SEMPER

Cross-border Semantic Interoperability of Powers and Mandates

Participants

- Graz University of Technology (AT)
- Ministerio de Asuntos económicos y transformación digital (ES)
- Ministry of Public Administration (SI)
- Rijksdienst voor Ondernemend Nederland (NL)

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

Grant Agreement Number: INEA/CEF/ICT/A2018/1633489

Outline

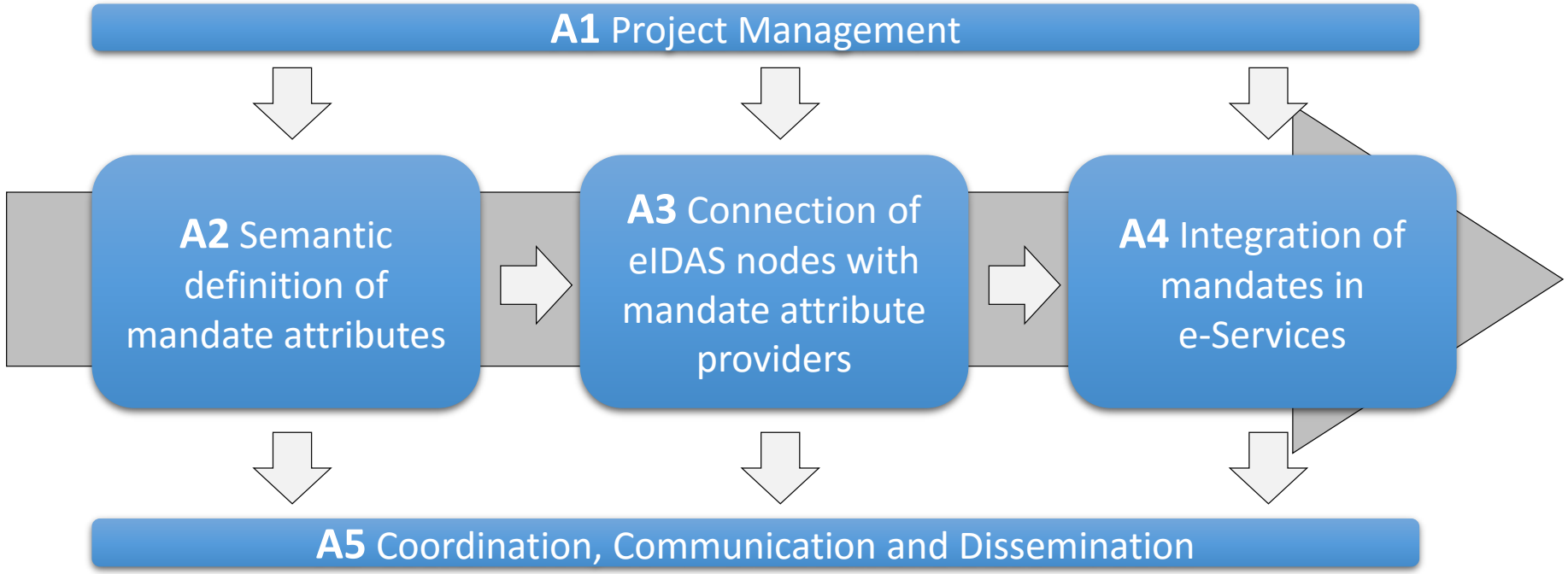
- The SEMPER project
- The SEMPER concept of powers validation
- Scope of piloting and limitations
- Demo-Video

The SEMPER project

The project

SEMPER: Cross-border Semantic Interoperability of Powers and Mandates

- Semantic definitions of mandate attributes
- Enhance the eIDAS Infrastructure (eIDAS nodes)
- Pilot and validate in partner services



Key data

- CEF Project by a consortium with participant from four MS
  - Austria (Graz University of Technology - EGIZ; A-SIT)
  - Slovenia (Ministry of Public Administration)
  - Spain (Ministerio de Política Territorial y Función Pública, MIHFP)
  - The Netherlands (Rijksdienst voor Ondernemend Nederland, RVO.nl)
- Started January 2019, Duration 24 months
- Specification and integration with services in 2019
- Piloting in 2020
  - First with testing services
  - Then with production services

The SEMPER concept of powers validation

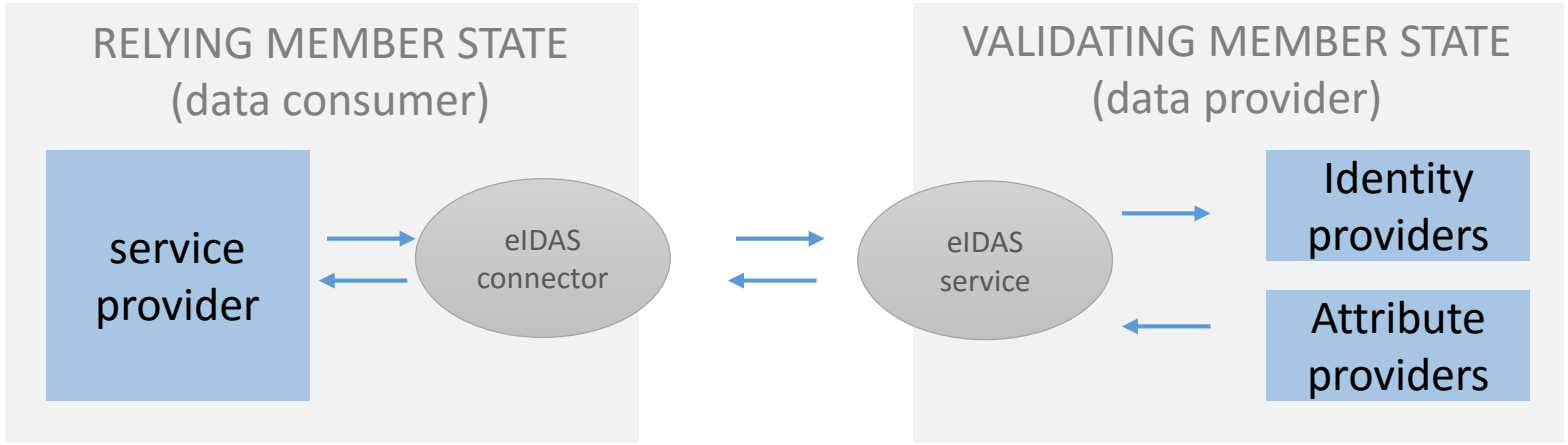
Representation scenarios

natural person representing another natural person 
natural person representing a legal person 
natural person acting on behalf of a legal person representing a natural person 
natural person acting on behalf of a legal person representing a legal person 

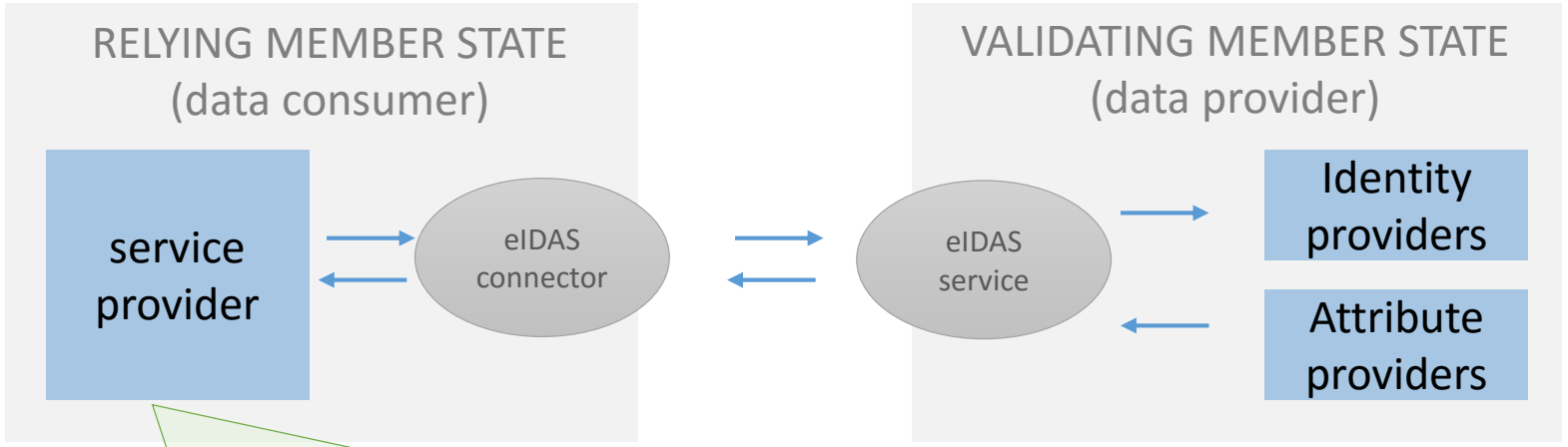
Not supported:

- Two legal representatives have joint powers / signing authority

High level proces flow



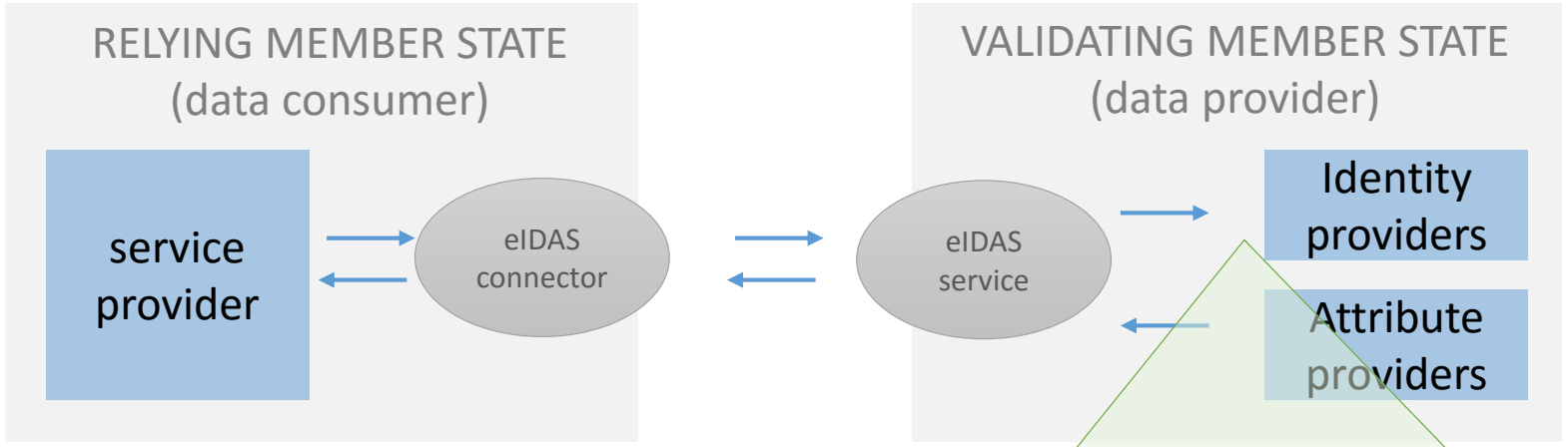
High level proces flow



1. INITIATE

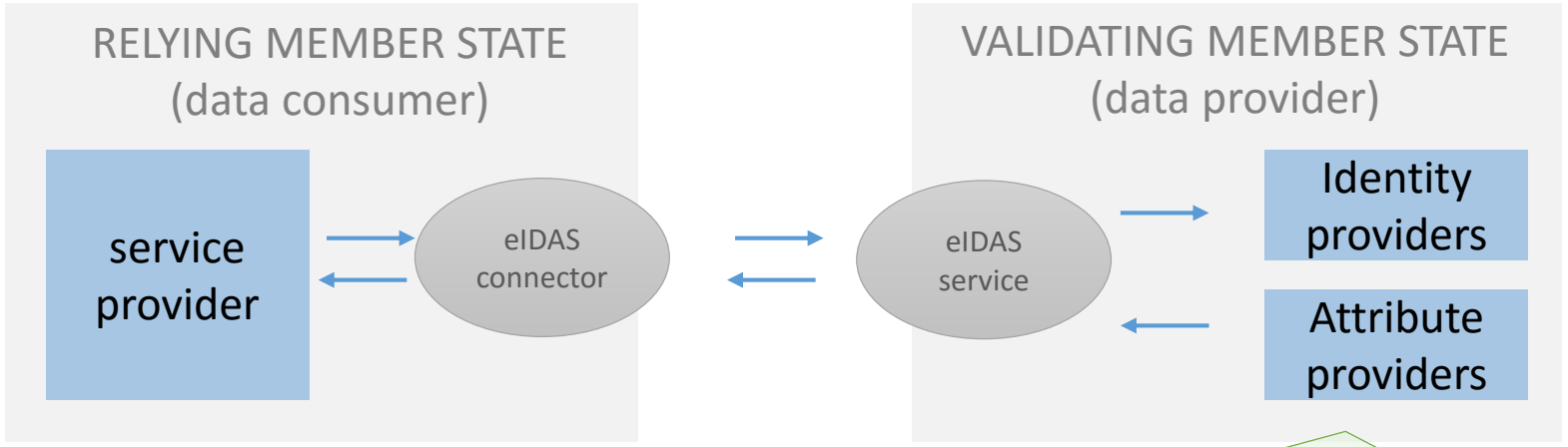
- A person browses to the website of a service provider and chooses to login from another country.
- The service provider initiates a cross border authentication by sending a request to the (central or decentral) eIDAS connector.
- The service provider specifies the person attributes it wants to receive **and the powers that need to be validated** (the scope the access is requested on and the type of representation that the Service provider allows).
- This request is validated and forwarded to the eIDAS service of the country the person has an eID of (the providing country).

High level proces flow



2. AUTHENTICATE REPRESENTATIVE
(One of) the identity providers of the validating member state authenticates the representative at (at least) the requested level of assurance (LoA).

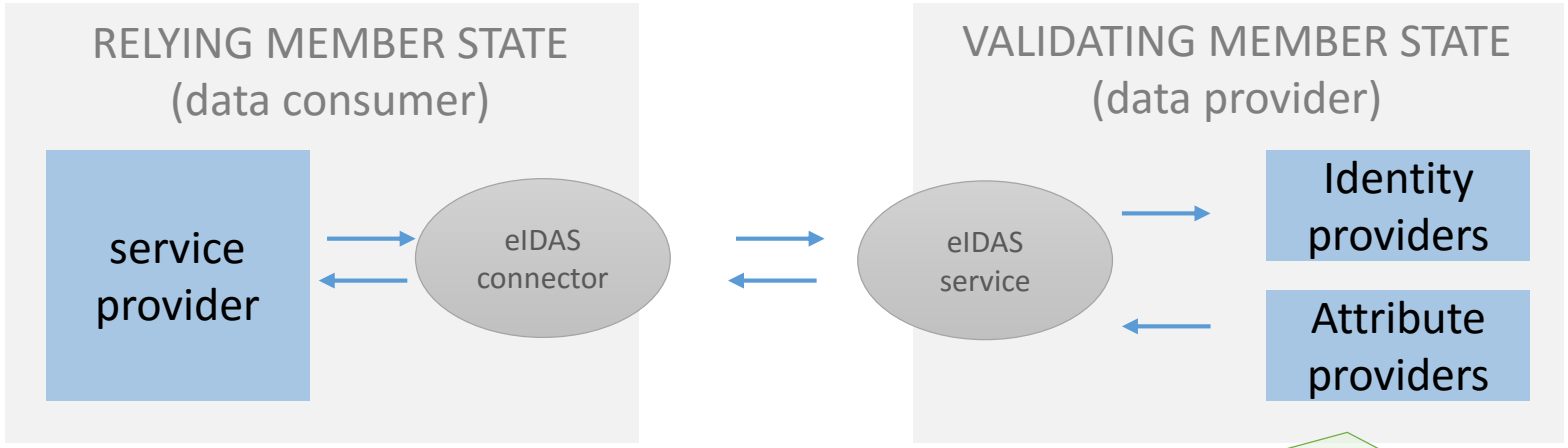
High level proces flow



3. IDENTIFY REPRESENTED

- The mandate management system of the validating member state identifies the represented.
- 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
  - select the representative from a list of persons he may represent (source: mandate management system)
  - select the mandate to execute directly (source: mandate management system)

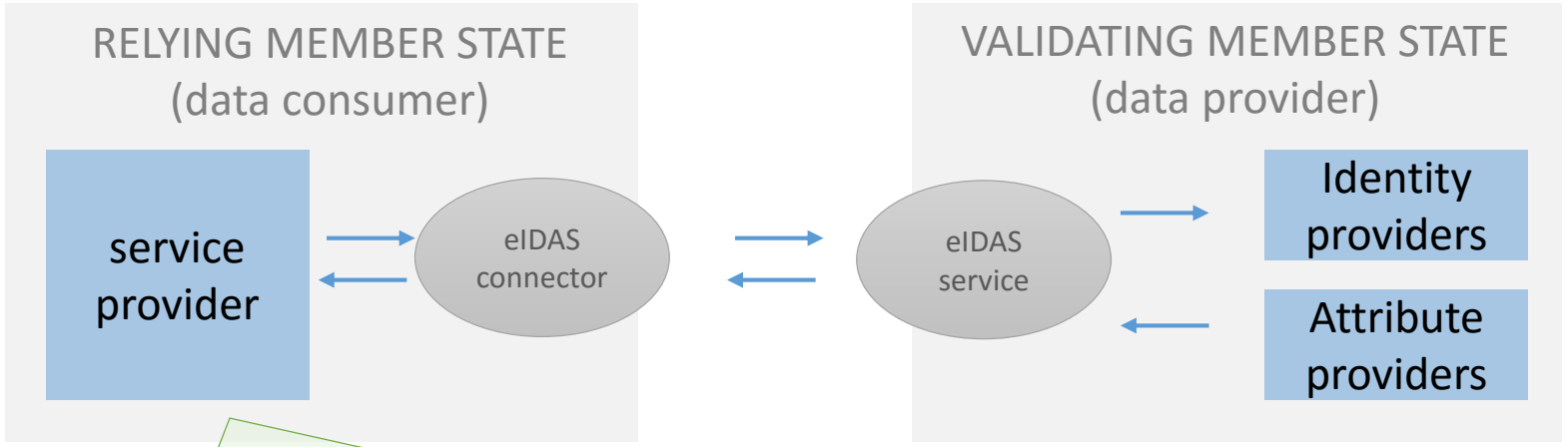
High level proces flow



4. VALIDATE POWERS TO REPRESENT

- The mandate management system validates the powers of the representative to act on behalf of the represented.
- 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 specific 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 country via the eIDAS service of the providing country. The response contains the scope requested and the outcome of the validation of powers: the powers are either sufficient or insufficient for the requested scope.

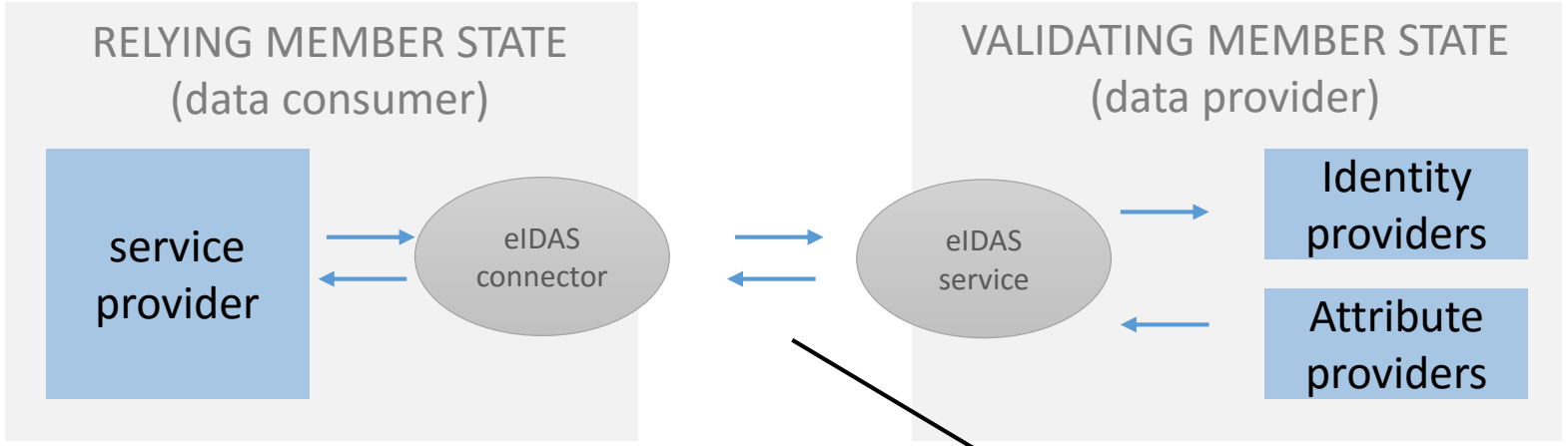
High level proces flow



5. GRANT ACCESS TO SERVICE

- The relying country uses the response to decide upon granting the representative access to the requested service on behalf of the represented (eAuthorisation).
- Therefore it assesses the authentication of the representative as well as the powers. Both need to provide enough assurance.

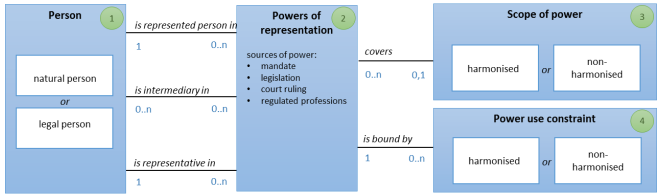
High level proces flow



SEMPER approach:

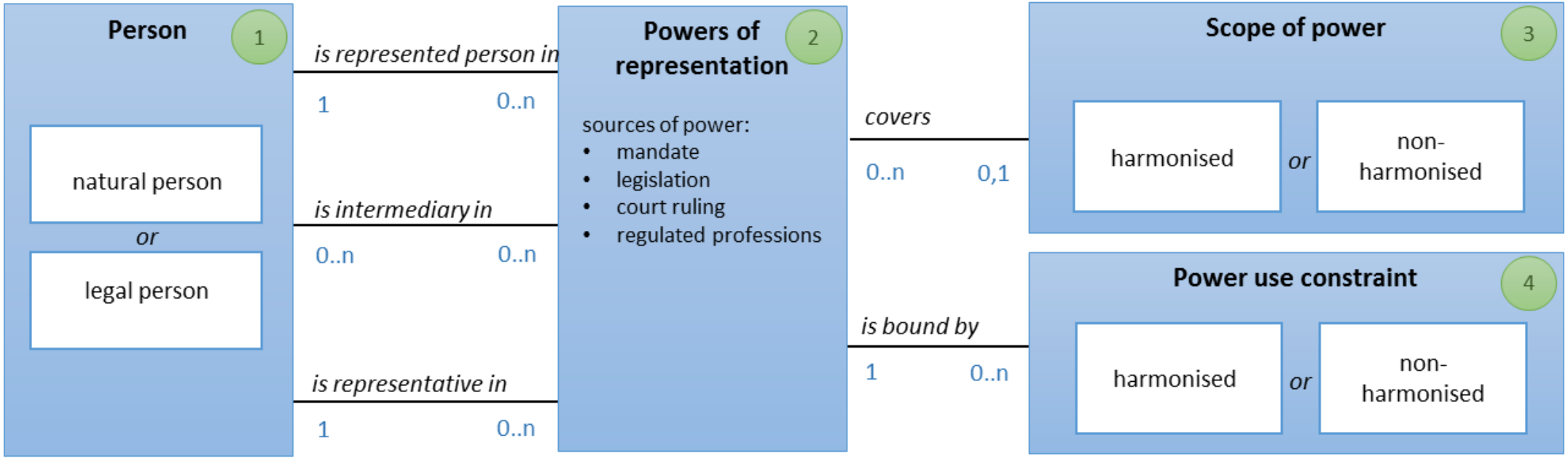
- powers validation **combined with eIDAS authentication**
- SEMPER sets standard for **communication on powers validation** only, not on mandate management
- strive for **simplest model** possible, with “access policy” as core criterion
- **snapshot of powers**: powers declaration valid for several minutes only
- **fit for SEMPER-purpose**: other approaches would have been possible as well

SEMPER extension on the eIDAS attribute profile



Main concepts

High level semantic model for cross border exchange of information on powers.



SEMPER messages

Powers validation request:

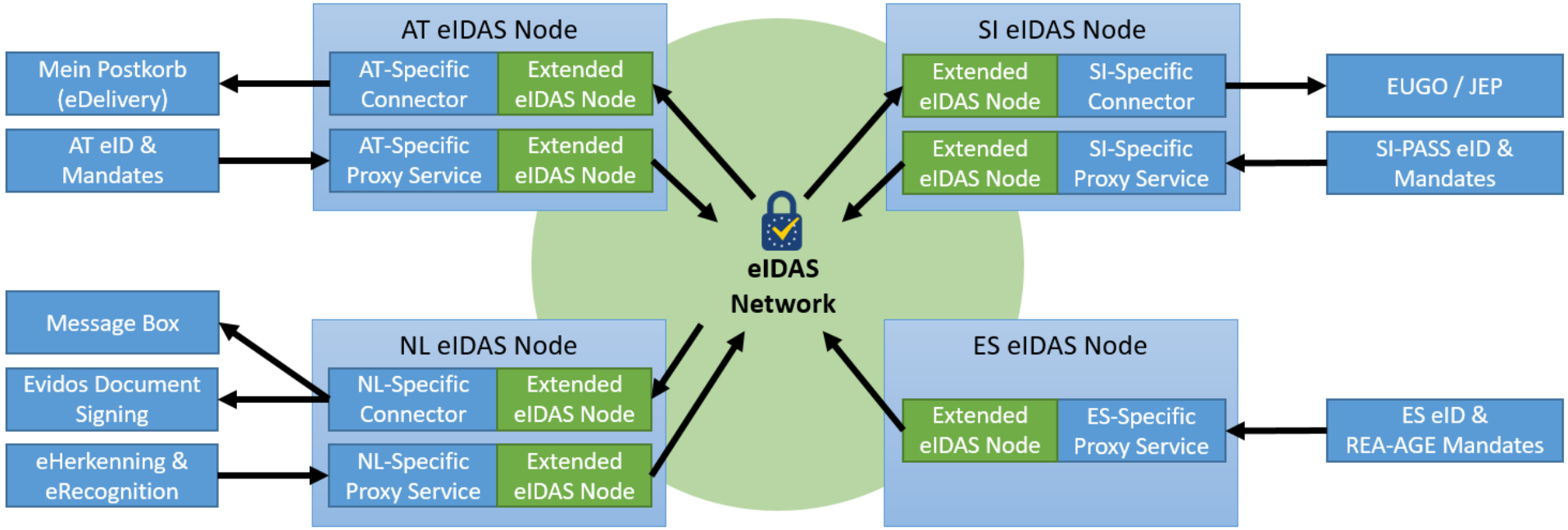
- Person
  - Person types allowed
  - Requested eIDAS attributes
- Requested Powers of Representation
  - Sources of power allowed
  - Regulated professions allowed
- Scope
  - Full powers
  - Service Catalogue, Harmonised Service
  - Non-Harmonised Service, Member State, Service Provider, Procedure, Type of Procedure

Powers validation declaration:

- Representative
- Represented person
- Intermediary person
- Powers of Representation
  - Validation result
  - Source of power
  - Regulated profession
- Power Use Constraints
  - Constraint, Value

Scope of piloting and limitations

Involved Services and Mandate Systems



Piloting eServices

- AT: Electronic delivery
- SI: Slovenian Business Point
- NL: Message Box for Businesses,
  Evidos signing service,
  Demo portal

Mandate Management Systems

- AT: Online Mandate System
- SI: Central eMandate Platform (CeP)
- ES: Public Administration Registry of e-Mandates (REA-AGE)
- NL: eHerkenning (eRecognition)

Scope and limitations to piloting

- SEMPER will **pilot public services only**.
  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.
- SEMPER will pilot with **natural persons representing legal persons only**.
  Piloting natural persons representing other natural persons are out of scope.
- chained mandates are out of scope as well, so the **intermediary** element will **not be piloted**.
- 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.
- the pilots will **not include regulated professions** as a source of powers.
- SEMPER will **only use harmonised services** to express powers. The method ‘non-harmonised’ is not part of the pilot.
- the pilots will **only validate the baseline scenario**.
  Alternative scenarios (including powers to delegate) are outside the scope of the pilots.

SEMPER Demo Videos

Questions?

Participants

- Graz University of Technology (AT)
- Ministerio de Asuntos económicos y transformación digital (ES)
- Ministry of Public Administration (SI)
- Rijksdienst voor Ondernemend Nederland (NL)

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.

Annex:
Extension of eIDAS Node Reference Implementation

Extending the eIDAS Node Reference Implementation

- eIDAS Node v2.3.1 as code base
- Generic Part of reference implementation – suitable for extensibility due to SAML Extensibility Points
  - Custom (SEMPER) Protocol Processor to handle custom (SEMPER-specific) extensions and Light <-> SAML conversions
- MS specific part -> needs a generic extension
  - Similar approach to the generic part for supporting extension without altering Light DTOs
  - New element `additionalProperties` with relaxed processing added to `LightRequest` and `LightResponse` DTOs

Extending the eIDAS SAML Authentication Request

- Power of Representation Requirements
  - `<por:RepresentationRequirements>` element under `<saml2p:Extensions>`

```
<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>
```

Extended eIDAS SAML AuthnRequest

- Requested Represented, Representative, Intermediary Attributes

```
<saml2p:Extensions>
    …
  <eidas:RequestedAttributes>
    <eidas:RequestedAttribute

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

Extended eIDAS SAML AuthnRequest

- Additional Representation Attributes

```
<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/RegulatedProfession"
            FriendlyName="RegulatedProfession"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            isRequired="false" />
…
```

Extending the eIDAS SAML Authentication Response

- Represented, Representative, Intermediary Attributes

```
<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>
```

Extended eIDAS SAML AuthnResponse

- Status, Error Code

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

- Powers of Representation Additional Attributes
  - Source, Regulated Profession

```
<saml2:Attribute FriendlyName="PoRSource"
    Name="http://eidas.europa.eu/attributes/PoR/PoRSource"
    NameFormat="urn:oasis:names:tc:saml2:2.0:attrname-format:uri">
    <saml2:AttributeValue xsi:type="por:PoRSourceType">
            Regulated Profession
    </saml2:AttributeValue>
</saml2:Attribute>

<saml2:Attribute FriendlyName="RegulatedProfession"
    Name="http://eidas.europa.eu/attributes/PoR/RegulatedProfession"
    NameFormat="urn:oasis:names:tc:saml2:2.0:attrname-format:uri">
    <saml2:AttributeValue xsi:type="por:RegulatedProfessionType">
            Notary
    </saml2:AttributeValue>
</saml2:Attribute>
```

Extended eIDAS SAML AuthnResponse

- Power of Use Constraints – <Constraint, Value> list

```
<xsd:complexType name="PowerUseConstraintStructuredType">
    <xsd:sequence>
        <xsd:element name="ConstraintName" type="xsd:string"
                  minOccurs="0" maxOccurs="1" />
        <xsd:element name="ConstraintValue" type="xsd:string"
                  minOccurs="0" maxOccurs="1" />
    </xsd:sequence>
</xsd:complexType>
<xsd:simpleType name="PowerUseConstraintType">
    <xsd:annotation>
              <xsd:documentation>
           Constraint as a base64 encoded string.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:restriction base="xsd:string" />
</xsd:simpleType>
```

Extended SAML Metadata Files

- Power Source, Regulated Profession, Power Use Constraints Attributes

```
<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" />
```