssPIN) derivation thereof has to be used instead.

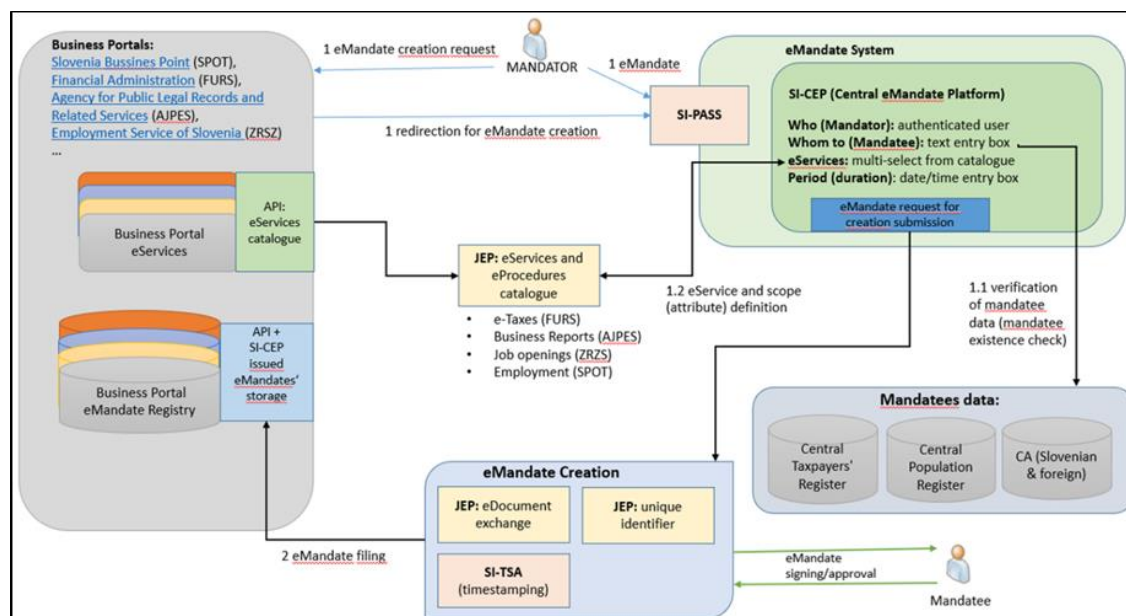
### 3.2. Slovenia: Central eMandate platform (CeP)

In Slovenia several years ago it was decided to centralize the e-government development, especially for the common functionalities, required by most of the e-services. The authentication and trust services were among the most important. In 2015 the State government center for trust services SI-TRUST at the Ministry of Public Administration launched the Service for authentication and e-signature SI-PASS that is now successfully integrated into the main e-government portals. SI-PASS also integrates an eIDAS node. SI-PASS offers the functionality of server-based e-signatures, following the eIDAS requirements.

The next year SI-PASS will also integrate the functionality for establishing mandates (as a willful act). SI-PASS will integrate the central e-Mandate Platform SI-CeP. At present, the mandates are offered by several e-government portals, like e-taxes, one stop shop for companies. Each portal has its own solution, at present not integrated with SI-PASS. The Slovenian Central eMandate Platform will offer the possibility to create a mandate for both natural and legal persons (and professionals, e.g. lawyers) as a willful act. The functional specification for SI-CeP is finished, and the development will be done by outsourcing (under the public procurement).

In Slovenia, companies are represented by persons so determined by law or by the founding act of the company under law (statutory representative). This type of presentation is out of the scope of SI-CeP. The representation can be retrieved from the Business Register. When a natural person (that is at the same time legal representative of one or several companies) access one e-services, where legal representation is important, he/she can use his/her credential (as a natural person) and based on the authentication of this person SI-PASS retrieves the legal representation from the Business register.

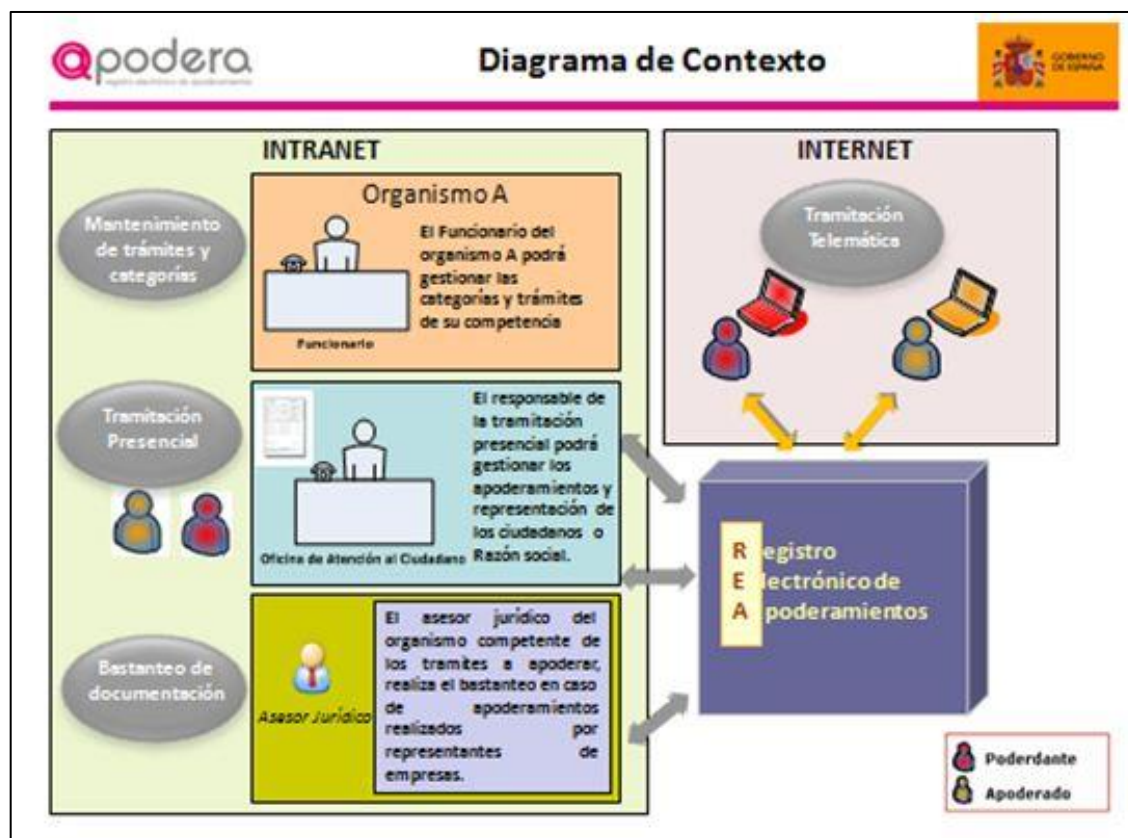
The Slovenian Central eMandate Platform will offer the central system for establishing a mandate for between natural and legal persons (and professionals, e.g. lawyers) as a willful act. The precondition to use SI-CeP for e-services is their integration to SI-PASS service. The user that wishes to establish a mandate can access the e-service directly (and he/she is redirected to SI-PASS with SI-CeP functionality) or via SI-PASS (as shown in the figure). He/she can choose different e-services to be subject of the mandate, or establish a general mandate. The SI-CeP will offer users through the catalogue of services different possibilities and potential limitations on mandates. Created mandates are stored within the e-services systems and activated when the user access the e-service through SI-PASS.



### 3.3. Spain: Public administration Registry of e-Mandates (REA-AGE)

Digital public services require electronic access to the representation registries in order to validate that representatives can represent other persons before public administrations in certain public services. REA-AGE allows the inscription of mandates that a natural or legal person can grant to third parties to act on their behalf when accessing a public service. The users of the system are natural or legal persons, who can empower any natural or legal person to act on their behalf. In case of a legal entity, the legal representation of the entity must be accredited with a general mandate to the natural person they are granting the mandate.

The mandates should be granted for the public services included in the system. These are grouped into Categories, determined by the competent body. If the latter updates the groups of procedures of a category, adds or eliminates procedures, mandates will be automatically updated without the need for intervention by the natural or legal person.



There are three types of administrative mandates:

- A general power for the mandatee to act on behalf of the mandator in any administrative act and before any administration.
- A power for the mandatee to act on behalf of the mandator in any administrative act before a specific administration or organization, as state government, autonomous communities (regional governments), local entities (local governments), public bodies and other institutions
- A power for the Mandatee to act on behalf of the Mandator only to carry out one or several specific procedures specified in the e-mandate (for instance paying taxes or receiving notifications).

In order to identify a represented/representative person, the data requested and stored is defined in Spanish regulations (<https://www.boe.es/buscar/act.php?id=BOE-A-2017-7719>). It does not correspond to the MDS defined in the eIDAS Regulation. The attributes requested to a natural person are: ID (DNI), First name, family names, address, email (optional) and phone number (optional). For a legal person are requested: ID (NIF), legal name, phone number (optional), email (optional) and address (optional). In addition, in the Public administration Registry of e-Mandates, chains of intermediaries are not allowed.

Overall, the process to register a mandate:

- REA-AGE: a mandator (natural or legal person) logs in the system using an eID. The mandatory chooses the type of the power he wants to give. If it is type B or C, he has to select also the public body and for type C the specific procedures. He provides the data about the mandate (natural or legal person). He signs the mandate.
- Attending a public office: the mandator identifies himself. He gives the documentation about the mandate to a civil servant. The civil servant enters the data in REA-AGE.



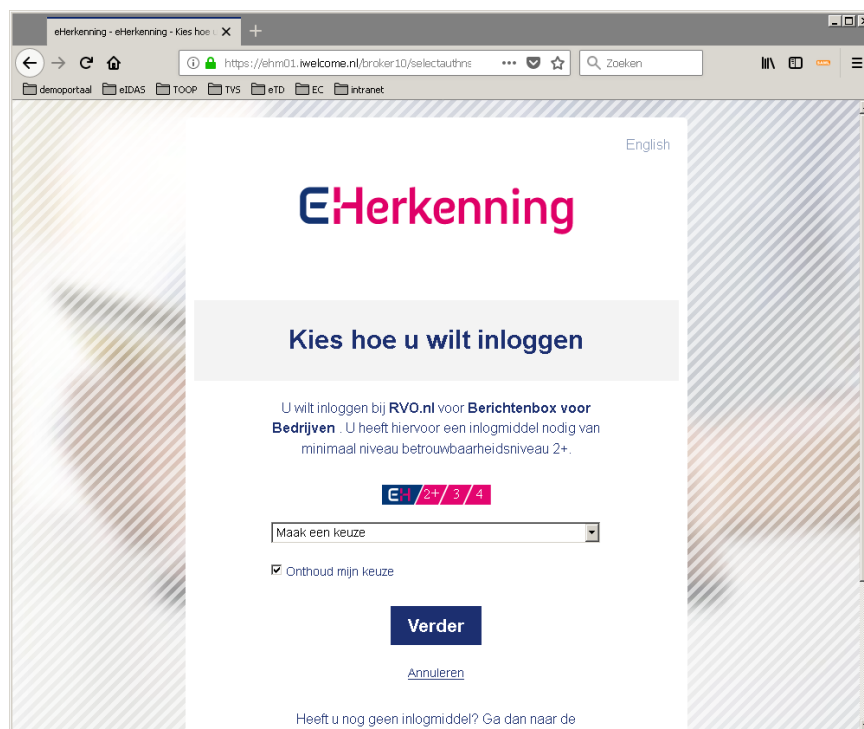
Looking up a mandate or to check the permissibility of the representation can be done by a civil servant or automatically by a service:

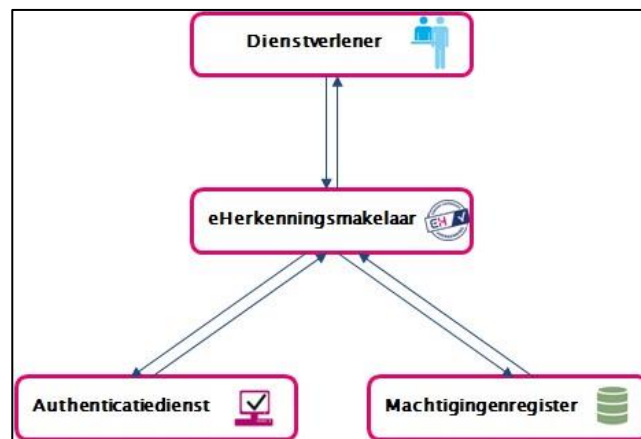
- civil servant: a civil servant can look up mandates and check their validity using REA-AGE system.
- online Public service: a mandatee identifies himself on a service. He enters the mandatory data. The service uses the REA-AGE web service to check the validity of the mandate. The mandatee will be authorized or denied access.

REPRESENTA is a layer above the representation systems to which the public service can connect to validate mandates. It is a broker web service to retrieve information on mandates from several sources at once, like REA and the different registries of professionals (e.g. the Registry of social graduates and the Registry of administrative agents).

### 3.4. The Netherlands: eHerkenning

eRecognition (eHerkenning) is an integrated solution for authentication and mandate management. Connected service providers define their services, the required attributes and requested LOA's. At authentication-time, the service provider requests authentication for one of its services. The broker initiates authentication by activating an identity provider (IdP, user selected) and subsequently requesting the mandate registry to validate the person's powers. As soon as a person does not have the powers to apply for the specified service, the authentication flow will fail.





Mandates in eRecognition are service-oriented, which means that a mandator may grant the powers to apply for a chosen service to a specific mandatee. Besides selecting one specific service, the mandator may also chose 'general representation' for all services at once. Usually, the mandator is a company and the mandate is a natural person involved in the company. To some extent eRecognition also supports company-company representation, creating chains of mandates with intermediate companies. A mandate gives the mandatee the right to represent, not the obligation to do so. Mandates in eRecognition are valid as soon as they are registered in a registry (in conformance to the rules set out to do so in the framework). Mandates may expire and may be revoked by the mandator. No additional documents will be stored (or required) to prove the existence of the mandate.

The framework supports restricting the powers to represent another person to - for example - a maximum amount. It also supports the registration of a professional powers (e.g. a healthcare professional, a notary, or a lawyer), although these functions are not being used (or implemented by the mandate registries) at this moment. eRecognition does not support isolated powers validation requests. Powers will only be verified after authentication of the user.

eRecognition has a joint public-private governance. Multiple commercial IdP's and mandate registries operate within the framework. Dutch service providers connect to eRecognition by contracting one of the eRecognition brokers. For cross-border service providers, the Dutch eIDAS node behaves towards eRecognition 'like a service provider'.

### 3.5. Capabilities

Our analysis of the mandate management systems revealed several common capabilities of the systems that are needed for SEMPER. The mandate management systems mostly:

- Support powers in which two persons are involved: the mandator and the mandatee. Possible sources are: mandates by willful act, legislation (civil law: parents may represent their child, business law: executives can act on behalf of their company) and court rulings.
- Support regulated professions as a source of powers. Member states can validate a person's profession. Regulated professions do not always require an explicit mandate. In some cases, the representative does not need to present his/her powers of representation because of the registration as a notary, lawyer, etc., while in other cases, he/she does.
- Allow for full powers: the mandatee may access all services on behalf of the mandator.

## SEMPER

### M3 Report on mandate attributes and solutions for cross-border mandate attributes

- Allow for non-full powers: allow scoping of powers to a service provider, service, procedure or type of procedure (receiving notifications, handling post, signing applications).
- Support a specified period of validity and support unlimited validity (until explicitly revoked).
- Allow for restriction to certain activities or transaction values (like Euros).

## 4. Concepts

This chapter defines the concepts of the SEMPER semantic model. Accurate definition of concepts is important for common understanding of cross-border mandate information.

### 4.1. Introduction

This model defines the core concepts for cross-border information flow on powers of representation:

#### 1. Person

*a natural or a legal person*

Persons are of interest to this model as far as their identification ('identifying the person') is concerned, for which in compliance with eIDAS, the eIDAS minimum dataset is used. For service fulfilment additional attributes may (or will be) required that are not incorporated in this model. As this model deals with representation, in every case at least two persons are identified in the process: one as represented person and one as representative. Additional persons may be identified as intermediaries in case of chained mandates, e.g. an accounting firm liable for the firm's employee (representative) acting on behalf of a client (represented person). Represented person, representative, and intermediary are the roles a person can have when using a mandate.

#### 2. Powers of representation

*the right to act on behalf of another person*

By using these powers, a representative acts on behalf of the represented person. In case the powers are full ('full powers'), the powers are not restricted to member states, services, etc. This model defines all other powers as non-full, meaning they cover a specified scope of activities and may be bound by constraints, like maximum transaction value. Powers to represent stem from sources, like mandates and regulated professions.

#### 3. Scope of power

*the extent to which the representative can act on behalf of the represented person*

The scope has to be expressed in a machine-readable way to provide digital access to services. Therefore, this model defines two methods for expressing the scope of powers:

- (1) harmonised services, like the services defined by SDGR;
- (2) non-harmonised services (or parts thereof).

Harmonised services are similar in all member states. Scopes expressed in terms of harmonised services are unambiguous cross-border. Non-harmonised services have been defined by individual service providers and are not harmonised across the EU. It is up to each service provider and mandate management system to choose one or more of these methods for expressing/interpreting powers of representation. For cross-border access to a service, both service provider and mandate management system need to support the same method or be able to resolve the scope of powers from one method to another.

#### 4. Power use constraints

*a restriction of the right to act on behalf of another person*

The power someone has to use one or more services may be restricted. Such restrictions are called Power Use Constraints (PUC). PUCs are expressed in an aspect, like "maximum transaction value", and a value like "€100.000". PUCs may be harmonised as well. Harmonised PUCs are defined as part of the service harmonisation process and should be recognised by mandate management systems as well as service providers. Non-harmonised PUCs are defined by individual mandate management systems. Enforcing

non-harmonised PUCs is less straight forward as service providers need to understand the meaning of the PUC as defined by the mandate management system.

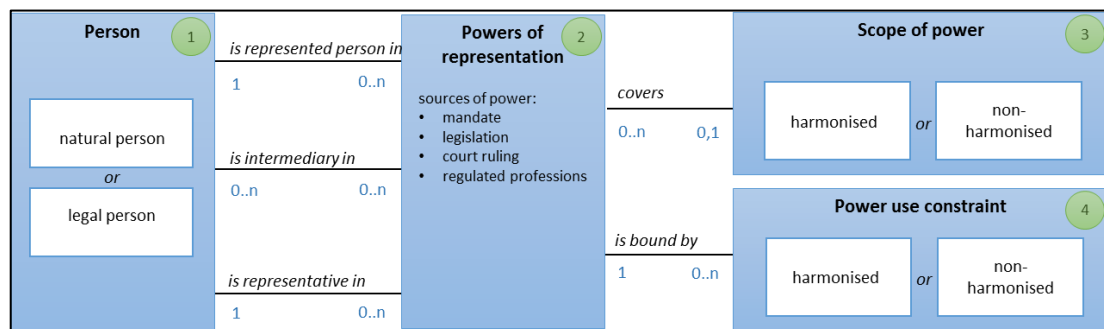


Figure 4 interrelated core concepts

Explanation of optionality and cardinality:

- Powers of representation always have one person represented and one person representing. Optionally, there may be one or more intermediary persons involved in the powers of representation. A person can be represented person by use of one or more powers of representation. The same goes for representative and intermediary.
- The powers of representation may cover a (one) scope. In case no scope has been specified, the powers are full. A certain scope (like for a harmonised service) may apply to multiple powers of representation as there can - for example - be lots of mandates granted on a specific harmonised service.
- Optionally, the powers of representation may be bound by one or more power use constraints. Each power use constraint is specific for one power of representation though.

All concepts are defined in annex II. The next chapters elaborate on these core concepts.

#### 4.2. Validation and access policy

In the SEMPER philosophy, it is up to the validating member state to define the rules for validation. These rules specify in which cases powers are valid. E.g. the guidelines for registering mandates at level of assurance low, substantial and high and the (type of) services for which the representative has to accept the mandate. National law, principles, and policy of the validating member state apply.

The validating member state basically answers to a powers validation request with an ok/not-ok response, which means that the member state has determined that the powers are valid or not according to national validation rules. The relying member state will trust the validating member state and accept the response as provided. The relying member state will not redo any validation of the powers or check proper execution of validation rules by the validating member state. Eventually, the validating member state should be legally liable for the validation of powers. And, just like in eIDAS, the relying member state should always accept a powers validation result from 'notified' member states.

Just as the validating member state is responsible for validating a person's powers, the relying member state is responsible for granting access according to its own rules (eAuthorisation). In granting access, the rules and legislating of the relying member state apply (in contrast to the rules of the validating member state). Each relying member state / relying service provider

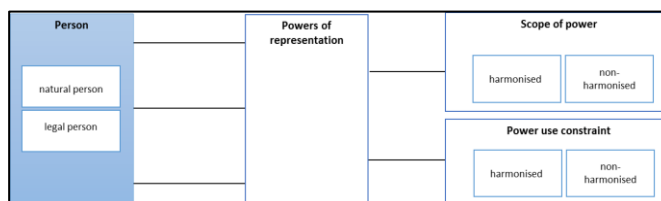
needs to determine the required level of assurance, the sources of power allowed, the need to receive information on the intermediary person(s), etc.

To allow for variations in access policy, the relying member state specifies:

- the required attributes and level of assurance (in compliance to eIDAS);
- the person types it allows for the represented person and representative, e.g. only legal persons can access the service;
- the requirement for providing attributes of one or more intermediary persons;
- the sources of power allowed;
- the regulated professions that it grants access to.

### 4.3. Person

The representative, represented person, and intermediary are all persons, either legal or natural. This semantic model adheres to the following principles regarding persons:



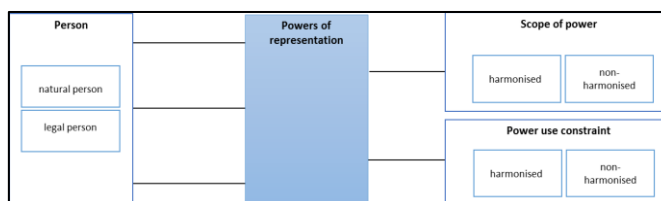
1. SEMPER uses eIDAS for identification and authentication of natural and legal persons.
2. SEMPER does not require additional person attributes. Identifying the represented person, representative and (optionally) one or more intermediaries is enough for making access decisions ('starting the service fulfilment process').
3. All possible representation scenarios between persons are supported: a natural person representing a legal person, a legal person representing a natural person, a natural person representing another natural person and a legal person representing another legal person.
4. Chained powers (a person has passed on the power of representation to another person) are supported.
5. SEMPER supports requesting and providing information on intermediary persons. The intermediary person is not actively involved in the use of a service, but is a person in the chain constructing the powers of the representative. An example of an intermediary person is the accounting firm responsible for the employee (representative) representing a client (represented person) of the firm. Not all member states will request and/or provide information of the intermediary.

Additional attributes might be needed for service fulfilment. eIDAS – in the future – aims to supports these as domain-specific attributes. Domain-specific attributes for service fulfilment are out of SEMPER's scope.

### 4.4. Power of Representation (PoR)

This semantic model adheres to the following principles regarding the power of representation:

1. Information on powers will be provided as a 'snapshot' as information may change quickly (e.g. a mandate may be revoked). The service provider should not use the cross-



border powers information any longer than the (eIDAS-)statement is valid (the current service, until logged out). Therefore, no information on the period of validity of the representational powers will be provided.

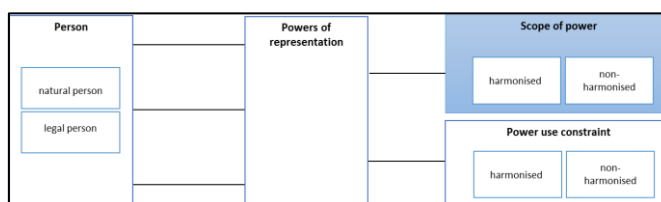
2. Full powers are the power of representation to apply for any service at any service provider in any member state. Non-full powers are powers of representation that are related to a specified scope: a harmonised service or a non-harmonised service (or part thereof).
3. Powers of representation stem from a source:
  - a mandate: powers granted by a wilful act (voluntary);
  - legislation: powers of representation that are defined in civil or business law (for example, a mother representing underage child, or an executive representing company);
  - a court ruling: a judge granting powers of representation to a person;
  - a regulated profession: the power someone has as a regulated professional (notary, lawyer).

Member states will provide information on the source of power to relying member states in the response, so that service providers can make informed access decisions. SEMPER allows service providers to differentiate in their access policies. E.g. one service provider may accept representation by a person with a regulated profession (e.g. notary registered in an official register) where the other service provider may require the existence of a mandate.

4. The subdivision in power sources is driven by differences in operational handling of the powers. Mandates will be registered in mandate management systems, powers based on legislation have their origin in citizen and business registers, court rulings in dedicated ruling registries and regulated professions will be registered in dedicated registers for these professions.
5. Joint powers (e.g. two executives that both have to sign a contract) are outside the scope of the SEMPER-model. A service provider will not be informed that a power is restricted in the form of a joint power, nor how many persons are involved in the joint power and the identities of the persons involved. If a mandate management system determines that a power is a joint power, the powers should be declared as insufficient.
6. Limitations in the power to act on one's own behalf (e.g. as the person is a ward of court) are out of scope of the SEMPER-model as this is not a representation scenario.
7. Feedback of the service provider on actual representation, for example, when the power is a one-time-only power which will be terminated after usage, is not part of the SEMPER-model. This type of communication is not compatible with the eIDAS interoperability framework nor with the eIDAS software.

#### 4.5. Scope of Power

The scope of power expresses the activities a representative can perform on behalf of the represented person. This semantic model adheres to the following principles regarding the scope of power:



1. The Scope of the Power of Representation can be defined with different methods:
  - a) harmonised;
  - b) non-harmonised.
2. Harmonised: there are several European initiatives for service taxonomies, such as the ISA<sup>2</sup> 2016.29 Catalogue of public services, the SDGR, and the ISA<sup>2</sup> action 2016.12 RPaM. These initiatives aim at standardising the structure for describing services as well as harmonising the services themselves. At this point in time, the standardisation is work in progress so that SEMPER cannot fully anticipate the final outcome. Therefore, the SEMPER model (1) supports the concept of harmonised services, (2) supports multiple catalogues of harmonised services but (3) does not – at this point in time – allow for a hierarchy in expression of these power, as a hierarchy might be in conflict with future standardisation results. Furthermore, such a hierarchy is not required for the SEMPER's pilots. For now, the SEMPER model defines harmonised services as a 'plain list of items from a specified catalogue' on which to express powers, which can later be replaced as outcomes of related standardisation activities outside the control of SEMPER become available.
3. Whenever available, cross-border communication on the scope of powers will be expressed as harmonised services. Service providers should request the validation on powers by reference to harmonised services as soon as appropriate harmonised service are available. To do so, the service provider can incorporate the harmonised service in its process, implement local mappings of the service provider's specific services to the harmonised equivalents or rely on national mapping tables whenever available.
4. Non-harmonised: not all services will be harmonised across the EU, either because harmonisation is an ongoing endeavour and the service was not yet harmonized, or because some services are less suitable for harmonisation as they are very specific to the member state or service provider. For this purpose, the SEMPER model supports expression of powers on 'non-harmonised services'. These scopes allow for a hierarchy with regards to: a member state, a service provider, a service, a procedure or a type of procedure. This hierarchy is a result of analysis of SEMPER services and mandate management systems. It does not pretend to be applicable for all (non SEMPER) use cases. Services delivered by EU institutions can also be expressed within the concept of non-harmonised services: the EU is seen as a 'member state' with country code EU<sup>6</sup>.
5. A power on a higher level element in this hierarchy should be considered as sufficient for all elements underneath. E.g. a mandate on service provider "RVO.nl" will be valid for all services of RVO.nl today and in the future. And a mandate on member state "Austria" will be valid for all services available from Austrian service providers.
6. Non-harmonised services and procedures are service provider specific (they are defined by the service provider).
7. The types of procedures, like requesting services, signing application forms, reading messages, don't have to be service provider specific. Some types of procedures may be in use country-wide.
8. Non-harmonised services are used to express powers in the absence of harmonisation.
9. The right to manage mandates (powers to delegate) is not incorporated in this model as a separate type of powers. The powers to delegate will be expressed as a scope of powers:
  - the mandate management system will be a "service provider"
  - delegating powers need to be a "service" of this provider

---

<sup>6</sup> In SEMPER the EU could be modelled as a separate entity governing EU-institutions that provide services (methodically more correct). As eIDAS has already tackled this issue with the "EU" country code, the SEMPER model has not been extended with a separate entity.



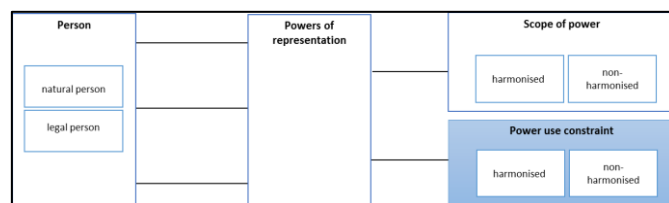
Each method of expressing the scope of the PoR has its own characteristics:

- a non-harmonised scope requires an exchange of service information for cross-border usage and additional measures may be needed to clarify the service of a service provider in one member state to persons in another member state (for example adding translated service-names);
- a harmonised scope does not require this exchange of service information as the scope will be selected from a sources of standardisation, for example SDGR or any other source of standardised services that is accepted by the member states.

The principles of the scope of power are explained with several examples in Annex III.

#### 4.6. Power use constraint

Representatives may perform the activities as defined by the scope of power. PUCs specify the limits in the extent to which these activities may be performed. This semantic model adheres to the following principles regarding the power use constraint:



principles regarding the power use constraint:

1. A Power of Representation can be restricted by one or more power use constraints (optional).
2. The constraints (aspect, value) are provided to the service provider. Example: The Power of representation for a service is restricted to the <financial limit> of <1M euro>. The service provider can use this information to make an informed access decision.
3. Harmonised constraints are unambiguously defined across the EU. Service providers and mandate management systems are encouraged to acknowledge these constraints. Service providers should be able to enforce and mandate management systems should be able to register these harmonised constraints. The availability of harmonised constraints will correlate to the existence of harmonised services. Proper harmonisation requires the definition of harmonised constraints as well.
4. Non-harmonised constraints should be provided to the service provider as well if no equivalent harmonized constraints are available. As a consequence of non-standardisation the service provider may require closer examination of the constraint or deny access directly. The service provider relies on explanation from the mandate management system for proper interpretation of non-harmonised constraints.
5. Both harmonised and non-harmonised constraints are in scope of the model.
6. The harmonisation of constraints ('the content') is out of scope of the SEMPER project.

## 5. Mandate attributes

This chapter specifies the logical request, the rules for processing the request by the validating member state, and the logical response. This specification is based on the premise that validation of representation is requested. In case no SEMPER representation is requested, the current eIDAS specifications (version 1.1) apply. Attributes in this model can, therefore, be defined as mandatory for powers validation, whereas they are not mandatory in the current eIDAS specifications.

### 5.1. Overview

The SEMPER model adds several mandate attributes to eIDAS. The next sections will elaborate on these mandate attributes. (m) = mandatory attribute, (o) = optional attribute.

- person
  - a) person types allowed (m)
- requested powers of representation
  - a) sources of power allowed (m)
  - b) regulated professions allowed (o)
- powers of representation
  - a) validation result (m)
  - b) source of power (o)
  - c) regulated profession (o)
- scope
  - a) full powers (m)
  - b) service catalogue (o)
  - c) harmonised service (o)
  - d) member state (o)
  - e) service provider (o)
  - f) service (o)
  - g) procedure (o)
  - h) type of procedure (o)
- power use constraints
  - a) constraint (o)
  - b) value (o)

### 5.2. Request

A relying party can request another member state to validate a power of representation and provide the identities of the persons involved. To do so effectively, the requesting member state needs to provide the information specified in this section.

#### **Relying party**

The relying party is the organisation requesting a SEMPER powers validation via the eIDAS network. The relying party usually is the service provider at which representative wants to access a service. The relying party will be a 'proxy organisation' in case another organisation initiates and processes the information flow under the responsibility of the service provider. Note that the member state's ISO code can be read from the eIDAS metadata file.

<i>element</i>	<i>cardinality</i>	<i>optionality</i>	<i>values allowed</i>	<i>definition</i>
<b>relying party</b>	1	M		
member state	1	M	ISO 3166 alpha-2 country code, EU	The ISO country code of the member state the service provider resides in.
relying party	1	O		The formal name of the organisation issuing the powers validation request and processes the response. Usually the service provider.

### Represented person

The specification of the information required of the person on whose behalf the service is to be used. The service provider can declare which type of persons are accepted, which eIDAS attributes are required (mandatory) and which are requested (optional).

<i>element</i>	<i>cardinality</i>	<i>optionality</i>	<i>values allowed</i>	<i>definition</i>
<b>represented</b>	1	M		
person types allowed	1	M	NP, LP, both	Specifies the person type(s) the service provider accepts.
requested NP attributes	N	O		List of requested attributes of a natural person.
eIDAS NP attribute is required	1	M	Yes, No	Indication whether the attribute is optional or mandatory.
requested LP attributes	N	O		List of requested attributes of a legal person.
eIDAS LP attribute is required	1	M	Yes, No	Indication whether the attribute is optional or mandatory.

Integrity rules:

- in case **person types allowed** = NP, then only NP attributes must be requested
- in case **person types allowed** = LP, then only LP attributes must be requested
- in case **person types allowed** = both, then both NP and LP attributes must be requested

### Representative

The specification of the information required of the person who wants to access the service. The service provider can declare which type of persons are accepted, which eIDAS attributes are required (mandatory) and which are requested (optional).

<i>element</i>	<i>cardinality</i>	<i>optionality</i>	<i>values allowed</i>	<i>definition</i>
<b>representative</b>	1	M		
person types allowed	1	M	NP, LP, both	Specifies the person type(s) the service provider accepts.
requested NP attributes	N	O		List of requested attributes of a natural person.
eIDAS NP attribute is required	1	M		cf eIDAS
	1	M	Yes, No	Indication whether the attribute is optional or mandatory.
requested LP attributes	N	O		List of requested attributes of a legal person.
eIDAS LP attribute is required	1	M		cf eIDAS
	1	M	Yes, No	Indication whether the attribute is optional or mandatory.

Integrity rules:

- in case **person types allowed** = NP, then only NP attributes must be requested
- in case **person types allowed** = LP, then only LP attributes must be requested
- in case **person types allowed** = both, then both NP and LP attributes must be requested

### Intermediary

The specification of the information required of other actors involved in the representation. The intermediary can, for example, be an accounting firm representing a client. Represented person and representative cannot be intermediary actors at the same time. The service provider may request information on the intermediary actor(s), but the service provider is in no scenario obliged to do this. All attributes of the intermediary should be requested as optional attributes as there may not be an intermediary person involved.

The service provider can declare which type of persons are accepted and which eIDAS attributes are requested (optional attributes). The request for attributes applies to all intermediaries provided (in case the validating member states provides information on more than one intermediary). In SEMPER, we have not encountered a use case which requires requesting a specified number of intermediaries and requesting combinations of allowed person types, e.g. requesting two legal person intermediaries and one natural person intermediary.

<i>element</i>	<i>cardinality</i>	<i>optionality</i>	<i>values allowed</i>	<i>definition</i>
<b>intermediary</b>	1	O		
person types allowed	1	M	NP, LP, both	Specifies the person type(s) the service provider accepts.
requested NP attributes	N	O		List of requested attributes of a natural person.
eIDAS NP attribute is required	1	M		cf eIDAS
	1	M	No	intermediary attributes must be optional
requested LP attributes	N	O		List of requested attributes of a legal person.
eIDAS LP attribute is required	1	M		cf eIDAS
	1	M	No	intermediary attributes must be optional

Integrity rules:

- in case **person types allowed** = NP, then only NP attributes must be requested
- in case **person types allowed** = LP, then only LP attributes must be requested

- in case **person types allowed** = both, then both NP and LP attributes must be requested
- **Intermediary** may only be specified in case the **source of power allowed** (within **power of representation**) includes at least one of: mandate, legislation or court ruling.

### Powers of representation

The service provider can declare what sources of power it allows and to what regulated professions it will grant access.

<i>element</i>	<i>cardinality</i>	<i>optionality</i>	<i>values allowed</i>	<i>definition</i>
<b>Powers of representation</b>	1	M		
sources of power allowed	N	M	all, mandate, legislation, court ruling, regulated profession	The sources of mandates that the service provider accepts. Values include "all": the SP accepts all power sources.
regulated professions allowed	N	O	values from REGPROF-table	The regulated profession a person needs to have to get access to the service.

Integrity rules:

- In case **sources of power allowed** = all, no other occurrences of this item may be specified.
- In case **sources of power allowed** contains "regulated profession" or "all", **regulated professions allowed** may be specified, otherwise **regulated professions allowed** may not be specified.

### Scope

This element specifies the scope for which access is requested and for which the power has to be validated. In case the service provider requests a validation of a regulated profession only, it must not specify the scope. In contrast to the other sources of power, the powers of a regulated professional will be defined by the service provider itself. The validating member state only declares the person is a regulated professional. Scope is not applicable in this case.

In case the service provider accepts power sources other than regulated professions, it has to specify the scope as:

1. full powers. This option will be used when requesting to validate powers to apply for any service. In this case, the Service provider does not specify a harmonised or non-harmonised service.
2. the harmonised scope. The identification of the service catalogue of harmonised services and the exact name of the service as registered in this catalogue should be provided.
3. the non-harmonised scope. In order to establish the identity of the service provider the member state's ISO code is mandatory. The naming of the elements (like service provider and service) should be done in such a way that they can be recognised uniquely by their names. Names should be persistent as well. Note that in case the requesting member state does not provide unique and persistent names, the chance of successful powers validation will be reduced.

This version of the model supports only one instance of scope in the validation of powers request. In future versions the option to allow multiple instances could be added. This would assist portals that grant access to multiple services and want to present only the services the person has the powers for. In this case, the response should include the scope as well to express the scope(s) for which the powers has/have been validated successfully.

<i>element</i>	<i>cardinality</i>	<i>optionality</i>	<i>values allowed</i>	<i>definition</i>
<b>scope</b>	1	O		
full powers	1	M	Yes, No	In case "Yes" the requested powers are unlimited. In case "No" the requested powers are limited.
<b>harmonised scope</b>	1	O		
service catalogue	1	M		The identification of the catalogue the harmonised service is part of.
harmonised service	1	M		The unique name of the harmonised service requested access to.
<b>non-harmonised scope</b>	1	O		
member state	1	M	ISO 3166 alpha-2 country code, EU	The ISO country code of the member state that delivers the service(s) requested access to.
service provider	1	O		The formal name of the service provider, unique in the context of the member state.
service	1	O		The name of the service requested access to, unique in the context of the service provider.
procedure	1	O		The name of the procedure of the service requested access to, unique in the context of the service provider.
type of procedure	1	O		The type of procedure requested access to.

#### Integrity rules:

- **scope** must be provided in case **power of representation.source of power allowed** include at least one other value than "regulated profession".
- In case **full powers** = Yes, no harmonised and no non-harmonised scope may be specified.
- In case **full powers** = No, a harmonised or non-harmonised scope must be specified.
- **harmonised scope** and **non-harmonised scope** may not be specified both in one request.
- in case a **non-harmonised scope** has been specified, at least one of the following has to be specified: [**member state** and **service provider**], [**member state** and **type of procedure**].
- in case **member state** and **service provider** have been specified, **service** and **procedure** may be specified as well.

### 5.3. Request processing rules

The validating member state receives and processes the request. While processing the request, the member state needs to take the following rules into consideration:

- by nature, regulated professions are related to the representative and not the represented person. E.g., the representative is a notary or lawyer. In theory, information could be provided about the professional without providing information on the represented person. Within the SEMPER baseline scenario the represented person will in all cases be identified. So even in case the service provider requests a validation of a

regulated profession only ([sources of power allowed](#) = regulated profession only), the validating member state will provide information on the represented person.

- in validation of the powers (are powers sufficient for requested scope?), the laws, regulation, principles, etc. of the validating member state will be applied.

Source of power allowed	Scope is specified	Processing rule
Regulated profession	N	Representative should have a valid registration in an official source of professionals for one or more of the specified regulated professions.
	Y	Not applicable (scope must not be specified).
One or more other than regulated profession	N	Not applicable (scope must be specified).
	Y	Powers of representative should be valid for at least the specified scope.
Regulated profession and other	Y	Representative should have a valid registration in an official source of professionals for one or more of the specified regulated professions and/or powers of representative should be valid for at least the specified scope
	N	Not applicable (scope must be specified).

#### 5.4. Response

The validating member state will process the request and provide an appropriate response. The response mainly contains the requested attributes of the representative, represented person, (optional) the intermediary, as well as the result of the powers validation. The latter will be expressed in one validation result for all validated powers. The service provider authorises the representative based on this “ok/not-ok” result as well as additional information received in the response.

The response message contains the reference (messageID) to the request so that the request and response can easily be related afterward and a full audit trail can be constructed. The validating member state is responsible for logging the validation process in such a way that it is indisputably linked to the request/response.

Note that in case of an error – independent of the specified optionality column - only the error element will be provided.

#### Represented person

The response contains the type of represented person, the requested mandatory attributes, and requested optional attributes if available, so that the service provider can establish the identity of the represented person. The represented person can be either a natural person or a legal person, but not both at once. Consequently, the response may only contain attributes of one.

<i>element</i>	<i>cardinality</i>	<i>optionality</i>	<i>values allowed</i>	<i>definition</i>
<b>represented</b>	1	M		
person type	1	M	NP, LP	The person is either a natural person or a legal person.
eIDAS NP attribute	N	O		cf eIDAS
eIDAS LP attribute	N	O		cf eIDAS

## Integrity rules:

- The response may contain requested/required attributes only
- in case **person type** = NP, only NP attributes must be provided
- in case **person type** = LP, only LP attributes must be provided

**Representative**

The response contains the type of person of the representative, the requested mandatory attributes, and requested optional attributes if available, so that the service provider can establish the identity of the representative.

<i>element</i>	<i>cardinality</i>	<i>optionality</i>	<i>values allowed</i>	<i>definition</i>
<b>representative</b>	1	M		
person type	1	M	NP, LP	The person is either a natural person or a legal person.
eIDAS NP attribute	N	O		cf eIDAS
eIDAS LP attribute	N	O		cf eIDAS

## Integrity rules:

- The response may contain requested/required attributes only
- in case **person type** = NP, only NP attributes must be provided
- in case **person type** = LP, only LP attributes must be provided

**Intermediary**

The response may contain (if explicitly requested) information on one or more intermediaries: the type of the person and requested attributes. The validating member state can always decide to provide no information about the intermediary in case there is none, or in case there is no information on the intermediary available.

<i>element</i>	<i>cardinality</i>	<i>optionality</i>	<i>values allowed</i>	<i>definition</i>
<b>intermediary</b>	N	O		
person type	1	M	NP, LP	The person is either a natural person or a legal person.
eIDAS NP attribute	N	O		cf eIDAS
eIDAS LP attribute	N	O		cf eIDAS

## Integrity rules:

- the validating member state may provide information on the **intermediary** if requested
- the response may contain requested attributes only
- in case **person type** = NP, only NP attributes must be provided
- in case **person type** = LP, only LP attributes must be provided
- the validating member state is not obliged to provide information on the **intermediary** person(s)
- The **intermediary** person must not be included as **represented person** or **representative** in the response as well.

**Powers of representation**

This element contains attributes of the resolved powers which are relevant for the service provider for the decision to grant or deny access to the service. It consists mainly of three sections:

1. Validation result: conclusion on the validation of powers. Have the powers been validated successfully or not? If, for any reason, the validating member state has chosen not to validate the powers, the validation result will be 'not validated'.



2. Powers specification: optionally, one or more specifications of the validated powers. In case the providing member state validated the powers successfully but cannot or does not want to disclose the sources, it does not provide a mandate specification. In case one or more regulated professions have been validated, the member state may specify which profession(s) has been/have been validated successfully.
3. Power use constraints: optionally, one or more power use constraints.

As a design philosophy, as well as for reasons of privacy and data-minimalization, the response only contains information regarding the validation result: ok or not ok. The response does not contain details of the mandate *as registered in the mandate management system* (e.g. that the person has full powers when validation on a single service has been requested), other persons the representative has representational powers for, the registry that the mandate is in, the organisation validating the mandate, etc. As with eIDAS, the relying member state will trust the validation of the validating member state.

Multiple power specifications may be included. The sources of power specified had a role in validating the powers. The total of these powers led to a positive validation result. The response does not elaborate on the weight of an individual power source in the powers validation process. E.g. when two sources are included, the response does not state which of the following applies:

- both individually lead to a positive validation result (two sources confirming the same powers);
- the two sources lead to a positive validation result in combination of the two only (each source confirming the powers partly).

Furthermore, the powers specification does not specify the intermediary the power source applies to (in case of intermediaries are included).

The validation result applies to the scope as specified in the request. This scope will not be copied into the response. In case – in a next version of this model – specifying multiple scopes will be allowed, including the positively validated scopes in the response is necessary.

<i>element</i>	<i>cardinality</i>	<i>optionality</i>	<i>values allowed</i>	<i>definition</i>
<b>Powers of representation</b>	1	M		
validation result	1	M	ok, not ok, not validated	The conclusion of the effort to confirm someone's powers to represent another person. - ok: the person has the powers to represent - not ok: the person does not have the powers to represent - not validated: no validation of the powers has been performed
<b>powers specification</b>	N	O		
source of power	1	M	mandate, legislation, court ruling, regulated profession	The type of the power of representation.
regulated profession	1	O	not specified, REGPROF table	The person's profession(s). In case the providing member state successfully validated one or more professions but does not want to disclose the profession(s), it responds with the value "not specified".
<b>power use constraint</b>	N	O		
constraint	1	M		The aspect of restriction on the use of the mandate
value	1	M		The specification of the constraint

## Integrity rules:

- in case the power source [regulated professions](#) is not allowed in the request, [regulated profession](#) must not be included in the response.
- In case only the power source [regulated professions](#) is allowed in the request, [power use constraint](#) must not be included in the response.
- [power use constraints](#) may be provided only in case [validation result](#) = ok.
- a [power specification](#) must not contain a [source of power](#) that is not included in [sources of power allowed](#) in the request.
- not more than one [power specification](#) for each [source of power](#) may be provided.

**Error**

In case of an error in the request message or while validating the response, the validating member state will respond with an appropriate error message. Error messages can have a technical nature (e.g. request message is incorrect, time-out, mandate management system offline) as well as a logical nature:

1. required attribute(s) not available
2. process cancelled by user

<i>element</i>	<i>cardinality</i>	<i>optionality</i>	<i>values allowed</i>	<i>definition</i>
<b>error</b>	1	O		
error code	1	M		Error code to clarify the reason why something went wrong in validating the powers.

## Integrity rules:

- in case an [error](#) is returned, the other elements will not be provided.

5.5. [Response processing rules](#)

The relying member state receives and processes the response. While processing the response, the member state needs to take the following rules with regard to the [validation result](#) into consideration:

- not validated: validation has not been performed and access to the service cannot be granted.
- not ok: powers are not sufficient and access to the service cannot be granted.
- ok: at least one of the allowed sources of power has been validated, powers are sufficient and access to the service may be granted.

In case of an “ok”, the validating member state may provide additional information about the validated power(s), this information can be used by the relying service provider in the decision to grant access:

Request: Source of power allowed	Response: Powers specification	Processing rule
Regulated profession	<ul style="list-style-type: none"> <li>- No power specification is provided</li> <li>- 1 power specification is provided and               <ul style="list-style-type: none"> <li>o a regulated profession is not provided</li> <li>o one or more regulated professions are provided.</li> </ul> </li> </ul>	<p>When (one of the) the validated profession is provided, then the service provider knows which professions are validated. The service provider cannot make any assumptions about the professions that are allowed but not provided in the response.</p> <p>When the validated profession(s) are not provided, then:</p> <ul style="list-style-type: none"> <li>- if only one regulated profession is allowed then the service provider can conclude that that allowed profession was validated;</li> <li>- if more than one regulated profession are allowed then the service provider cannot conclude which profession(s) are validated.</li> </ul>
One of Mandate, Legislation, Court ruling	<ul style="list-style-type: none"> <li>- No power specification is provided</li> <li>- 1 power specification is provided with one source of power</li> </ul>	<ul style="list-style-type: none"> <li>- If no power specification is provided, the validating member state cannot or does not want to specify the source of power, however since only one source of power is allowed this must be the source the validation is based upon.</li> <li>- If one source of power is provided, then this specifies the source the power originates from.</li> <li>- If intermediaries are involved, the full chain of powers consists of powers originating from the specified source of power.</li> </ul>
Two or more of Mandate, Legislation, Court ruling	<ul style="list-style-type: none"> <li>- No power specification is provided</li> <li>- 1 power specification is provided with one source of power</li> <li>- More power specifications are provided, each with one source of power</li> </ul>	<ul style="list-style-type: none"> <li>- If no power specification is provided, the validating member state cannot or does not want to specify the source, since two or more sources are allowed the service provider cannot determine from which source the power originates.</li> <li>- If one power specification is provided, then this specifies the source the power originates from.</li> <li>- If more than one power specifications are provided, then the power originates from each of these sources.</li> <li>- If intermediaries are involved, the powers in the chain of power originates from the provided sources of power.</li> <li>- The service provider cannot derive any conclusions about source(s) of power that are allowed but not provided in the response.</li> </ul>
Regulated profession and other(s)	<ul style="list-style-type: none"> <li>- No power specification is provided</li> <li>- 1 power specification is provided</li> <li>- More power specifications are provided</li> <li>- A regulated profession is not provided</li> <li>- One or more regulated professions are provided</li> </ul>	<ul style="list-style-type: none"> <li>- If no power specification is provided, the validating member state cannot or does not want to specify the source or profession, since one or more sources and regulated professions are allowed the service provider cannot determine from which source or regulated profession the power originates.</li> <li>- If one power specification is provided, then this specifies the regulated profession or source the power originates from.</li> <li>- If more than one power specifications are provided, then the power originates from each of these sources and/or regulated professions.</li> <li>- If intermediaries are involved, the powers in the chain of power originates from the provided sources of power.</li> <li>- The service provider cannot derive any conclusions about source(s) of power or regulated professions that are allowed but not provided in the response.</li> </ul>

## 6. eIDAS SAML extension







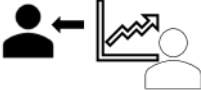







### 6.1. Design principles

Chapter 2.8 of the eIDAS SAML Attribute Profile specification (v1.1) defines the structure for the information flow in the case of representation. According to the current version of the specification, an additional person data set that indicates a natural or a legal person representative has to be included to express representation in the MDS. For representation cases, the Sending MS returns two sets of MDS attributes: namely the requested attributes for the *represented* natural or legal person, AND the attributes of the *representative* natural or legal person, prefixed with “Representative”.

standard eIDAS attributes		representative eIDAS attributes	
natural person	legal person	natural person	legal person

This structure is somewhat limiting for the implementation of the SEMPER semantic model. It allows attributes of a maximum of three persons: (i) the *represented* (natural or legal) person, (ii) a natural person *representative*, and (iii) a legal person *representative*. Consequently, within these boundaries, only one intermediary person can be included in the response. This intermediary person needs to be a legal person. The attributes of the legal person intermediary will be included as legal person attributes of the representative in eIDAS. Natural person intermediaries are not supported within the eIDAS specification.

SEMPER supports the following representation scenarios based on the authentication with a natural person eID:

	standard eIDAS attributes		representative eIDAS attributes	
	natural person	legal person	natural person	legal person
natural person representing another natural person 	represented natural person attributes 		representative natural person attributes 	
natural person representing a legal person 		represented legal person attributes 	representative natural person attributes 	
natural person acting on behalf of a legal person representing a natural person 	represented natural person attributes 		representative natural person attributes 	intermediary legal person attributes 
natural person acting on behalf of a legal person representing a legal person 		represented legal person attributes 	representative natural person attributes 	intermediary legal person attributes 

In order to accommodate the concepts of the SEMPER semantic model, such as the scope and restrictions of representation, as well as the representation scenarios that SEMPER supports, we propose to extend the specification as described in the following sections.

We begin by identifying the main parts of the eIDAS specification that need to be extended for our purpose and continue to specify the exact components of the underlying SAML protocol used for communication and error handling that allow for such an extension.

## 6.2. SAML Extensibility

SAML supports extensibility in several ways, including extending the assertion and protocol schemas. This allows for the definition of new profiles, which can be combined with extensions to put the SAML framework to new uses. The SAML schemas use wildcard constructs in some locations to allow the use of elements and attributes from arbitrary namespaces, which serves as a built-in extension point without requiring an extension schema.

The constructs that are of particular interest to both the eIDAS and the SEMPER SAML extensions are:

- i. the `<Extensions>` and `ExtensionsType` elements of the SAML AuthnRequest schema, which allows elements from other namespaces with lax schema validation processing,
- ii. the `<Attribute>`, and `AttributeType` elements of the Assertion Schema, which allow arbitrary global attributes
- iii. the `<AttributeValue>` of the Assertion Schema, which uses `xs:anyType` and allows any sub-elements and attributes.

In particular, the `<Extensions>` element is used to send optional protocol message extension elements that are agreed on between the communicating parties. No extension schema is required in order to make use of this extension point, and even if one is provided, the lax validation setting does not impose a requirement for the extension to be valid. The schema for the `<Extensions>` element of the SAML protocol is as follows:

```
<element name="Extensions" type="samlp:ExtensionsType"/>
<complexType name="ExtensionsType">
  <sequence>
    <any namespace="##other" processContents="Lax" maxOccurs="unbounded"/>
  </sequence>
</complexType>
```

### 6.2.1. Current eIDAS SAML extension

The current schema for the eIDAS SAML extension, makes use of the `<Extensions>` element mentioned above to request attributes via the `<eidas:RequestedAttributes>` element under `<saml2p:Extensions>`. According to the current specification, mandatory attributes need to be requested with `isRequired="true"`, while optional attributes are requested with `isRequired="false"`. Moreover, each `<saml2p:AuthnRequest>` needs to request all attributes defined as mandatory within the minimum dataset (MDS).

The current schema for the eIDAS SAML extension is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns=http://eidas.europa.eu/saml-extensions
  xmlns:xsd=http://www.w3.org/2001/XMLSchema
  targetNamespace=http://eidas.europa.eu/saml-extensions
  elementFormDefault="qualified" attributeFormDefault="unqualified"
  xmlns:eidas=http://eidas.europa.eu/saml-extensions version="1">
  <xsd:element name="SPTYPE" type="SPTYPE" />
  <xsd:simpleType name="SPTYPE">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="public" />
      <xsd:enumeration value="private" />
    </xsd:restriction>
  </xsd:simpleType>
  <xsd:element name="RequestedAttributes" type="eidas:RequestedAttributesType"/>
  <xsd:complexType name="RequestedAttributesType">
    <xsd:sequence>
      <xsd:element minOccurs="0" maxOccurs="unbounded"
        ref="eidas:RequestedAttribute" />
    </xsd:sequence>
  </xsd:complexType>
  <xsd:element name="RequestedAttribute" type="eidas:RequestedAttributeType"/>
  <xsd:complexType name="RequestedAttributeType">
    <xsd:sequence>
      <xsd:element minOccurs="0" maxOccurs="unbounded"
        ref="eidas:AttributeValue" />
    </xsd:sequence>
    <xsd:attribute name="Name" use="required" type="xsd:string"/>
    <xsd:attribute name="NameFormat" use="required" type="xsd:anyURI" />
    <xsd:attribute name="FriendlyName" use="optional" type="xsd:string" />
    <xsd:attribute name="isRequired" use="optional" type="xsd:boolean" />
    <xsd:anyAttribute namespace="##other" processContents="Lax" />
  </xsd:complexType>
  <xsd:element name="AttributeValue" type="xsd:anyType" />
</xsd:schema>
```

In the following subsections, we consider each element of the information flow (request/response) described in Chapter 5 (Mandate Attributes) and propose a mapping between the logical SEMPER request/response model to the SAML Protocol Request and Response elements.

### 6.3. Extending the eIDAS SAML Authentication Request

This section goes into the details of the extension elements added to the eIDAS SAML Authentication Request in order to accommodate representation-specific requested attributes. Firstly, a `<por:RepresentationRequirements>` element is added to the `<Extensions>` element of the `AuthnRequest`. The Service Provider uses the element to specify its requirements related to the represented and representative person types, the different representation profiles (scenarios), as well as the source and scope of the representation. In addition to declaring the values considered as acceptable by the SP for these criteria, additional attributes may be included in the request if the SP requests to know the actual value of a specific requirement attribute amongst the options that it allows. The SP may optionally include the Relying Party issuing the request, and explicitly request MDS attributes for the representative and intermediary persons.

#### 6.3.1. Powers of Representation Requirements

The service provider can declare in the Request its requirements regarding power of representation, such as what sources of mandates it allows and to what regulated professions it will grant access. For this purpose, we define a new Power of Representation

(<por:RepresentationRequirements>) element under <saml2p:Extensions>. The main sub-elements include:

- a. The allowed representation profile(s) or scenarios: NP-NP, NP-LP, LP-NP, or LP-LP
- b. The allowed sources of mandates: Wilful Act, Legislation, Court Ruling, and Regulated Profession, or all
- c. The allowed regulated profession type, only in the case that the source of the mandate is a regulated profession, with values taken by the harmonized Regulated Professions Table.
- d. The specified representation scope: full powers, harmonized or non-harmonized.

A high-level schema for this element is provided below:

```
<xsd:element name="RepresentationRequirements"
  type="por:RepresentationRequirementsType"/>
<xsd:complexType name="RepresentationRequirementsType">
  <sequence>
    <element ref="por:AllowedRepresentationProfiles" minOccurs="1" />
    <element ref="por:AllowedPoRSources" minOccurs="1" />
    <element ref="por:AllowedRegulatedProfessions" minOccurs="0" />
    <element ref="por:PoRScope" minOccurs="0" />
  </sequence>
</complexType>
```

According to the SEMPER information flow model, the SP must include its requirements regarding the the representation profiles and the sources of representation in the request. The values allowed for Regulated Profession may be optionally included in the request with the condition that Regulated Profession is specified in the allowed sources of representation element. The scope of representation must be specified in case the SP allows for sources of representation other than Regulated Profession. The scope can be specified in the request as either 'full powers', for representation not restricted to an SP or an MS, or one of the 'harmonized' or 'non-harmonized' options.

The values allowed for these subcomponents can be defined in the request schema as follows:

a. Allowed Representation Profiles:

```
<xsd:element name="AllowedRepresentationProfiles"
  type="AllowedRepresentationProfilesType" />
<xsd:complexType name="AllowedRepresentationProfilesType">
  <xsd:sequence>
    <xsd:element minOccurs="1" maxOccurs="4"
      ref="por:AllowedRepresentationProfile" />
  </xsd:sequence>
</xsd:complexType>
<xsd:element name="AllowedRepresentationProfile"
  type="AllowedRepresentationProfileType" />
<xsd:complexType name="AllowedRepresentationProfileType">
  <xsd:attribute name="representedType" use="required">
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
        <xsd:enumeration value="NaturalPerson" />
        <xsd:enumeration value="LegalPerson" />
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:attribute>
  <xsd:attribute name="representativeType" use="required">
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
        <xsd:enumeration value="NaturalPerson" />
        <xsd:enumeration value="LegalPerson" />
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:attribute>
  <xsd:attribute name="intermediariesAllowed" use="optional" type="xsd:boolean"/>
  <xsd:attribute name="intermediariesType" use="optional">
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
        <xsd:enumeration value="NaturalPerson" />
        <xsd:enumeration value="LegalPerson" />
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:attribute>
</xsd:complexType>
```

b. Allowed Sources of Representation:

```
<xsd:element name="AllowedPoRSources" type="AllowedPoRSourcesType" />
<xsd:complexType name="AllowedPoRSourcesType">
  <xsd:sequence>
    <xsd:element minOccurs="0" maxOccurs="unbounded"
      ref="por:AllowedPoRSource" />
  </xsd:sequence>
</xsd:complexType>
<xsd:element name="AllowedPoRSource" type="AllowedPoRSourceType" />
<xsd:simpleType name="AllowedPoRSourceType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="WilfulAct" />
    <xsd:enumeration value="Legislation" />
    <xsd:enumeration value="CourtRuling" />
    <xsd:enumeration value="RegulatedProfession" />
  </xsd:restriction>
</xsd:simpleType>
```



## c. Allowed Regulated Professions:

```

<xsd:element name="AllowedRegulatedProfessions"
  type="por:AllowedRegulatedProfessionsType" />
<xsd:complexType name="AllowedRegulatedProfessionsType">
  <xsd:sequence>
    <xsd:element minOccurs="1" maxOccurs="unbounded"
      ref="por:AllowedRegulatedProfession" />
  </xsd:sequence>
</xsd:complexType>
<xsd:element name="AllowedRegulatedProfession"
  type="AllowedRegulatedProfessionType" />
<xsd:simpleType name="AllowedRegulatedProfessionType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Notary" />
    <xsd:enumeration value="Lawyer" />
    <!--other values from REG-PROF table-->
  </xsd:restriction>
</xsd:simpleType>

```

## d. Power of Representation Scope(s):

```

<xsd:element name="PoRScope" type="PoRScopeType" />
<xsd:complexType name="PoRScopeType">
  <xsd:sequence>
    <xsd:element minOccurs="0" ref="por:HarmonizedPoRScope" />
    <xsd:element minOccurs="0" ref="por:NonHarmonizedPoRScope" />
  </xsd:sequence>
  <xsd:attribute name="fullPowers" use="required" type="xsd:boolean" />
</xsd:complexType>
<xsd:element name="HarmonizedPoRScope" type="HarmonizedPoRScopeType" />
<xsd:complexType name="HarmonizedPoRScopeType">
  <xsd:sequence>
    <xsd:element name="HarmonizedCatalogName"
      minOccurs="1" type="xsd:string" />
    <xsd:element name="HarmonizedServiceName"
      minOccurs="1" type="xsd:string" />
  </xsd:sequence>
</xsd:complexType>
<xsd:element name="NonHarmonizedPoRScope" type="NonHarmonizedPoRScopeType" />
<xsd:complexType name="NonHarmonizedPoRScopeType">
  <xsd:sequence>
    <xsd:element name="ServiceProviderMS" minOccurs="1" type="xsd:string"/>
    <xsd:element name="ServiceProvider" minOccurs="0" type="xsd:string"/>
    <xsd:element name="NonHarmonizedServiceName" minOccurs="0" type="xsd:string"/>
    <xsd:element name="Procedure" minOccurs="0" type="xsd:string"/>
    <xsd:element name="ProcedureType" minOccurs="0" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>

```

### 6.3.2. Represented

The Represented person is authenticated via the standard eIDAS authentication flow. The attributes of the Represented are requested as per usual via the `<eidas:RequestedAttributes>` element under `<saml2p:Extensions>`:

```

<saml2p:Extensions>
...
  <eidas:RequestedAttributes>
    <eidas:RequestedAttribute
      Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      isRequired="true"/>
    <eidas:RequestedAttribute
      Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      isRequired="true"/>
    <eidas:RequestedAttribute
      Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      isRequired="true"/>
    <eidas:RequestedAttribute
      Name="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      isRequired="true"/>
  </eidas:RequestedAttributes>
...
</saml2p:Extensions>

```

### 6.3.3. Representative

The information flow in SEMPER is based on the principle that representation validation information may be explicitly requested. In order to distinguish between the attributes that are required for the represented person and those required for representative attributes, we propose to add the “Representative” prefix to the attributes’ friendly name and to amend the SAML attribute name by “representative”. This approach was already specified in the eIDAS SAML Attribute Profile document for the MDS of attributes returned in the response in the case of representation. This prefix now is being added to the requested attributes of the representative in the `<AuthnRequest>` element as well. The name prefixes thus become <http://eidas.europa.eu/attributes/naturalperson/representative/> or <http://eidas.europa.eu/attributes/legalperson/representative/>.

We list the requested Representative attributes under the `<eidas:Requested Attributes>` element, and use the already existing “isRequired” element to indicate whether an attribute is requested as mandatory or not for representation validation.

Following this approach, the requested representative attributes would take place in the request as follows:

```

<saml2p:Extensions>
...
<eidas:RequestedAttributes>
  <eidas:RequestedAttribute

    Name="http://eidas.europa.eu/attributes/naturalperson/representative/PersonId
    entifier"
    FriendlyName="RepresentativePersonIdentifier"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    isRequired="true" />
  <eidas:RequestedAttribute

    Name="http://eidas.europa.eu/attributes/naturalperson/representative/CurrentF
    amilyName"
    FriendlyName="RepresentativeCurrentFamilyName"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    isRequired="true" />
  <eidas:RequestedAttribute

    Name="http://eidas.europa.eu/attributes/naturalperson/representative/CurrentG
    ivenName"
    FriendlyName="RepresentativeCurrentGivenName"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    isRequired="true" />
  <eidas:RequestedAttribute

    Name="http://eidas.europa.eu/attributes/naturalperson/representative/DateOfBi
    rth"
    FriendlyName="RepresentativeDateOfBirth"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    isRequired="true" />
</eidas:RequestedAttributes>
...
</saml2p:Extensions>

```

#### 6.3.4. Intermediary

Similar to attributes requested for the representative person, attributes can be requested for at most one intermediary, with the constraint of this intermediary being a legal person. This can already be requested using the same “representative” prefix approach, with the implication that the usage of this prefix with legal person attributes infers the presence of an intermediary. Note that given that information requested on the intermediary should be considered as optional, the value of the “isRequired” element should be set to false.

```

<saml2p:Extensions>
...
<eidas:RequestedAttributes>
  <eidas:RequestedAttribute

    Name="http://eidas.europa.eu/attributes/Legalperson/representative/LegalPers
    onIdentifier"
    FriendlyName="RepresentativeLegalPersonIdentifier"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    isRequired="false" />

  <eidas:RequestedAttribute

    Name="http://eidas.europa.eu/attributes/Legalperson/representative/LegalName
    "
    FriendlyName="RepresentativeLegalName"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    isRequired="false" />
...
</eidas:RequestedAttributes>

```

```
...
</saml2p:Extensions>
```

### 6.3.5. Additional Representation Attributes

Besides declaring the possible values for the representation source or the regulated professions that it allows via the `<por:RepresentationRequirements>` element, the SP may also request the exact values to be included in the response. In this case, these attributes must be explicitly requested in the request, such as:

```
<eidas:RequestedAttribute
  Name="http://eidas.europa.eu/attributes/Representation/Source"
  FriendlyName="RepresentationSource"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  isRequired="true" />

<eidas:RequestedAttribute
  Name="http://eidas.europa.eu/attributes/attributes/Representation/RegulatedPr
ofession"
  FriendlyName="RegulatedProfession"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  isRequired="false" />

...
```

Below we provide some examples of possible combinations of these requirements in the extended Authentication Request.

Example of a representation originating from a Wilful Act:

```
<saml2p:Extensions>
  ...
  <por:RepresentationRequirements
    xmlns="http://eidas.europa.eu/saml-semper-extensions">
    <por:AllowedRepresentationProfiles>
      <por:AllowedRepresentationProfile
        representativeType="NaturalPerson" representedType="NaturalPerson" />
      <por:AllowedRepresentationProfile
        representativeType="LegalPerson" representedType="LegalPerson" />
    </por:AllowedRepresentationProfiles>
    <por:AllowedPoRSources>
      <por:AllowedPoRSource>WilfulAct</por:AllowedPoRSource>
    ...
    </por:AllowedPoRSources>
  </por:RepresentationRequirements>
</saml2p:Extensions>
```

Example of a representation related to a regulated Profession:

```
<saml2p:Extensions>
  ...
  <por:RepresentationRequirements
    xmlns="http://eidas.europa.eu/saml-semper-extensions">
    ...
    <por:AllowedPoRSources>
      <por:AllowedPoRSource>RegulatedProfession</por:AllowedPoRSource>
    </por:AllowedPoRSources>
    <por:AllowedRegulatedProfessions>
      <por:AllowedRegulatedProfession>Notary</por:AllowedRegulatedProfession>
      <por:AllowedRegulatedProfession>Lawyer</por:AllowedRegulatedProfession>
    </por:AllowedRegulatedProfessions>
    ...
  </por:RepresentationRequirements>
</saml2p:Extensions>
```

### Example of a Harmonized Service Scope

```
<saml2p:Extensions>
  ...
  <por:RepresentationRequirements>
    <por:PoRScope fullPowers="false">
      <por:HarmonizedPoRScope>
        <por:HarmonizedCatalogName>semper</por:HarmonizedCatalogName>
        <por:HarmonizedServiceName>eDelivery</por:HarmonizedServiceName>
      </por:HarmonizedPoRScope>
    </por:PoRScope>
  ...
</por:RepresentationRequirements>
</saml2p:Extensions>
```

### Example of a Non-Harmonized Scope

```
<saml2p:Extensions>
  ...
  <por:RepresentationRequirements>
    <por:PoRScope fullPowers="false">
      <por:NonHarmonizedPoRScope>
        <por:ServiceProviderMS>AT</por:ServiceProviderMS>
        <por:ServiceProvider>ATPost</por:ServiceProvider>

        <por:NonHarmonizedServiceName>eDelivery</por:NonHarmonizedServiceName>
        <por:Procedure>readIncomingMail</por:Procedure>
      </por:NonHarmonizedPoRScope>
    </por:PoRScope>
  ...
</por:RepresentationRequirements>
</saml2p:Extensions>
```

## 6.4. Extending the eIDAS SAML Authentication Response

### 6.4.1. Powers of Representations, Status, Error Code

The status of the SAML response must be indicated using the `<saml2p:Status>` element providing at least one `<saml2p:StatusCode>`. Following this requirement, the power validation and authentication status is included in this element of the `<saml2p:AuthnResponse>` as follows:

```
<saml2p:Status>
  <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
</saml2p:Status>
```

The attributes of the represented, the representative and other attributes of the powers of representation validated, such as values for the source and regulated profession, and restrictions on the usage of the powers are added in the `<saml2:AttributeStatement>` element as additional attributes.



```
</saml2:Attribute>
```

#### 6.4.2. Represented

Represented attributes are returned as in the normal eIDAS authentication response, in the encrypted form of the SAML Assertion.

```
<saml2:AttributeStatement>
  <saml2:Attribute FriendlyName="PersonIdentifier"
    Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
    NameFormat="urn:oasis:names:tc:saml:2.0:attrname-format:uri">
    <saml2:AttributeValue xsi:type="eidas:PersonIdentifierType">
      ES/AT/02635542Y
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="FamilyName"
    Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
    NameFormat="urn:oasis:names:tc:saml:2.0:attrname-format:uri">
    <saml2:AttributeValue xsi:type="eidas:CurrentFamilyNameType">
      Onasis
    </saml2:AttributeValue>
    <saml2:AttributeValue LatinScript="false"
      xsi:type="eidas:CurrentFamilyNameType">
      Ωνάσης
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="FirstName"
    Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
    NameFormat="urn:oasis:names:tc:saml:2.0:attrname-format:uri">
    <saml2:AttributeValue xsi:type="eidas:CurrentGivenNameType">
      Sarah
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="DateOfBirth"
    Name="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"
    NameFormat="urn:oasis:names:tc:saml:2.0:attrname-format:uri">
    <saml2:AttributeValue xsi:type="eidas:DateOfBirthType">
      1970-05-28
    </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

### 6.4.3. Representative

Following the same approach as for the extended Authentication Request, we return an additional set of attributes in the Response for the Representative Person, with the Friendly Name of the respective attributes prefixed with "Representative".

```
<saml2:Attribute
  FriendlyName="RepresentativePersonIdentifier"
  Name="http://eidas.europa.eu/attributes/naturalperson/representative/PersonIdentifier"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:uri">
  <saml2:AttributeValue xsi:type="eidas:PersonIdentifierType">
    ES/AT/02635542Y
  </saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute
  FriendlyName="RepresentativeFamilyName"
  Name="http://eidas.europa.eu/attributes/naturalperson/representative/CurrentFamilyName"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:uri">
  <saml2:AttributeValue xsi:type="eidas:CurrentFamilyNameType">
    Chalk
  </saml2:AttributeValue>
</saml2:Attribute>
```

### 6.4.4. Intermediary

As in the request, we support attributes for at most one intermediary, that being a legal person.

```
<saml2:Attribute FriendlyName="RepresentativeLegalPersonIdentifier"
  Name="http://eidas.europa.eu/attributes/Legalperson/representative/LegalPersonIdentifier"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:uri">
  <saml2:AttributeValue xsi:type="eidas:LegalPersonIdentifierType">
    ES/AT/02735442Z
  </saml2:AttributeValue>
</saml2:Attribute>

<saml2:Attribute FriendlyName="RepresentativeLegalName"
  Name="http://eidas.europa.eu/attributes/Legalperson/representative/LegalName"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:uri">
  <saml2:AttributeValue xsi:type="eidas:LegalNameType">
    Acme Corporation
  </saml2:AttributeValue>
</saml2:Attribute>
```

## 6.5. Extending the eIDAS SAML Metadata Objects

Each eIDAS Connector and each eIDAS Service must provide metadata about the Connector/Service in the form of SAML Metadata that complies to SAML Metadata Interoperability Profile, and make it publicly available under a HTTPS URL. The eIDAS Connector can include in the SAML Authentication Request only attributes that were previously published in the eIDAS Service metadata file. Consequently, no change is required for eIDAS Connector SAML objects for the SEMPER extension. As for eIDAS Services Metadata Files, they must be extended with supported PoR-specific attributes by adding them as `<saml:Attribute>` elements in the `<md:IDPSSODescriptor>` element. Examples of such attributes added to the extended Metadata Files are given below.



## Extended metadata file example: representative, intermediary

```

<saml2:Attribute
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  FriendlyName="RepresentativeLegalName"
  Name="http://eidas.europa.eu/attributes/Legalperson/representative/LegalName"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />

<saml2:Attribute
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  FriendlyName="RepresentativeLegalPersonIdentifier"
  Name="http://eidas.europa.eu/attributes/Legalperson/representative/LegalPersonIdentifier"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />

<saml2:Attribute
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  FriendlyName="RepresentativeFamilyName"
  Name="http://eidas.europa.eu/attributes/naturalperson/representative/CurrentFamilyName"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />

<saml2:Attribute
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  FriendlyName="RepresentativeFirstName"
  Name="http://eidas.europa.eu/attributes/naturalperson/representative/CurrentGivenName"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />

<saml2:Attribute
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  FriendlyName="RepresentativeDateOfBirth"
  Name="http://eidas.europa.eu/attributes/representative/naturalperson/DateOfBirth"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" />

```

## Extended metadata file example – source, regulated profession, power use constraints:

```

<saml2:Attribute
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  FriendlyName="PoRSource"
  Name="http://eidas.europa.eu/attributes/PoR/PoRSource"
  NameFormat="urn:oasis:names:tc:saml2:2.0:attrname-format:uri" />

<saml2:Attribute
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  FriendlyName="RegulatedProfession"
  Name="http://eidas.europa.eu/attributes/PoR/RegulatedProfession"
  NameFormat="urn:oasis:names:tc:saml2:2.0:attrname-format:uri" />

<saml2:Attribute
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
  FriendlyName="PowerUseConstraints"
  Name="http://eidas.europa.eu/attributes/PoR/PowerUseConstraints"
  NameFormat="urn:oasis:names:tc:saml2:2.0:attrname-format:uri" />

```

## Annex I: pilots

The SEMPER pilots provide real implementations of this semantic model. The pilot services do not require the full flexibility of the semantic model yet. Therefore, some simplifications will be introduced for piloting purposes:

1. SEMPER will only pilot public services. Although the semantic model does not exclude private services and service providers, no private partners are involved in the SEMPER project and no private service providers have validated the model;
2. SEMPER will pilot with natural persons representing legal persons only. Piloting natural persons representing other natural persons are out of scope;
3. chained mandates are out of scope as well, so the intermediary element will not be piloted;
4. SEMPER will only use harmonised services to express powers. The method 'non-harmonised' is not part of the pilot;
5. the pilots will only validate the baseline scenario. Alternative scenarios (including powers to delegate) are outside the scope of the pilots;
6. the pilots will not harmonise power use constraints, but allow provision of constraints information. As this information is not harmonised, providing such information most likely will lead to an access denial by the service provider;
7. the pilots will not include regulated professions as a source of powers.

## Annex II: definitions

### Person definitions<sup>7</sup>

Concept	SEMPER interpretation	Description	Examples	National terms
Person	A natural or legal person			AT: Person ES: persona NL: persoon SI: oseba
Natural person	A human being.		Herbert Leitold Arne Tauber Felix Hörandner	AT: natürliche Person ES: persona física NL: natuurlijk persoon SI: fizična oseba
Legal person	An entity constituted under, or governed by, the law of a Member State.	This is an eIDAS definition.	Graz University of Technology	AT: nicht-natürliche Person ES: persona jurídica NL: niet-natuurlijk persoon SI: pravna oseba
Represented person	A person on whose behalf another person acts.	This is a role the person has in accessing and using a service.	Arne Tauber	AT: Vertretener ES: representado NL: vertegenwoordigde SI: zastopani
Representative	A person acting on behalf of another person.	This is a role the person has in accessing and using a service. The representative is the person authenticating.	Felix Hörandner	AT: Vertreter ES: representante NL: vertegenwoordiger SI: zastopnik
Intermediary	An actor in the chain of mandates, not being the represented person or the representative.	This is a role the person has in managing mandates. There can be multiple intermediaries involved in a mandate chain.	An accounting firm of which an employee is representing a client.	AT: Intermediär ES: intermediario NL: intermediair SI: posrednik

<sup>7</sup> The natural person and legal person correspond with the natural person and legal person as defined as subtypes of the object AGENT in the RPAM-model. The RPAM subtype 'System' is out of scope of the SEMPER semantic model.

## SEMPER

### M3 Report on mandate attributes and solutions for cross-border mandate attributes

Note that the concepts “mandator” and “mandate” are used in the process of mandate management. As the focus of the SEMPER model is on the use of the mandate, the SEMPER model uses “represented person” and “representative” instead. A mandatee becomes a representative as soon as he uses the mandate. However, a mandatee will not be representative as long as he does not use the mandate or he delegates the mandate to someone else. In other words: mandator and mandatee are concepts for mandate management and represented person and representative are concepts for service fulfilment.

#### PoR definitions

Concept	SEMPER interpretation	Description	Examples	National terms
Power of representation	The right to act on behalf of another Person.	Powers of representation can originate from several sources. SEMPER distinguishes powers from several sources: <ul style="list-style-type: none"> <li>- a mandate</li> <li>- legislation</li> <li>- a court ruling</li> <li>- a regulated profession</li> </ul>		AT: Vertretungsmacht ES: poder de representación NL: vertegenwoordigingsbevoegdheid SI: upravičenost za zastopanje
Source of power: mandate	A person’s powers that have been granted by a wilful act of another person.	This wilful act is registered in a mandate management system and might need registration in an official document or source to be valid, or in some cases require an official confirmation by a notary.	The mandate Herbert has granted to Arne grants Arne the power to take care of Herbert’s health care insurance.	AT: Vollmacht ES: apoderamiento NL: machtiging SI: pooblastilo
Source of power: legislation	A person’s powers that have been explicitly defined in law.	Company law specifies the powers of persons holding certain positions in the company, like a CEO.  Civil law specifies the powers a person has a parent to his child and a heir to his family.	<ul style="list-style-type: none"> <li>- Being head of eGovernment Innovation Center grants Arne the power to represent the Center in several services.</li> <li>- A mother has powers to represent her underaged child in medical affairs.</li> </ul>	AT: Gesetzgebung ES: legislación NL: wetgeving SI: zakonodaja
Source of power: court ruling	A person’s powers that have been granted by a judge.	A court ruling may specify the powers a person has to represent another person, e.g. because the other person has gone bankrupt or insolvent.	A court ruling gives the curator the powers to sell all assets of the company that has gone bankrupt.	AT: Gerichtsbeschluss ES: sentencia judicial NL: rechterlijke uitspraak SI: odločba

## SEMPER

### M3 Report on mandate attributes and solutions for cross-border mandate attributes

Source of power: regulated profession	A person's powers that originate from his/her profession.	This may be the case for certain legally defined professions. As soon as the person is not a regulated professional anymore, his representational powers are withdrawn.  See directive 2005/36/EC on the recognition of professional qualifications (REGPROF).	Examples of regulated professions: - Notary - Lawyer - Doctor  Being a notary grants Felix the power to represent his clients in specific formal procedures in front of public organisations.	AT: berufsmäßige Parteivertreter ES: profesión regulada NL: beschermd beroep SI: reguliran poklic
---------------------------------------	---	--	--	--

### Scope of power definitions

Concept	SEMPER interpretation	Description	Examples	National terms
Scope of power	The activities the representative can perform on behalf of the represented person	The scope of powers can – if powers are not full – be expressed as harmonised or non-harmonised activities. In SEMPER the scope of powers need to be expressed in a machine-readable way.	A list of services the representative can use on behalf of the represented person.	AT: Wirkungsbereich ES: alcance del poder NL: reikwijdte SI: obseg pooblastila
Service provider	An organisation providing an online service.	Based on RPaM.	RVO.nl	AT: Anwendungsbetreiber ES: proveedor de servicios NL: dienstverlener SI: ponudnik storitve
Service	The chain of activities performed by a service provider to create added value for natural or legal persons.	A public service is always based on rules and regulations. By fulfilling a service, a natural or legal person exercises a right or complies with an obligation as defined in law.	- Car registration - Income tax - Student enrolment - Electronic delivery of mail	AT: Anwendung ES: servicio NL: dienst SI: storitev
harmonised service	A service that has been standardised regarding its name, input and output.	There are several initiatives aiming for EU-wide harmonisation of services.	- SDGR - Service directive - SEMPER	AT: harmonisierte Anwendung ES: servicio armonizado NL: geharmoniseerde dienst SI: poenotena storitev

non-harmonised service	A service that has been defined by a service provider.	Not all services are harmonised. Service providers can define their own services as well.	<ul style="list-style-type: none"> <li>- Berichtenbox voor bedrijven</li> <li>- Subsidie jonge akkerbouwers</li> </ul>	AT: nicht-harmonisierte Anwendung ES servicio no armonizado NL: niet-geharmoniseerde dienst SI: posebna storitev
Relying party	A natural or legal person that relies upon an electronic identification or a trust service.	This is an eIDAS definition.		AT: Anwendung, Anwendungsbetreiber ES: parte usuaria NL: relying party SI: zanašajoča se stranka

## Power use constraint definitions

Concept	SEMPER interpretation	Description	Examples	National terms
Power use constraint <sup>8</sup>	A restriction of the right to act on behalf of another person.	Representatives may perform the activities as defined by the scope of power. PUCs specify the limits in the extent to which these activities may be performed.  PUCs have been defined in the RPaM model.	Transaction limit = €10.000	AT: Einschränkung ES: restricción NL: inperking SI: omejitev pravic zastopanja
Harmonised PUC	A PUC that has been standardised as part of service harmonisation.	Service harmonisation may include harmonisation of PUCs as well. Mandate management systems as well as service providers should acknowledge these PUCs so cross-border effectuation can be easily accomplished.		AT: harmonisierte Einschränkung ES: restricción armonizada NL: geharmoniseerde inperking SI: poenotena omejitev pravic
Non-harmonised PUC	A PUC defined by an individual mandate management system.	Not all PUCs will be harmonised across the EU. Each mandate management system may present its users with the option to limit powers on aspects that have been defined by the owner of the		AT: nicht-harmonisierte Einschränkung ES: restricción no armonizada NL: niet-geharmoniseerde inperking SI: posebna omejitev pravic

<sup>8</sup> The RPaM-concept eAuthorisation criteria (eAC) is relevant for service delivery and not for accessing a service, hence it is out of scope of the SEMPER-model.

		specific mandate management system. Cross-border effectuation of these PUCs is more difficult, as acknowledgment of non-harmonised PUCs by service providers is much more complex.		
--	--	--	--	--

## Annex III: structure and examples of scope

The diagram below depicts the objects and their relations relevant for the “scope” concept.

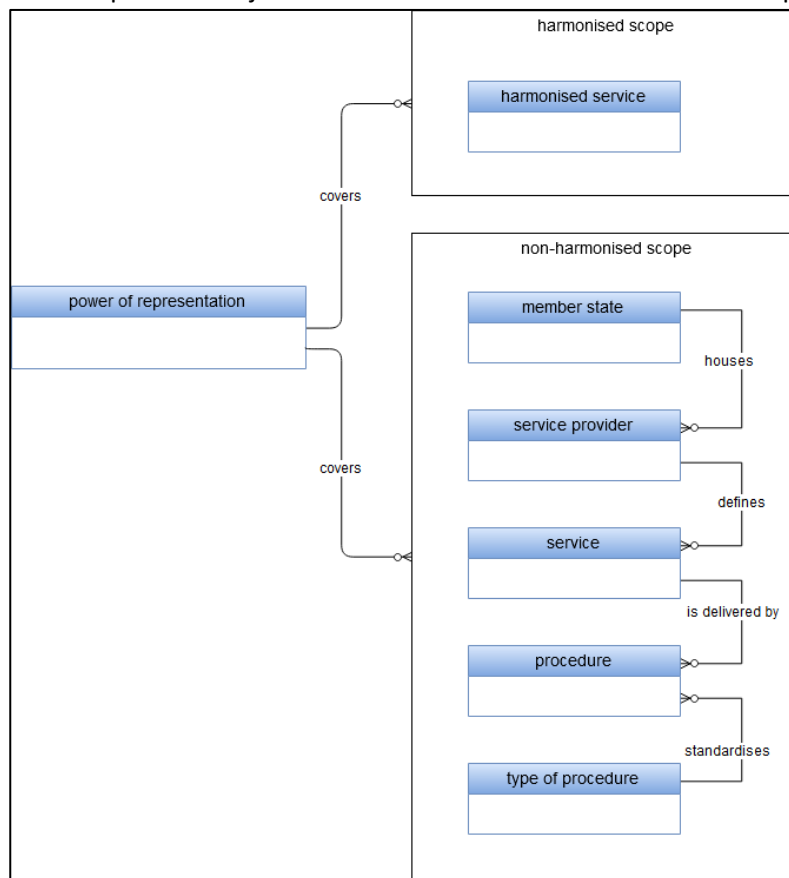


Figure 5 Model of Scope of Power

The principles of the scope of power are explained with different examples for the implementation of the use-case “A Spanish (natural) person wants to represent a Spanish (legal) person in the Netherlands to handle their digital mail”.

### Method 1: Harmonised scope

#### *Request*

1. The specified service is provided by RVO.nl and it is an harmonised service called ‘Electronic delivery’.
2. RVO.nl’s request to validate the power contains ‘harmonised service: Electronic Delivery’.

#### *Response*

1. In case the Spanish mandate management system has included this harmonised service in the catalogue and finds a valid mandate on this harmonised service: the powers are valid.
2. In case the Spanish mandate management system has included “The Netherlands” in the catalogue and finds a valid mandate on this member state: the powers are valid.
3. In case the Spanish mandate management system has included “RVO.nl” in the catalogue and finds a valid mandate on this service provider: the powers are valid.

In any case, it will always be up to the Spanish mandate management system to decide on which of the above elements to include in the catalogue.



<i>Service provider:</i>	<i>Mandate management system:</i>	<i>Mandate management system:</i>
<i>Specified scope in request</i>	<i>Sufficient powers in case of a valid mandate on one of</i>	<i>Insufficient powers in case of a valid mandate on one of</i>
Harmonised service	<ul style="list-style-type: none"> <li>- Member state</li> <li>- Service provider</li> <li>- Harmonised service</li> </ul>	Everything else

### Method 2: Non-harmonised scope

#### *Request*

1. The specified 'non-harmonised service' is provided by RVO.nl and is called 'Berichtenbox voor bedrijven'.
2. RVO.nl requests to validate the PoR on the scope 'member state: NL, service provider: RVO.nl, service: 'Berichtenbox voor bedrijven'.

#### *Response*

1. To be able to verify the scope of this request, the Spanish mandate management system should at least have registered 'member state: NL' in the catalogue. A valid mandate on 'member state: NL' will be sufficient to use all services in the Netherlands, including 'Berichtenbox voor bedrijven'
2. If desirable, the Spanish mandate management system can also add the service provider "RVO.nl" to the catalogue of the mandate management system. A valid mandate on "RVO.nl" will be sufficient to use all services of 'member state: NL, service provider: RVO.nl', including 'Berichtenbox voor bedrijven'.
3. Furthermore, the Spanish mandate management system can add the service 'Berichtenbox voor bedrijven' to the catalogue. As this is exactly the service for which the validation of powers has been requested, a valid mandate is of course sufficient to use this service.
4. In case the Spanish mandate management system has also added the procedures of this service to the catalogue, like 'berichten lezen' (read messages) and 'berichten verwijderen' (delete messages), persons can grant mandates on this granularity in the Spanish registry as well. A valid mandate on one of these procedures will *not* be sufficient to use the full service 'Berichtenbox voor bedrijven'. The mandate management system can only declare powers on parts of the service (the procedures) and not the service as a whole.

The same logic goes for powers validations on the level of the member state as a whole, the service provider, a specific procedure or a type of procedure. In any case, it will always be up to the mandate management system to decide upon the level of granularity it wants to support. The less granular, the shorter the catalogue and less specific mandates can be granted. The more granular, the longer the catalogue and the more specific mandates can be granted.

From a service provider perspective: the more specific the scope definition (lower in the hierarchy), the bigger the chance powers can be successfully validated. The scope of requested powers becomes smaller stepping down the hierarchy (the person needs less powers to have a valid mandate for the requested scope).

<i>Service provider: Specified scope in request</i>	<i>Mandate management system: Sufficient powers in case of a valid mandate on one of</i>	<i>Mandate management system: Insufficient powers in case of a valid mandate on one of</i>
Member state	- Member state - - -	- - Service provider - Service - Procedure - Type of procedure
Service provider	- Member state - Service provider - -	- - Service - Procedure - Type of procedure
Service	- Member state - Service provider - Service - -	- - - Procedure - Type of procedure
Procedure	- Member state - Service provider - Service - Procedure - Type of procedure	- - - -
Type of procedure	- Member state - - - - Type of procedure	- - Service provider - Service - Procedure -

## Annex IV: legal

The SEMPER project identifies some legal topics to address in more detail as soon as large scale implementation of the SEMPER baseline scenario is foreseen.

### Liability

SEMPER follows the eIDAS philosophy on responsibility and liability. The validating member state is responsible for proper validation of powers for the requested scope. The relying member state should accept the resulting 'declaration of powers' to grant or deny access. In the eIDAS regulation this has been specified for the authentication part of the process. Similar regulation is lacking for powers validation. The legal basis for large scale implementation of the SEMPER baseline scenario should be taken care of.

### Consent

eIDAS is the legal basis for processing personal data. This legal basis is needed under the GDPR. The legal basis needs to be extended to powers information. By the absence of this legal basis today, the validating member state should implement "consent" on the powers information. GDPR allows explicit consent of the user as a basis for processing personal data.

### Quality assurance framework

eIDAS defines three levels of assurance for authenticating persons and mentions the attacks it should be resistant to for each level: low, substantial, and high. SEMPER adds information on powers to eIDAS. On a European scale, it lacks a quality assurance framework for powers. This framework has to be formulated and agreed upon. SEMPER expects the framework to consist of requirements on (at least): the registration of powers, authentication of the person(s) registering the mandate, quality of updating registered powers (like extending the period of validity), detecting unintended use or misuse of powers information.

## Annex V: process

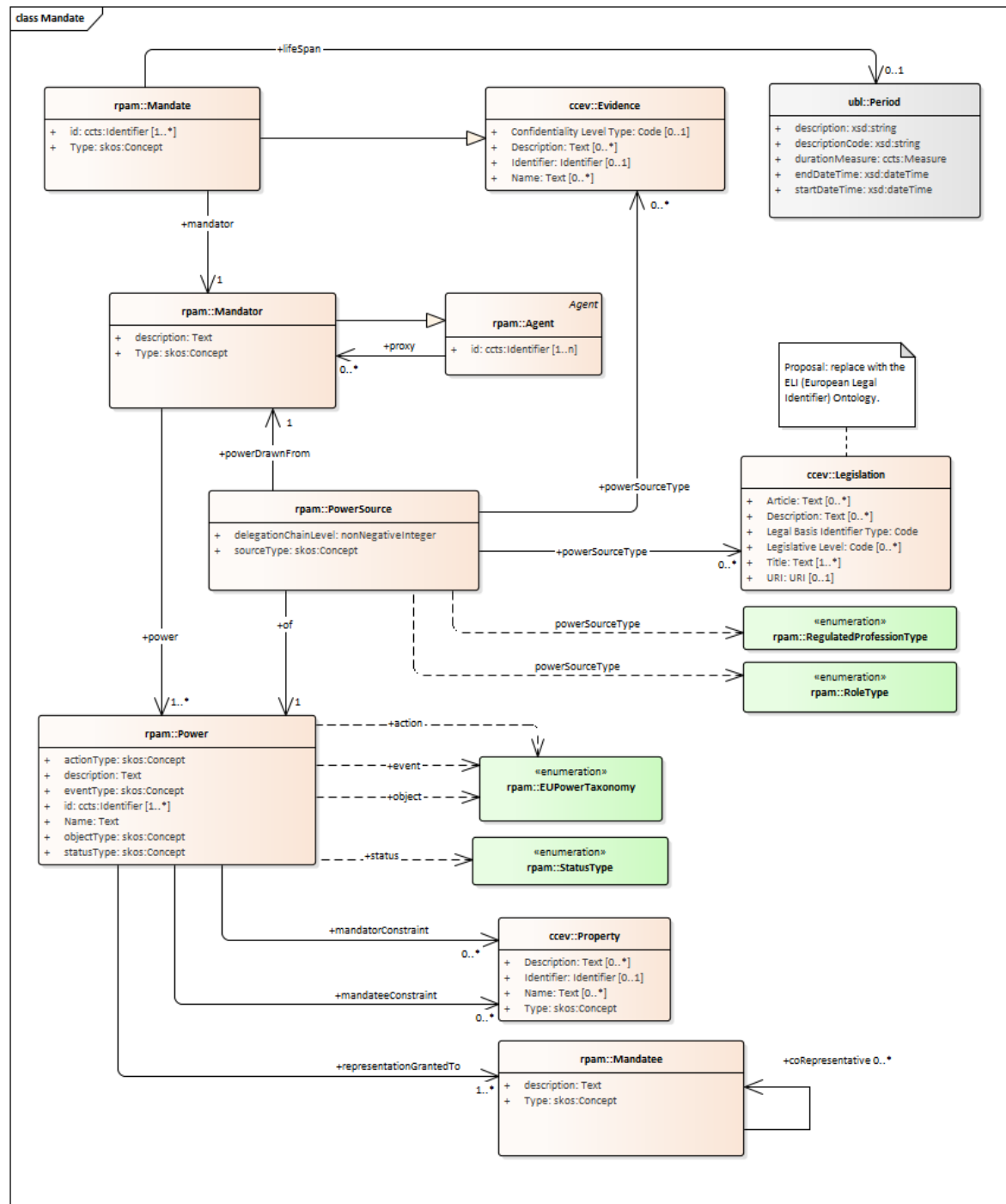
This semantic model has been constructed in the period March 2019 to the end of May 2019 by participants of the SEMPER project. In this period, two physical workshops and multiple remote calls have been organised. Several versions have been reviewed. First of all, within the project. In April a draft version has been validated by national experts of the participating member states (not directly involved in the project). Their feedback has been discussed in the second workshop and incorporated in the final version. This draft version was shared with the ISA2 2016.12 project (Everis) and discussed in a telco. The SEMPER project received feedback in Word from this project as well. The comments were processed to a large extent.

## Annex VI: ISA2 2016.12 RPaM

ISA2/RPaM action aims at providing a common vocabulary that makes it possible to map the national models to the common vocabulary and assuring that the core data can be shared cross-border and cross-domain.

SEMPER concept	Alignment SEMPER-RPaM
Person	<p>The SEMPER-objects 'natural person' and 'legal person' correspond with the 'natural person' and 'legal person' as defined as subtypes of the object AGENT in the RPaM-model. The RPaM subtype 'System' of the object AGENT is out of scope of the SEMPER semantic model.</p> <p>In the SEMPER-model a person can fulfill a role regarding powers of representation: a representative, a represented person or an intermediary. In the RPaM-model a person can be a mandator, which corresponds with the represented person role; the RPaM-model also defines the concept of mandate, which corresponds with the role of the representative. As explained in de definitions annex, SEMPER differentiates between the registration of the mandate (mandator/mandatee) and the use of the mandate (represented person/representative).</p>
Power of representation	<p>SEMPER defines the power of representation as the right to act on behalf of another person, which covers a specific scope and can be bound by constraints.</p> <p>RPaM defines a <i>mandate</i> as the terms under which a mandator grants a representation power and defines the power as a capacity to act on a person's own behalf or on behalf of another person. This power is related to a power source which can be of a certain type: Evidence, Legislation, RegulatedProfessionType or Role Type.</p> <p>SEMPER integrated both RPaM concepts into one: "powers of representation". Furthermore, SEMPER uses "mandate" for one of the power sources: powers that originates from a wilful act. Other SEMPER power sources are: legislation, court ruling and regulated profession.</p> <p>This subdivision in power sources is driven by differences in operational handling of the powers. Mandates will be registered in mandate management systems, powers based on legislation have their origin in citizen and business registers, court rulings in dedicated ruling registries and regulated professions will be registered in dedicated registers for these professions.</p>
Scope of power	<p>SEMPER defines the scope which is covered by powers of representation either as a harmonised scope, based on SGDR or other harmonisation-models, or as a non-harmonised scope (for services that are not yet or will not be harmonised). This corresponds with the current mandate management systems and pilot-services of the participating member states. It differs though from the RPaM-model: RPaM defines the scope by relating the power to an</p>

SEMPER concept	Alignment SEMPER-RPaM
	EUPowerTaxonomy-object, which, among other components, contains a decomposition of services on the basis of subject of the service (work, mobility, ...).
Power use constraint	<p>The SEMPER-object power use constraint (PuC) corresponds with the same RPaM-concept implemented as a property of a power. The RPaM-concept eAuthorisation criteria (eAC) is out of scope of the SEMPER-model.</p> <p>In the RPaM-model the PuC and eAC are based on the Core Criterion and Evidence Vocabulary (CCEV). SEMPER defines EU-harmonised and non-harmonised constraints, which can be described in the terms of the CCEV but this is not mandatory.</p> <p>In the SEMPER model, a power use constraint restricts the power of representation. A PoR can be bound by multiple PUCs. This corresponds with the mandateeConstraint relation of the RPaM-model.</p>



RPaM v1.1.0 Overall.png

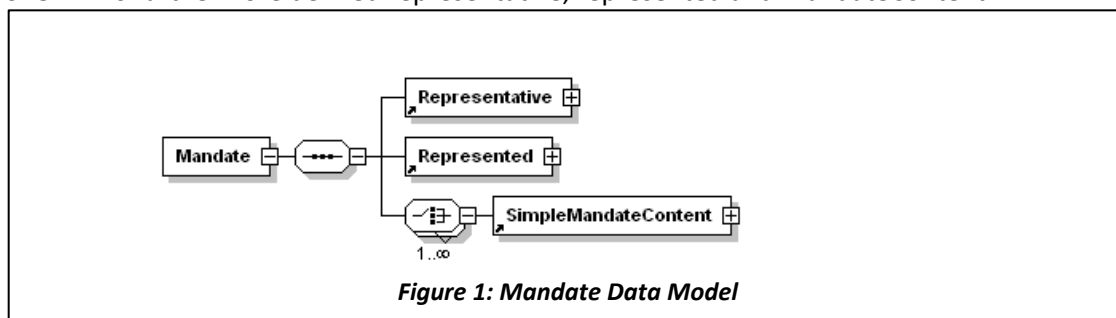
## Annex VII: STORK 2.0

The STORK 2.0 project started in 2012 and involved 55 organizations, both public and private, across 19 European countries. It has further built on the STORK framework for cross-border electronic identification and authentication (eID) of citizens and businesses in the EU and Associated Countries. STORK 2.0 allows citizens to identify themselves across-borders by using identity-related data from authentic and reliable sources (attribute providers) or to represent other natural or legal persons, in the context of different business domains.

STORK 2.0 defined a mandate as: “A mandate is a bundle of one or more authorizations granted by an identified entity (the principal, the represented person) to another identified entity (the agent, the representative) to perform well-defined actions with legal consequences in the name and for the account of the former.”

This is similar to the SEMPER definition and use of the concept “mandate”. SEMPER acknowledges other sources of powers as well that were outside of STORK 2.0’s scope: legislation, court ruling, and regulated profession.

STORK 2.0 furthermore defined representative, represented and MandateContent.



STORK concept	STORK definition	SEMPER
representative	The entity which received the permission to act on behalf of the represented entity.	This definition resembles the one of SEMPER, but the focus of the SEMPER definition is on use of the mandate instead of receiving the mandate (mandate management process). The use of this concept is the same in both models though.  Both models distinguish between natural and legal persons. In the SEMPER model, the attributes of natural persons and legal persons are exactly aligned with eIDAS. STORK 2.0 is pre-eIDAS.
represented	The entity granting the authorisations to the representative so as to act on its behalf.	See “representative” for similarities and differences.



STORK concept	STORK definition	SEMPER
MandateContent	The authorizations granted by the represented entity to the representative entity along with restrictions.	This closely resembles the “powers of representation” concept in SEMPER.
The type of power	The type of powers is the main ‘scoping element’ for expressing the powers <sup>9</sup> .	The STORK 2.0 type of powers can be seen as a list of harmonised services (with the STORK 2.0 project as harmonisation authority). The SEMPER project adds more flexibility to the scope, by enabling other harmonised and non-harmonised services as well.
The period of validity		This attribute is not relevant in SEMPER’s scope due to the principle of snapshot powers validation. The cross-border information on powers is only valid as long as the user session is active. Independent of the period of validity of the mandate itself (as the mandate may, for example, be revoked directly after validation).
Transaction limits	currency and amount	This is a power use constraint in the SEMPER model.
isJoint	some powers may only be executed with someone else, e.g. two company owners that both need to sign a contract).	Out of scope for SEMPER.
isChained	indicating there is a chain of powers	In SEMPER this is a direct consequence of having one or more intermediary persons. In SEMPER there is no need for an additional attribute.

Finally, STORK 2.0 defined sector specific attributes for academia, banking, and health. Some sector specific attributes deal with the person’s profession, like “isHealthCareProfessional”, “isAdminStaff” and “isCourseCoordinator”. This resembles SEMPER’s regulated profession concept, although in STORK this concept is not explicitly used in the context of someone’s powers.

<sup>9</sup> STORK 2.0 distinguished between: 0=General Powers, 1=Commercial Powers, 2=Human Resource Powers, 3=General Services Powers, 4=Financial powers, 5=Public Interest Representation Powers, 6=Health Powers.

## Annex VIII: SDGR

The single digital gateway will facilitate online access to the information, administrative procedures, and assistance services that citizens and businesses need to get active in another EU country. By the end of 2020, citizens and companies moving across EU borders will easily be able to find out what rules and assistance services apply in their new residency. By the end of 2023 at the latest, they will be able to perform a number of procedures in all EU member states without any physical paperwork, like registering a car or claiming pension benefits.

The Regulation that brings the gateway into effect also requires that more administrative procedures can be performed online than currently, by users in their own country and cross-border users. By December 2023 at the latest:

- A list of 21 important administrative procedures will be available fully online in all EU countries
- All national online procedures will have to be made fully accessible to cross-border users
- The 'once-only principle' (i.e. users should not have to submit to authorities documents or data already held by other authorities) will be applied to cross-border exchanges of evidence for a range of procedures. For these procedures, users will be given the option to request the direct exchange of evidence between authorities in different member states

At first, the focus will lie on making 13 key public services available as part of the Gateway. These central administrative procedures are expected to have the highest impact and shall be eventually provided digitally by all EU Member States. They include: Requests for a birth certificate, Car registration, Starting a business and Registering for social security benefits.

For SEMPER the SDGR provides a list of harmonised services to express the scope of powers.

## ANNEX II

## Procedures referred to in Article 6(1)

Life events	Procedures	Expected output subject to an assessment of the application by the competent authority in accordance with national law, where relevant
Birth	Requesting proof of registration of birth	Proof of registration of birth or birth certificate
Residence	Requesting proof of residence	Confirmation of registration at the current address
Studying	Applying for a tertiary education study financing, such as study grants and loans from a public body or institution	Decision on the application for financing or acknowledgement of receipt
	Submitting an initial application for admission to public tertiary education institution	Confirmation of the receipt of application
	Requesting academic recognition of diplomas, certificates or other proof of studies or courses	Decision on the request for recognition
Working	Request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004 <sup>(1)</sup>	Decision on applicable legislation
	Notifying changes in the personal or professional circumstances of the person receiving social security benefits, relevant for such benefits	Confirmation of receipt of notification of such changes
	Application for a European Health Insurance Card (EHIC)	European Health Insurance Card (EHIC)
	Submitting an income tax declaration	Confirmation of the receipt of the declaration
Moving	Registering a change of address	Confirmation of deregistration at the previous address and of the registration of the new address
	Registering a motor vehicle originating from or already registered in a Member State, in standard procedures <sup>(2)</sup>	Proof of registration of a motor vehicle
	Obtaining stickers for the use of the national road infrastructure: time-based charges (vignette), distance-based charges (toll), issued by a public body or institution	Receipt of toll sticker or vignette or other proof of payment
	Obtaining emission stickers issued by a public body or institution	Receipt of emission sticker or other proof of payment

21.11.2018		EN	Official Journal of the European Union	L 295/37
Life events	Procedures	Expected output subject to an assessment of the application by the competent authority in accordance with national law, where relevant		
Retiring	Claiming pension and pre-retirement benefits from compulsory schemes	Confirmation of the receipt of the claim or decision regarding the claim for a pension or pre-retirement benefits		
	Requesting information on the data related to pension from compulsory schemes	Statement of personal pension data		
Starting, running and closing a business	Notification of business activity, permission for exercising a business activity, changes of business activity and the termination of a business activity not involving insolvency or liquidation procedures, excluding the initial registration of a business activity with the business register and excluding procedures concerning the constitution of or any subsequent filing by companies or firms within the meaning of the second paragraph of Article 54 TFEU	Confirmation of the receipt of notification or change, or of the request for permission for business activity		
	Registration of an employer (a natural person) with compulsory pension and insurance schemes	Confirmation of registration or social security registration number		
	Registration of employees with compulsory pension and insurance schemes	Confirmation of registration or social security registration number		
	Submitting a corporate tax declaration	Confirmation of the receipt of the declaration		
	Notification to the social security schemes of the end of contract with an employee, excluding procedures for the collective termination of employee contracts	Confirmation of the receipt of the notification		
	Payment of social contributions for employees	Receipt or other form of confirmation of payment of social contributions for employees		

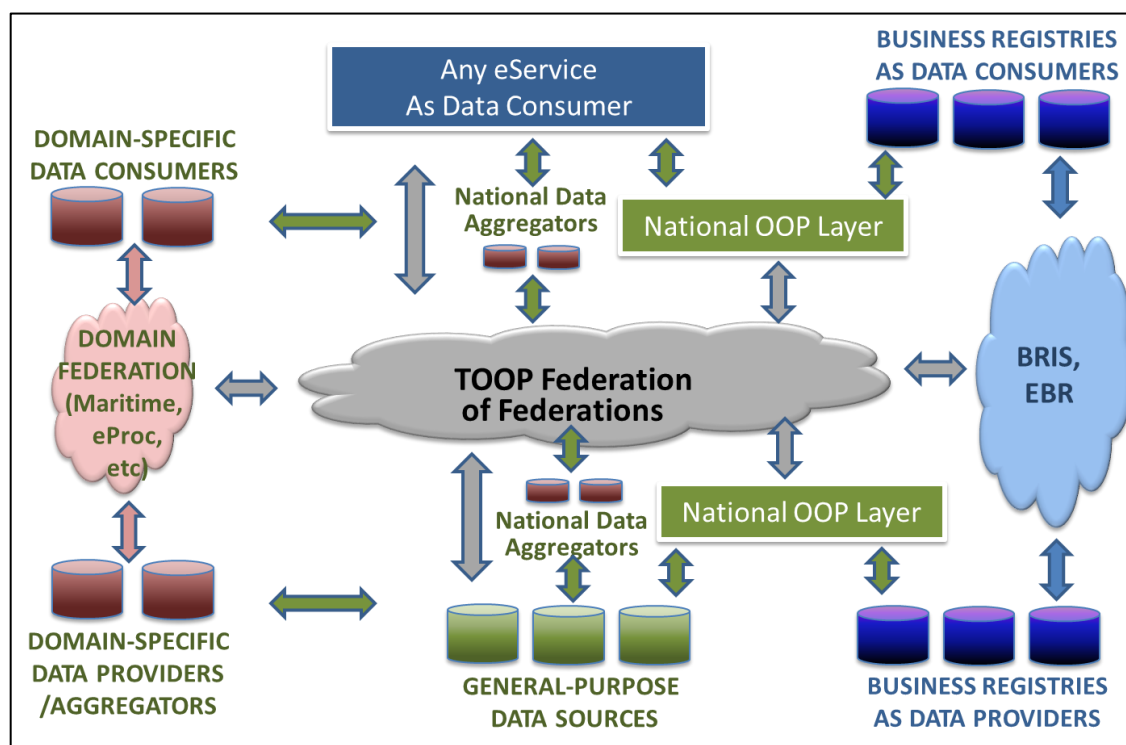
(<sup>1</sup>) Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems (OJ L 166, 30.4.2004, p. 1).

(<sup>2</sup>) This covers the following vehicles: (a) any motor vehicle or trailer as referred to in Article 3 of Directive 2007/46/EC of the European Parliament and of the Council (OJ L 263, 9.10.2007, p. 1); and (b) any two- or three-wheel motor vehicle, whether twin-wheeled or otherwise, intended to travel on the road, as referred to in Article 1 of Regulation (EU) No 168/2013 of the European Parliament and of the Council (OJ L 60, 2.3.2013, p. 52).

## Annex IX: TOOP

The Once - Only Principle Project (TOOP) was launched by the European Commission in January 2017. It is an initiative of 51 organisations from EU Member States and Associated Countries to explore and demonstrate the once - only principle on a cross-border scale. Therefore, TOOP is aiming to develop a generic federated architecture that is able to connect 60 systems from at least 21 countries.

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 in respect of data protection regulations and other constraints.



Although TOOP does not explicitly deal with mandate information, the SEMPER project sees some common ground between both projects:

- SEMPER follows the once only principle as mandate information will be used cross-border directly from the source. Persons do not need to provide papers proving their powers to represent. The quality of eAuthorisation by service providers will improve by up-to-date powers information. Access to services will become more secure and reliable.
- TOOP piloted to a large extent with cross-border provision of company information from official business registers. In many use cases, this starts with a user authenticating via eIDAS, creating a strong eIDAS-TOOP combination. The representation of a company has been a missing link so far. SEMPER fills this gap:
  1. eIDAS: identifying the representative
  2. SEMPER: validating his powers to act on behalf of the represented person
  3. TOOP: retrieving information of the represented person