D3.4 Semantic Framework – Final Version

Document Identification			
Status	Final	**Due Date**	31/12/2021
Version	1.0	**Submission Date**	28/02/2022

Related WP	WP3	**Document Reference**	D3.4
Related Deliverable(s)	D2.4, D3.2, D3.3, D3.5 D3.6	**Dissemination Level (*)**	PU
Lead Participant	IHU	**Lead Author**	C. Berberidis (IHU)
Contributors	T. Karunaratne, E. Kontopoulos (SU); A.-R. Guzmán (MTFP-SGAD); Slavko Žitnik, Dejan Lavbič (SI-MPA) S.-Iftikhar. H Shah, E. Kapantai, I. Konstantinidis (IHU)	**Reviewers**	Alberto Crespo (ATOS)
			Miha Jesenko (SI-MPA)

Keywords:
semantic framework, data model, ontologies, semantic assets, information desk, semantic mapping, evidence modelling, canonical evidence, information exchange, access authorization

Document Information

List of Contributors	
Name	Partner
Christos Berberidis	IHU
Syed Iftikhar H. Shah	IHU
Ioannis Konstantinidis	IHU
Eleni Kapantai	IHU
Thashmee Karunaratne	SU
Efstratios Kontopoulos	SU
Ana-Rosa Guzman	MTPF-SGAD
Slavko Žitnik	SI-MPA
Dejan Lavbič	SI-MPA

Document History			
Version	Date	Change editors	Changes
0.1	20/10/2021	IHU	Initial version of document
0.2	02/12/2021	IHU	2nd version of the document (structure of the document outline)
0.3	27/01/2021	IHU, SI-MPA, SU, MTFP-SGAD	3rd version of the document (main content of the document has included by all contributors)
0.4	02/02/2022	IHU, SI-MPA, SU, MTFP-SGAD	Internal revision of chapters 1-4
0.5	04/02/2022	IHU, SI-MPA, SU, MTFP-SGAD	Internal revision of chapters 5 & 6
0.6	07/02/2022	IHU	Submission for initial review
0.7	23/02/2022	IHU, SI-MPA, SU, MTFP-SGAD	Document after 1st reviewer's comments
0.8	25/02/2022	IHU, SI-MPA, SU, MTFP-SGAD	Document after 2nd reviewer's comments
0.9	28/02/2022	Julia Wells (Atos)	Quality check for Submission
1.0	28/02/2022	Ana Piñuela (Atos)	Final for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Christos Berberidis (IHU)	25/02/2022
Quality manager	Julia Wells (ATOS)	28/02/2022
Project Coordinator	Ana Piñuela Marcos (ATOS)	28/02/2022

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
ABAC	Attribute-Based Access Control
AC	Authorization Controller
ADMS	Asset Description Metadata Schema
API	Application Programming Interface
BRIS	Business Registers Interconnection System
CAAR	Cross-border Access Authorization Registry
CBAC	Claims-Based Access Control
CCCEV	Core Criteria and Core Evidence Vocabulary
CEF	Connecting Europe Facility
CERB	Criterion & Evidence Type Rule Base
CLV	Core Location Vocabulary
CPOV	Core Public Organization Vocabulary
CPSV	Core Public Services Vocabulary
CPSV-AP	Core Public Services Vocabulary - Application Profile
CPV	Core Person Vocabulary
DAC	Discretionary Access Control
DBA	Doing Business Abroad – one of the three DE4A pilots
DC	Data Consumer
DCAT	Data Catalog Vocabulary
DE	Data Evaluator
DE4A	Digital Europe for All
DE4ASem	DE4A Semantic framework
DO	Data Owner
DP	Data Provider
DR	Data Requester
DSD	Data Services Directory
DSI	Digital Service Infrastructure
DT	Data Transferor
Dx.y	Deliverable number y, belonging to WP number x
EB	Evidence Broker
EBSI	European Blockchain Services Infrastructure
EC	European Commission
EDCI	Europass Digital Credentials Infrastructure
EDM	Exchange Data Model

Abbreviation / acronym	Description
EESSI	Electronic Exchange of Social Security Information
eID	Electronic Identification
eIDAS	Electronic Identification and Signature (EU regulation)
EIF	European Interoperability Framework
EIRA	European Interoperability Reference Architecture
ESL	Evidence Service Locator
FOAF	Friend of a Friend (ontology)
GBAC	Graph-Based Access Control
HEI	Higher Education Institution
IAL	Issuing Authority Locator
IDK	Information Desk
IEM	Information Exchange Model
IHU	International Hellenic University
IM	Intermediation Pattern
IOP	Interoperability
ISA2	Interoperability solutions for public administrations, businesses and citizens
JSON	JavaScript Object Notation
LAU	Local Administrative Units
MA	Moving Abroad – one of the three DE4A pilots
MAC	Mandatory Access Control
MIME	Multipurpose Internet Mail Extensions
ML	Machine Learning
MOR	Multilingual Ontology Repository
MVP	Minimum-Viable-Product
NACE	Nomenclature of Economic Activities
NUTS	Nomenclature of territorial units for statistics
OOP	Once-Only Principle
OOTS	Once-Only Technical System
OWL	Web Ontology Language
PKI	Public Key Infrastructure
PSA	Project Start Architecture
RDF	Resource Description Framework
RDFS	Resource Description Framework Schema
RPAM	Representation Powers and Mandates (ontology)
SA	Studying Abroad – one of the three DE4A pilots
SCOOP4C	Stakeholder Community Once-Only Principle for Citizens

Abbreviation / acronym	Description
SDG	Single Digital Gateway
SDGR	Single Digital Gateway Regulation
SEMIC	Semantic Interoperability Centre Europe
SKOS	Simple Knowledge Organization System
SML	Service Metadata Locator
SMP	Service Metadata Publisher
SP	Service Provider
TL	Task Leader
TOOP	The Once-Only Principle Project
U	User
UC	Use Case
UML	Unified Modeling Language
URN	Uniform Resource Name
USI	User-Supported Intermediation pattern
UUID	Universally Unique Identifier
VC	Verifiable Credential (pattern)
W3C	World Wide Web Consortium
WP	Work Package
WPL	Work Package Leader
XML	Extensible Markup Language
XSD	XML Schema Definition

Glossary

Term	Explanation
Application Profile	An application profile (AP), as yet another group of assets within the 'models' category, describes how a standard is to be applied in a particular domain or application. Standards typically do not contain constraints such as cardinality; these constraints are defined in the application profile. An application profile only applies to the specified domain [34]
Controlled Vocabulary	Controlled vocabularies provide a consistent way to describe data. They are standardized and organized arrangements of words and phrases presented as alphabetical lists of terms or as thesauri and taxonomies with a hierarchical structure of broader and narrower terms [35].
Code Lists	Predefined set of terms from which some statistical coded concepts take their values [36].
Canonical Evidence	Structured data model that includes a common set of attributes associated with the evidence type and which can be provided by the corresponding lawfully issued evidences [2].
Competent Authority	Any Member State authority or body established at national, regional or local level with specific responsibilities relating to the information, procedures, assistance and problem-solving services covered by this Regulation [37].
Certificate	A document certifying the truth of something.
Criteria	Procedural requirements as conditions to be met and used as a basis for making judgements or decisions in the procedure.
Data Model	A collection of entities, their properties and the relationships among them, which aims at formally representing a domain, a concept or a real-world thing. It includes core vocabularies [38].
eDelivery	eDelivery helps public administrations to exchange electronic data and documents with other public administrations, businesses and citizens, in an interoperable, secure, reliable and trusted way [39].
Electronic Evidence	Lawfully issued evidence by competent authorities ranging from completely unstructured formats (such as pdf or picture formats) to structured formats (e.g. XML).
Event	In general, an event is something that happens. It is an arbitrary classification of a space/time region, by a cognitive agent. An event may have actively participating agents, passive factors, products, and a location in space/time. For example in computer coding, an event is when something happens that triggers the code to run.
Evidence	Any document or data, including text or sound, visual or audiovisual recording, irrespective of the medium used, required by a competent authority to prove facts or compliance with procedural requirements referred to Article 2.2.b (SDGR) [37].
Evidence Type	It may be seen as a dataset according to an agreed common data model that is composed of complex or simple data elements.
Information Desk	A central system that provides evidence metadata to parties in order to make the direct exchange of Evidence between Data Provider (DP) and Data Consumer (DC) possible [39].

Term	Explanation
Legal Entity	An association, corporation, partnership, proprietorship, trust, or individual that has legal standing in the eyes of law.
Once Only Principle	The once-only principle is one of the seven underlying principles of the EU eGovernment Action Plan 2016-2020. It means that public administrations should ensure that citizens and businesses supply the same information only once to a public administration. Public administration offices take action if permitted to internally re-use this data, in due respect of data protection rules, so that no additional burden falls on citizens and businesses [41].
Ontology	An ontology is a formal, explicit specification of a shared conceptualisation. In computer science and information science, an ontology encompasses a representation, formal naming and definition of the categories, properties and relations between the concepts, data and entities that substantiate one, many or all domains of discourse [42].
Person, Legal	A legal person is a registered organization, having its registered office in a Member State.
Person, Natural	A natural person is a citizen of the Union or a human residing in a Member State [43].
Procedure	a sequence of actions that must be taken by users to satisfy the requirements, or to obtain from a competent authority a decision, in order to be able to exercise their rights as referred to in point (a) of Article 2(2) [37].
Procedure Category	Category of procedures according to the codes provided by the Commission for the areas and subareas of the SDGR Annex I, life events and procedures of the SDGR Annex II, and for the directives mentioned in SDGR Article 14.
Proof	1.Fact or piece of information that shows that something exists or is true [44], 2. a) something that induces certainty or establishes validity (Merriam-webster) b) evidence operating to determine the finding or judgment of a tribunal [45].
Public Service	The concept of public service is twofold: it embraces both the bodies providing services and the services of general interest they provide. Public service obligations may be imposed by the public authorities on the body providing a service (airlines, road or rail carriers, energy producers and so on) either nationally or regionally [46].
Scenario	One typical way in which a system is used or in which a user carries out some activity [43].
Semantic Agreement	Serves to determine -per canonical evidence- what standard fact is proven and what set of attributes compose the canonical evidence (considering the attributes used to prove such fact in each country) and how these attributes are codified for language neutrality and, where applicable, using labels in the official languages of the issuing countries. Semantic agreements should be defined by business-domain experts with the help of semantic experts.
Semantic Asset	A specific type of standard which involves highly reusable metadata (e.g. xml schemata, generic data models) and/ or reference data (e.g. code lists, taxonomies, dictionaries, vocabularies).
Taxonomy	A systematic arrangement in groups or categories of concepts according to established criteria [47].

Term	Explanation
TOOP	The Once-Only Principle Project (TOOP) was launched by the European Commission in January 2017 as an initiative of about 50 organizations from 20 EU Member States and Associated Countries. The main objective of TOOP is to explore and demonstrate the once-only principle across borders, focusing on data from businesses. Doing this, TOOP wants to enable better exchange of business-related data or documents with and between public administrations and reduce administrative burden for both businesses and public administrations [48].
Use case	A specification of one type of interaction with a system. One use case may involve several scenarios (usually a main success scenario and alternative scenarios) [43].
User	User is anyone who is a citizen of the Union, a natural person residing in a Member State or a legal person having its registered office in a Member State, and who accesses the information, the procedures, or the assistance or problem-solving services, referred to in Article 2(2), through the gateway [37] .
Vocabulary	A collection of terms for a particular purpose. Vocabularies can range from simple, such as the widely used RDF schema, FOAF and DCMI element set, to complex vocabularies with thousands of terms, such as those used in healthcare to describe symptoms, diseases and treatments. Vocabularies play a very important role in linked data, specifically to help with data integration. For example, metadata vocabulary. The use of this term overlaps with that of 'ontology' within the scope of computer and information sciences [49].

Executive Summary

This document is the final version of the DE4A semantic framework produced in the context of Task 3.2 "Design of the semantic interoperability framework" in "WP3 Semantic Interoperability Solutions". This framework sets the basis for semantic interoperability needed for evidence exchanges at a pan-European level of public service provision. This document along with the deliverable D3.2 "*Final Requirements for Semantic Assets*" serves as the key design guidelines for the implementation of the DE4A Semantic toolkit (D3.6 *"Semantic Toolkit – Final version"*).

The previous version of the subject deliverable (D3.3 *"Semantic Framework-Initial version"*) mostly identified the needs for the implementation, based on which the initial version of the D3.5 *"Semantic Toolkit – Initial Version"* was produced. D3.6 *"Semantic Toolkit – Final version"* clearly updates the tools and lists only the ones that are necessary to build semantic resources and were also used during the project. There is a clear distinction between initial (D3.3 *"Semantic Framework-Initial version"*) and final version (*D3.4 "Semantic Framework-Final Version"*)-current document- of semantic framework in the table below:

Table 1: Overview of initial and final versions of Semantic Framework

Semantic Framework - Initial Version (D3.3)	Semantic Framework - Final Version (D3.4)
General description of evidence modelling approach and use of semantics.	Description of proven approach for evidence modelling, which is updated according to real-case scenarios used within DE4A.
Identification of relevant semantic assets and identification of the needs for the DE4A pilots.	Presentation and definition of modelled evidence types - 10 models.
Initial definition of Information Desk, along with semantic assets and identified main components.	Description of built Information Desk along with defined components. Information Exchange Model definition that supports communication and exchange of evidences.

The initial version of the document (D3.3 *"Semantic Framework-Initial version"*) outlined the semantic framework (**Information Desk**, **Information Exchange Model**, and **pilot-specific data models**) and reviewed all the relevant semantic assets that were used for development of semantic resources and technologies.

The Information Desk (IDK) offers information to the Data consumer (DC), and the Data Provider (DP) that is required for smooth cross-border exchange of evidence in the context of DE4A. The IDK consists of the following core components: the **Issuing Authority Locator** (IAL) that helps the DC to find out the issuing authority that can provide the required canonical evidence within a particular country, the **Evidence Service Locator** (ESL) that helps the DC to locate the evidence service to request a canonical evidence to a particular issuing authority, the **Cross-border Access Authorisation Registry** (CAAR) that helps the DP to check if the request has the required authorization, the **Multilingual Ontology Repository** (MOR**)** that helps to understand the meaning of canonical evidence attributes and, specifically, helps the Preview Component to show the user the evidence data along with their corresponding labels in the language chosen by the user to interact with the portal, and the **Authorization Controller** (AC) that contains Authorities Editor and manages the consultation between Data Evaluator and Data Owner when requesting evidence data.

The Information Exchange Model (IEM) provides the specification of the messages to be exchanged between competent authorities that include metadata and evidence data as payload. IEM is agnostic to any technical implementation and according to the DE4A project specific pilot needs and

architecture. The second iteration of the IEM supports all the updated information flows and canonical evidence interchange.

WP3 provides data models for the DE4A pilots' domain-specific information needs. The evidence data models are defined based on these data models. Ten evidence types have been designed in DE4A. They are the following: Birth Evidence, Marriage Evidence, Domicile Registration Evidence, Pension Means of Living Evidence, Unemployment Means of Living Evidence, Working Life Means of Living Evidence, Higher Education Diploma Evidence, Secondary Education Completion Evidence, Non Academic Information Evidence, and Company Registration Evidence.

1 Introduction

1.1 Purpose of the document

The purpose of this document is to present the final design of the DE4A semantic interoperability framework (DE4A Sem) for the delivery of integrated cross-border public services.

Towards this purpose, relevant efforts like TOOP project and initiatives like SDG, ISA[2] and eIDAs are considered. Moreover, existing infrastructures and standard approaches in the EU context that facilitate access to information have been taken into account. One key aspect of the DE4A approach is **reusability**, thus the semantic framework will reuse relevant metadata efforts (e.g., EDCI data model) as well as central components and services from other initiatives (e.g., DSD, Evidence Broker) and will attempt to link those with the needs and requirements identified by other work packages within DE4A. Consequently, the work and scope of this deliverable is taking into consideration the following dimensions:

▸ The three DE4A cross-border pilots
▸ The WP2 Project Start Architecture (PSA)
▸ The SDG OOP Architecture

The DE4A Semantic framework (DE4A Sem) focuses on two aspects of semantic interoperability:

▸ to safeguard that the correct semantics of exchanged data and information is preserved and understood throughout exchanges between EU Member States needed to deliver integrated cross-border public services. The disclaimer is that these data models are dedicated to the ones promoted and used by the three DE4A pilots. Towards this direction it is worth mentioned the close collaboration with SEMIC SDG-OOP WP4 - Data Semantics, Formats & Quality [1] in refining the common data formats for the evidence types.

▸ to provide the central components of the Information Desk (IDK), which offers information to Data Consumers and Data Providers that is required for smooth cross-border exchange of evidence in the context of DE4A. As described in deliverable D2.4 *"Project Start Architecture"*[2], there are two approaches for mapping between domestic and cross-border evidence: criteria-based and evidence-based. The DE4A Semantic Framework considers both approaches. However, according to the DE4A pilot needs, the criteria-based approach is not needed in the scope of the project.

The process for the design of the semantic framework has been the following:

▸ First, having thoroughly investigated in deliverable D3.3 *"Semantic Framework-Initial version"* [3] the existing data models, controlled vocabularies, services, EU infrastructures (e.g., eID, eIDAS), metadata efforts, and IT systems for evidence exchange that apply standards from relevant bodies (e.g., ISA[2] and W3C) and core public service vocabularies that facilitate the access to information, the project presented the semantic assets that were considered in alignment with DE4A pilots.

▸ Second, in order to link this work to other DE4A Workpackages, the project studied and detailed evidence modelling of the three DE4A pilots. From these pilots, WP3 analysed the required data and mapped the relevant attributes with standard vocabularies, resulting in a design of a holistic common data model per DE4A pilot. As a next step, the fields of each data model were combined with the requirements specified in deliverable D3.2 *"Requirements for Semantic Assets"*.

▸ Last, apart from the common evidence data models, the DE4A semantic framework also covers the Information Desk and Information Exchange Model components. The following TOOP components [4] and some relevant components of SDG OOTS architecture and their information models were considered in terms of IDK and IEM: TOOP DSD, TOOP RoA, CERB.

It should be mentioned that the output of this deliverable will serve as the groundwork for the deliverable D3.6 *"Semantic Toolkit – Final Version"*, which covers the implementation of the semantic tools. More specifically, the semantic framework comprises the conceptual representation of the DE4A data models and identifies the vocabularies to be reused and extended. This information will be used

as input in D3.6 *"Semantic Toolkit – Final Version"*, for developing the semantic components and the final serialisations of the data models with the related data types introduced in the vocabularies and with any additional custom DE4A data type.

1.2   Structure of the document

This deliverable is structured as follows:

▸ **Chapter 2** presents an overview of the DE4A Semantic framework (DE4ASem) core components along with the semantic assets with relevance to DE4A pilots that were used.

▸ **Chapter 3** presents the approach to define DE4ASem, covering the process of the evidence modelling of common data models along with the semantic assets adoption methodology and the multilingual description of evidences.

▸ **Chapter 4** describes the Pilot-related canonical evidences. The appropriate fields of each evidence type are presented here based on their common data models, along with definitions, data types, and a cross-reference to the respective (non)-functional requirements specified in D3.2 *"Requirements for Semantic Assets"*.

▸ **Chapters 5 and 6** present the Information Desk (IDK) and Information Exchange Model (IEM), respectively.

▸ **Chapter 7** describes the conclusions.

2 Overview of DE4ASem and Semantic Assets

This chapter presents an overview of the semantic assets reused in relation to the DE4A pilot use cases followed by the semantic components that compose the DE4ASem Framework.

2.1 DE4A Semantic Assets

Table 2: List of assets with semantic relevance to DE4A

Assets with semantic relevance	Description
Core Person Vocabulary	Captures the fundamental characteristics of a person, e.g., name, gender, date of birth, location [5]
Core Business Vocabulary	Captures the fundamental characteristics of a legal entity (e.g., its identifier, activities) which is created through a formal registration process, typically in a national or regional register [6].
Core Location Vocabulary	Captures the fundamental characteristics of a location, represented as an address, a geographic name or geometry [7].
Core Public Organisation Vocabulary	Describes public organisations in the European Union [8].
Core Criterion and Core Evidence Vocabulary	Supports the exchange of information between organisations that define criteria and organisations that respond to these criteria by means of evidence [9].
DCAT-AP	The DCAT Application Profile for data portals in Europe (DCAT-AP) is a specification based on W3C's Data Catalogue vocabulary (DCAT) for describing public sector datasets in Europe. Its basic use case is to enable a cross-data portal search for data sets and make public sector data better searchable across borders and sectors [10].
ADMS-AP	ADMS-AP is a specification used to describe interoperability solutions helping everyone to search and to discover them [11]. ADMS-AP is used to describe the identifier of resources for all DE4A pilots.
BRegDCAT-AP	An extension of the DCAT application profile for base registers, aiming to provide a standard data model / specification for base registries access and interconnection, thus to facilitate Member States (MSs) work on the creation of their own Registry of Registries. [12].
ROV	The Registered Organization Vocabulary (ROV) is a vocabulary for describing organizations that have gained legal entity status through a formal registration process, typically in a national or regional register [13]. It focuses solely on such organizations and excludes natural persons, virtual organizations and other types of legal entity or 'agent' that are able to act. It is a profile of the more flexible and comprehensive Organization Ontology [14].
TOOP Criterion & Evidence Type Rule Base (CERB)	The CERB is a central authoritative system that maps specifics sets of Data as Evidence that prove specific requirements. DE4A's proposed component "Issuing Authority Locator" (described at

Assets with semantic relevance	Description
	forthcoming section) of the Information Desk is partially inspired by the TOOP CERB and its purpose is to find out the issuing authority that can provide the required evidence within a particular country by adapting this according to the requirements of DE4A pilot use cases. Additionally, in SDG OOTS, this semantic asset is known as Evidence Broker. [15].
TOOP DSD	The TOOP Data Services Directory (DSD) is a central service of the TOOP solution architecture that holds a catalogue of Data Providers with the Datasets they are capable to offer upon request [16]. It is utilized in the Evidence Exchange Process by the Data Consumers to find out the Data Providers that can give the evidences they require. TOOP DSD consists of the following classes: dataset, distribution, data service, data provider, address, and catalogue. DE4A took inspiration from the said semantic asset in terms of Information Desk (IDK) component.
TOOP EDM	The TOOP Exchange Data Model (EDM) specification describes the process of exchange of evidences, which can be concepts or documents. This information model consists of two different types of messages: the TOOP request message and the TOOP response message. While the TOOP request enables DCs to initiate concept and document queries to the DPs, the TOOP response provides the possibility to return the concrete concept values and document metadata that were requested [17]. After careful investigation and analysis of the TOOP EDM it was identified that: i) the TOOP EDM is too specific since concentrating on the one and only pilot of the TOOP project and it is not reusable for DE4A pilots and needs; ii) EDM is not use case agnostic and sufficiently abstract. DE4A's proposed semantic asset Information Evidence Model (IEM) is different from TOOP EDM to accommodate both DE4A architecture and pilots' specificities.
TOOP RoA	Registry of Authorities (RoA) is a TOOP core service that maintains a catalogue of Data Consumers with the Procedures they are able to execute [18]. The service is used by the Data Providers in the Member States which are required to determine whether a particular public administration in another Member State is allowed to ask for a certain requested type of evidence in a particular context. RoA facilitates this by listing, for public administrations in EU Member States, the procedures for which these administrations are authorized to request which types of evidence.
	In DE4A, the Cross-border Access Authorization Registry (CAAR), as a part of IDK, is also inspired from the said semantic asset. Moreover, the CAAR stores access authorizations registered by the corresponding data owners to access their provisions. It helps to represent multi/bilateral agreements with Data Owner authorities for accessing their evidences or by-law authorisations. The detailed explanation of the CAAR component is mentioned in the chapter 5 of this document.

Assets with semantic relevance	Description
Verifiable Credentials	Credentials are a part of our daily lives; driver's licenses are used to assert that people can operate a motor vehicle, university degrees can be used to assert our level of education, and government-issued passports enable us to travel between countries. It describes a data model for a digital entity profile and a collection of digital entity credentials that assert verifiable claims about that entity profile [19], [20].
EDCI	European Commission, Directorate-General for Education, Youth, Sport and Culture (DG EAC) is emerging a Europass framework for digitally signed credentials intended at fostering the implementation of verified, trustworthy digital certificates, and at encouraging the recognition of qualifications, competences and skills acquired [21]. Europass Digital Credentials Infrastructure (EDCI) is a set of standards, services and software that permits institutions to issue digital, tamperproof qualifications and other learning credentials within the European Education Area. The EDCI Data Model is an extension of the W3C Verifiable Credentials Data Model [20]. Europass and EDCI data model can constitute the basis for describing the concepts of higher and secondary education, while providing the necessary credentials for certifying the evidences related to the domain of education. These concepts will be used by the Diploma/Certs/Studies/Professional Recognition use case of the pilot "Studying abroad".
SDG evidence data models	The SDG OOP Data Semantics, Formats and Quality Working Group [1]is in the process of developing common data models for different evidence types (e.g., birth certificate, marriage certificate) that best serve the interests of the SDG regulation and the Member States (MS).
ISA2 models for multilingual public documents	Regulation (EU) 2016/1191 of the European Parliament and of the Council of 6 July 2016 on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents in the European Union and amending Regulation (EU) No 1024/2012 aims to simplify the circulation of certain public documents between Member States. It applies to public documents issued by the authorities of a Member State that need to be presented to the authorities of another Member State. The Regulation abolishes the apostille requirement and simplifies formalities with regards to certified copies and translations. ISA2 has provided XML Schemas for describing these public documents in a structured format. DE4A has reused these XML Schemas, and SDG data models and extended them according to the DE4A pilot requirements.

2.2 Framework Overview

The DE4A semantic framework is a general framework for the semantically interoperable, cross-border, once-only principle implementation that capitalizes on available semantic standards. At the

heart of this framework lies the "Information Desk", which constitutes a catalogue of semantic assets for facilitating the exchange of information between cross-border, public authorities. For the optimal automated exchange of information every single link in the chain of interoperability must function correctly to achieve sufficient and correct information exchange among European Member States.

This section presents an overview of the semantic components and services of the DE4A semantic framework along with the semantic assets that were considered and reused for delivering cross-border public services related to the DE4A pilot use cases. Towards this perspective, the inputs from D3.2 *"Requirements for Semantic Assets"* and D3.3 *"Semantic Framework-Initial version"* [3]were utilized and, more specifically, the semantic assets that were defined in respect to D3.2 *"Requirements for Semantic Assets"* and the identified infrastructure and models that facilitate the access to information in terms of D3.3 *"Semantic Framework-Initial version"*. The following table connects the semantic assets that were used in terms of DE4ASem to describe the main actors, concepts and events of DE4A architecture components.

Table 3: Mapping of assets with semantic relevance with the DE4ASEm core components

DE4ASem Components		Semantic Assets
Canonical Evidence Type		
	Studying Abroad Pilot Canonical Evidence Types	CCCEV, EDCI, Codelists (Country, Main field of study, mode of study, Currency)
	Moving Abroad Pilot Canonical Evidence Types	CPV, CLV, CPOV, SDG WP4 data models, Codelists (Cause of end of marriage, Marital status, Country, Human Sex, NUTS/LAU, Currency), ISA^2 models for multilingual public documents
	Doing Business Abroad Pilot Canonical Evidence Types	CCCEV, Codelists (Country, NUTS/LAU, Company type, Company status, Company activity, Language Code)
Information Desk (IDK)		
	Information Authority Locator (IAL)	CERB, CPSV-AP, ISA2 Core Vocabularies, NUTS/LAU
	Evidence Service Locator (ESL)	TOOP DSD (BRegDCAT-AP), CPSV-AP, ISA2 Core Vocabularies
	Cross-border Access Authorization Registry (CAAR)	TOOP RoA
	Multilingual Ontology Repository (MOR)	Multilingual standard forms for public documents, TOOP Semantic Repository
Information Exchange Model (IEM)		TOOP EDM, eIDAS Profiles

The additional information about the code lists will be explained in the deliverable D3.6 *"Semantic Toolkit – Final Version"*.

3 Evidence Modelling

This section establishes the background for modelling evidence, starting with the adopted approach within DE4A for designing and implementing the canonical evidence data models, followed by the adopted criteria for selecting relevant semantic assets during the modelling process. Finally, the approach for modelling multilingual evidence is presented.

3.1 Evidence Modelling Approach

In the approach for designing and implementing the DE4A canonical evidence data models, DE4A adopts the following steps, as also illustrated in the diagrammatic overview in the figure below. Identification of mandatory and optional data for the canonical evidence types based on semantic requirements from the deliverable D3.2 *"Requirements for Semantic Assets"* and consulting with the related MS.

1. Identification of mandatory and optional data for the canonical evidence types based on semantic requirements from D3.2 *"Requirements for Semantic Assets"* and consulting with the related MS.

2. Selection of relevant semantic assets identified in D3.2 *"Requirements for Semantic Assets"* that can be reused and extended for the DE4A semantic framework. As there are ongoing efforts on related initiatives more semantic assets could be identified.

3. Creation of conceptual models for each use case canonical evidence from step 1 based on the concepts of the ISA^2 Core Vocabularies providing an initial understanding of the pilot required and available data.

4. Mapping the elements of the conceptual models to existing semantic data models (ontology mapping).

5. Mapping element values to controlled vocabularies based on recommended controlled vocabularies with focus on vocabularies from the EU publication office [35] and in case of unavailability agree with the piloting MS on related codelists.

6. Implementation of the canonical evidence data models (serialization of the models, specifications, etc.). For the purpose of the pilots, the data models were implemented in XML Schema format.
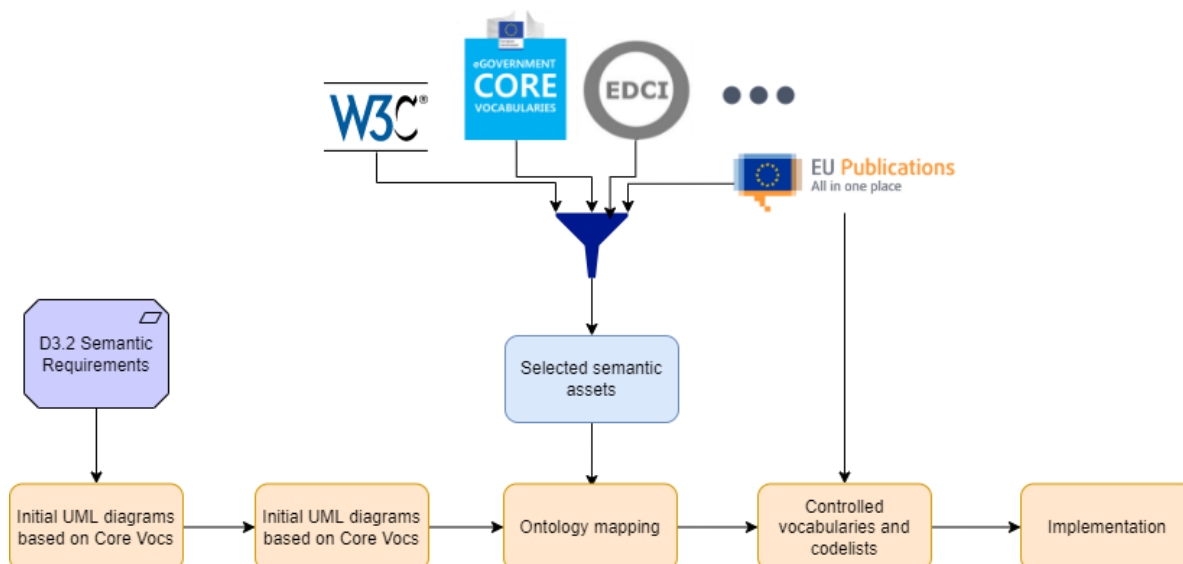
Figure 1: The process of the evidence modelling of common data models

3.2 Semantic Assets Adoption Methodology

The inclusion and exclusion criteria for selecting relevant semantic assets for the canonical evidence types are the following.

▶ Inclusion Criteria

    a. The semantic asset is a vocabulary, ontology, data model or an application profile (e.g., ISA^2 core vocabularies).

    b. The domain of the semantic asset is related to the required attributes based on each pilot use case, i.e., studying abroad, doing business abroad and moving abroad.

    c. The semantic asset is recommended by W3C and EU (e.g., ISA^2 Core Vocabularies).

    d. Consideration of building blocks that include related data models that can be used in the context of DE4A (e.g., EDCI data model).

▶ Exclusion criteria

    a. Assets cover only legal, organizational, and semantical aspects of interoperability of cross-border evidence exchange

3.3 Multilingual Evidence

In the public administration context, evidence is information to legally prove that procedural requirements are met. Because of the required legal value of evidence, the provided information must be expressed in an official language legally recognized by the competent authority of the procedure. It is a problem in a cross-border scenario when evidence is issued in a non-recognised language, not only because of the lack of legal value but also due to lack of correct semantic understanding by both humans and machines.

Traditionally, public administrations resolve this issue for humans by asking the applicant to provide a legal translation of the evidence along with the evidence itself. However, traditional legal translations are not applicable when evidence pieces are automatically exchanged between competent authorities and the multilingual issue needs to be resolved otherwise. Due to their limited accuracy, automatic translations are not a solution at all, so other solutions should be implemented.

When evidence represents written information, such information can be presented as unstructured or as structured data. However, for the collaborative provision of public services in line with the Once-Only principle within the EU, there are semantic agreements for certain evidence types to provide their information in accordance with ad-hoc common data models[1]. Then, per evidence type, evidence pieces as structured data are transformed to the corresponding semantic agreement. Evidence pieces as unstructured data can be accompanied by the equivalent structured data according to such a semantic agreement.

Common data models are composed of sets of attributes with labels that are not expressed in any human-style language, but each label has an agreed meaning known by the machine algorithms that process such information. In this sense, the multilingual issue is reduced to understanding the language in which attribute values are expressed; this issue can be mostly avoided by using standardized lists that are mainly classifications, code lists or dictionaries developed for statistical purposes at European level (Eurostat). For specific-domain concepts, there are international and European standardized lists as well. However, there are some values that cannot be easily standardized because they are peoples' names, or they are old names of places that are not included in the standard lists now. In these cases, the only possible agreement is using a common alphabet to represent the characters.

Nonetheless, automatic processing of evidence is not the only need for the collaborative provision of public services in the EU, because (a) quite often human processing of evidence is required, (b) the exchanged data needs to be re-accessed later for transparency or auditability purposes. When evidence information has to be presented to people (applicants or civil servants), labels and standardised lists need to be translated into a human-understandable language according to the language of the procedure. Most of the standardised lists have an official translation to every European language that can be used in this context, but mostly there are no official translations for attributes of the common data models. Thus, human interfaces need labels in each of the official languages of the EU and, for such a task, the methodology used by the Regulation on Public Documents (Regulation 2016/1191) [22] may serve as a major reference.

The Regulation 2016/1191 methodology is based not only on the agreement of which fields (attributes) can be found in each public document type, but also on the labels of such fields in each of the EU official languages, as well as in the recognition of the legal value of such multilingual labels. In this way, any evidence is expressed in the languages of both the issuing and consuming authorities, with recognised legal value on both sides. However, the legal recognition of these multilingual labels is only aimed to replace the need of legal translations; it is not aimed to provide legal value to the information expressed with such labels. In this sense, Regulation 2016/1191 leaves at the discretion of each Member State either the recognition of the legal value of the agreed multilingual set of attributes or their use as attachment to legal evidence as a replacement of legal translations.

Because the implementation of the Once-Only principle at EU-level mostly requires the agreement on a common data model per evidence type, their attributes can be labelled and defined in each of the EU official languages and the agreement can be extended to recognise such labels and definitions for avoiding legal translations, provided that attribute values do not require translation (e.g., standardised lists and proper names). The recognition of information expressed with such common data models as evidence of legal value can be left at the discretion of each Member State or competent authority; if such legal value is not recognised, then the evidence with legal value has to be attached and the information expressed accordingly to the multilingual common data model is aimed only to replace the need of legal translations. Besides, the multilingual labels of the issuing and consuming authorities may be used to show the information to users and civil servants with equivalent value to legal translations, so applicants save costs and burdens.

---

[1] Efforts already made in key domains are reusable for the definition of canonical evidence types (eJustice, Taxes, Social Security, Education, etc.).

An evidence type may be seen as a dataset according to an agreed common data model that is composed of complex or simple data elements. These data elements are part of some domain-specific or general ontology, and their description is registered with two strings per language, a label and a definition; at least, each data element in any ontology should be defined in English. Besides, data elements might be composed of other data elements. Because data elements that belong to domain-agnostic ontologies might represent different concepts in different evidence types (parent, newborn, spouse, etc.), these concepts can be seen as specialised data elements that are described with their own set of labels and definitions according to their meaning in the associated evidence type. Besides, the same specialised data element might be present in several evidence types, such as "applicant". A visual representation of the subject aspect is mentioned in the figure below:
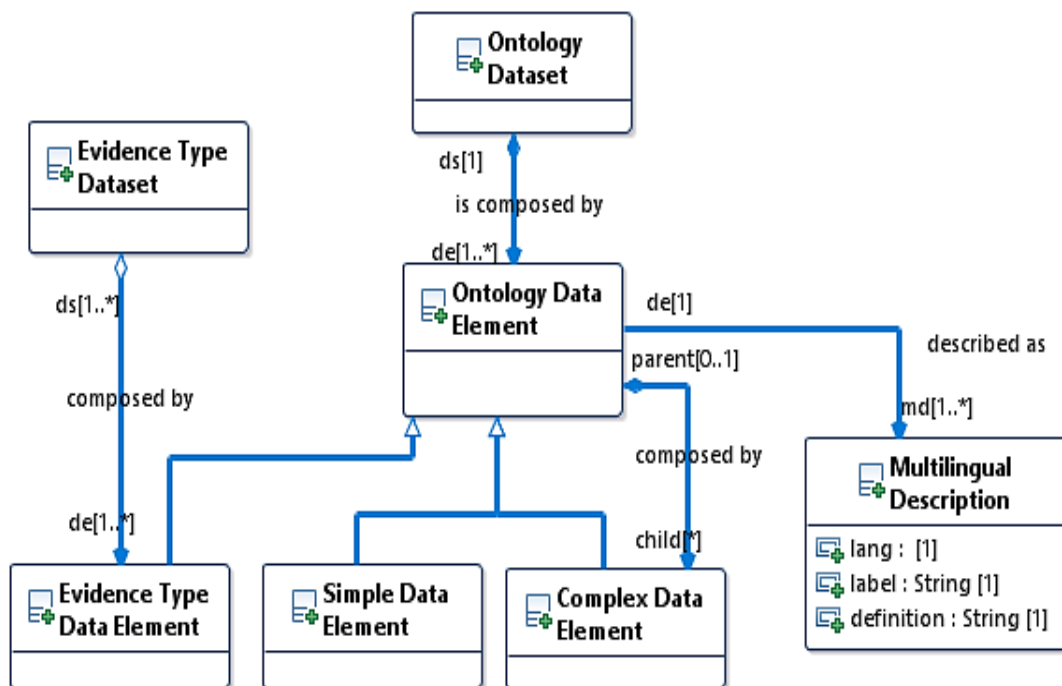
Figure 2: Multilingual description of evidences

In summary, multilingual labels and descriptions are useful for cases from two different points of view:

▶ Purpose:

1. Replacement of legal translations (if required)
2. Human understandability

▶ Functionality:

3. User preview
4. User a posteriori access to exchange data (transparency)
5. Evidence processing by civil servants
6. Procedure processing auditability

4 Canonical Evidence Type

This chapter presents the final design of the data models for representing Canonical Evidence (CE) types for the three DE4A pilots. The below sections describe the appropriate concepts, along with definitions, data types, and a cross-reference to the respective requirements specified in D3.2 *"Requirements for Semantic Assets"*. The actual implementation of the models will be reported in the deliverable D3.6 *"Semantic Toolkit – Final Version"*.

4.1 Moving Abroad Pilot Evidence

4.1.1 Birth Evidence

This type of evidence proves the birth of a child. It is related to DE4A Moving Abroad Pilot (Use Case 2- Request an Extract or Copy of a Birth evidence) and can be used in many public services.
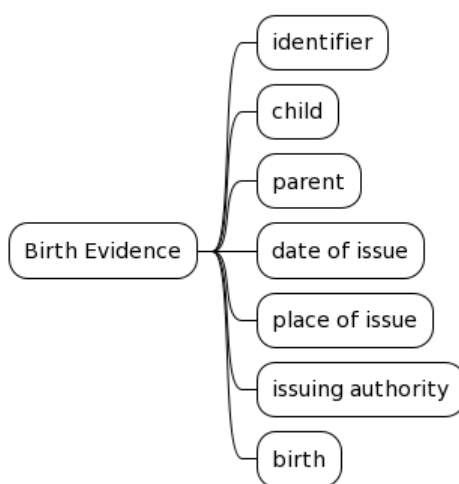
Figure 3:Birth Evidence - fields overview

Table 4: Birth Evidence - fields specification

Field	Definition	Data type	Relevant reqs
identifier	An unambiguous reference to the Birth Evidence.	Identifier	MA-GE-01
child	A Person of any age, who is a son or daughter.	Person (CPV)	MA-GE-02 MA-GE-03 MA-BE-01
parent	One of the two Persons who are jointly the cause of the Child's Birth, i.e., natural parent.	Person (CPV)	MA-GE-02 MA-GE-03 MA-BE-01 MA-BE-02

Field	Definition	Data type	Relevant reqs
date of issue	Date of issue of the certificate	Date (XSD[2])	MA-GE-01 MA-GE-08
place of issue	Place of issue (location) of the certificate	Address (CLV)	MA-GE-01 MA-GE-04 MA-GE-05 MA-GE-06 MA-GE-07
issuing authority	Public Organization with official authority in charge of issuing the certificate	Public Organization (CPOV)	MA-GE-01
birth	The event indicating the moment a Child emerges from the body of another Person, i.e., start of life.	Custom type	MA-BE-01

4.1.2   Marriage Evidence

This type of evidence proves the marriage of two persons. It is related to the DE4A Moving Abroad Pilot Use Case "Request an Extract or Copy of a Civil State Certificate" (UC2) and can be used in many public services.
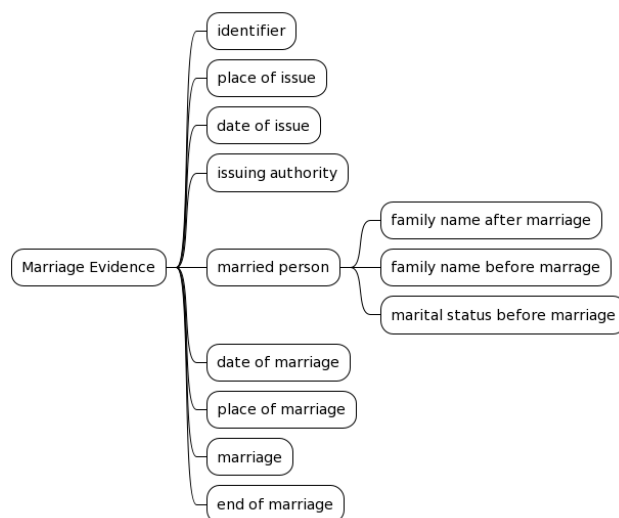
Figure 4: Marriage Evidence - fields overview

Table 5: Marriage Evidence - fields specification

Field	Definition	Data type	Relevant reqs
identifier	An unambiguous reference to Marriage Evidence.	Identifier	MA-GE-01

---

[2] "XSD" stands for the XML Schema Definition

Field	Definition	Data type	Relevant reqs
married person	Person who has entered a marriage	Person (CPV)	MA-GE-02 MA-GE-03 MA-ME-03 MA-ME-05
date of issue	Date of issue of the certificate	Date (XSD)	MA-GE-01 MA-GE-08
place of issue	Place of issue (location) of the certificate	Address (CLV)	MA-GE-01 MA-GE-04 MA-GE-05 MA-GE-06 MA-GE-07
issuing authority	Public Organization with official authority in charge of issuing the certificate	Public Organization (CPOV)	MA-GE-01
family name after marriage	This property contains the family name after the Marriage of the Person.	String (XSD)	MA-ME-03
family name before marriage	This property contains the family name before the Marriage of the Person.	String (XSD)	MA-ME-03
marital status before marriage	Situation with regards to whether a Person was married, unmarried, separated, divorced, widowed, cohabit or polygamous.	Enumeration (EuroVoc-Marital Status)	MA-ME-05
date of marriage	Date on which the marriage took place	Date (XSD)	MA-GE-08 MA-ME-02
place of marriage	The location where the marriage took place	Address (CLV)	MA-GE-04 MA-GE-05 MA-GE-06 MA-GE-07 MA-GE-08 MA-ME-02
marriage	A legally accepted relationship between two Persons in which they live together.	Custom type	MA-ME-01 MA-ME-02
end of marriage	Describes date and cause of end of marriage	Custom type	MA-ME-01 MA-ME-04 MA-ME-05

4.1.3   Domicile Registration Evidence

This type of evidence proves that an individual has successfully completed his/her domicile registration in terms of change of address, to another Member State of EU. Additional information is mentioned in the forthcoming paragraphs.
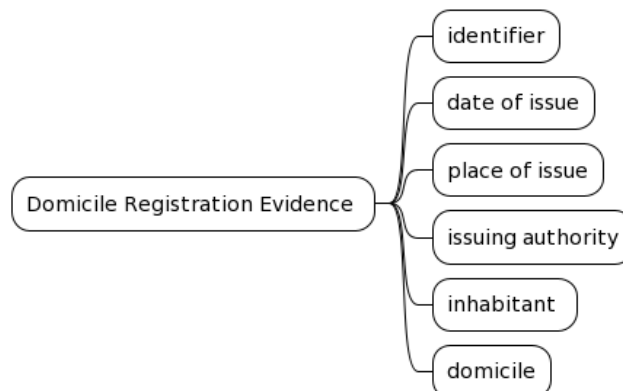
Figure 5: Domicile Registration Evidence - fields overview

Table 6: Domicile Registration Evidence - fields specification

Field	Definition	Data type	Relevant reqs
identifier	An unambiguous reference to the Domicile Registration Evidence.	Identifier	MA-GE-01 MA-DRE-02
date of issue	The most recent date on which the domicile registration evidence instance was issued.	Date (XSD)	MA-GE-01 MA-DRE-02
issuing authority	A public organization with official authority in charge of issuing the domicile registration evidence.	Public Organization (CPOV)	MA-GE-01 MA-DRE-01 MA-DRE-02
place of issue	It indicates the address of respective domicile registration authority	Address (CLV)	MA-GE-01 MA-GE-04 MA-GE-05 MA-GE-06 MA-GE-07 MA-DRE-02
inhabitant	Person, living in the domiciled area i.e., the person who has successfully completed	Person (CPV)	MA-GE-02 MA-GE-03 MA-GE-04 MA-GE-05

Field	Definition	Data type	Relevant reqs
	his/her domicile registration in terms of change of address, in a Member State of EU.		MA-GE-06 MA-GE-07 MA-GE-08 MA-GE-10 MA-DRE-01 MA-DRE-02 MA-DRE-03
domicile	state/country that a person treats as their permanent home, or lives in and has a substantial connection with. It is independent of a person's nationality, and it may change from time to time.	Address (CLV)	MA-GE-04 MA-GE-05 MA-GE-06 MA-GE-07 MA-GE-09 MA-DRE-01 MA-DRE-02 MA-DRE-03

4.1.4   Domicile Deregistration Evidence

Domicile Deregistration is required by some EU Member States as a part of the procedure to register a domicile of a person in another EU Member State. In other words, once the person is registered in his/her new domicile, the country of the previous (old) domicile gets to be notified of the new address. The member states piloting this use case in DE4A currently has differences in the requirements as well as in executing the procedure. To mitigate these discrepancies, three possible scenarios are under consideration at the time of this deliverable:

1) Reuse Domicile registration canonical evidence data model as it is (with same labels and classes) under the name of "Domicile deregistration". The reason for not introducing a single evidence registration and deregistration is that the two evidences serve two different purposes.

2) Finding an agreeable subset of fields from the domicile registration evidence that allow transferring of the new domicile information cross-border. This information should only contain the data fields of the new address, but not any information that the receiving MS already know about the user, following the SDGR recommendation of data minimalization.

3) Domicile Deregistration is a notification from the new domicile country to the old country with the information of the new address. This process however is an event that is not generated by the user, but a "push" notification from the back office of the new domicile country. However, this is the least likely option to be implemented by the DE4A due to the implementation demand of this scenario.

Further decision making and development of this canonical evidence will be documented in the DE4A wiki pages [23]and in the GitHub repository [24].

4.1.5   Means of Living Evidence

The means of living evidence consists of three different canonical evidence types regarding pension, unemployment and working life benefits. This evidence is part of the Moving Abroad pilot Use Case "Request Pension Information – Claim Pension" (UC3) and will be piloted for exchange of information between Spain (data owner) and Portugal (data evaluator). The process to model the evidence started with initial description of available information from Spain and matched to requirements of procedure

in Portugal for a person moving into that country and for which there is need to assess his/her means of living.

As this is an ongoing effort, the information will be updated in the DE4A wiki page [23] and the GitHub Repository [24]. Based on the current status, Figure 6 and Table 7 provide an overview of the Pension Means of Living evidence.

Figure 6: Pension Means of Living Evidence- fields overview

Table 7: Pension Means of Living Evidence- fields specification

Field	Definition	Data type	Relevant reqs
identifier	An unambiguous reference to the Means of Living evidence.	Identifier	MA-GE-01
date of issue	Date of issue of the information	Date (XSD)	MA-GE-01 MA-GE-08
issuing authority	A public organization with official authority in charge of issuing the domicile registration evidence.	Public Organization (CPOV)	MA-GE-01
data subject	The person who is subject to this information	Person (CPV)	MA-GE-02 MA-GE-03 MA-ML-01
pension list	List of pensions and benefits. Contains information on the pensions of the	Custom type	MA-ML-01

Field	Definition	Data type	Relevant reqs
	person for whom the query was made.		
pension category	A list of possible values for the pension category.	Enumeration (XSD)	MA-ML-02 MA-ML-03
status	Status of the benefit (e.g., active, non-active, etc)	Enumeration (XSD)	MA-ML-02 MA-ML-09
gross amount	It corresponds to the amount of the benefit, including the amounts of possible deductions plus the amount of Personal Income Tax (if applicable).	MonetaryAmount (Custom type that includes the amount and the currency)	MA-ML-02 MA-ML-05 MA-ML-06
net amount	It corresponds to the amount of the benefit after the possible deductions have been applied, plus the amount of Personal Income Tax (if applicable).	MonetaryAmount	MA-ML-02 MA-ML-05 MA-ML-06
number payments year	Number of payments corresponding to that benefit in the period of one year.	Numeric (XSD)	MA-ML-02
period of time	It includes the effect date of the benefit and the date on which the benefit ends	Custom type	MA-ML-02

Figure 7 and Table 8 below, provide an overview of the Unemployment Means of Living evidence.
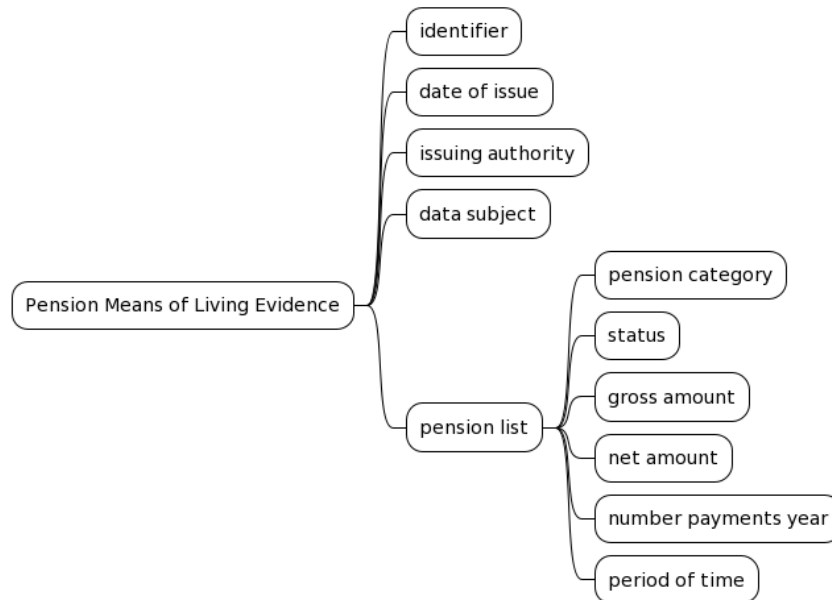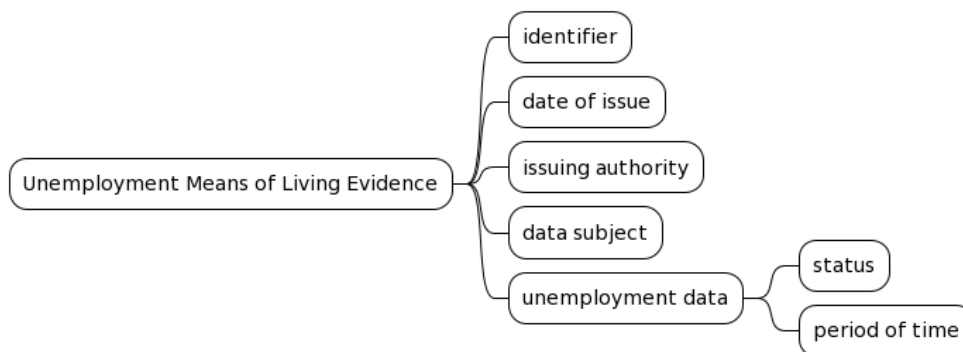
Figure 7: Unemployment Means of Living Evidence - fields overview

Table 8: Unemployment Means of Living Evidence - fields specification

Field	Definition	Data type	Relevant reqs
identifier	An unambiguous reference to the Means of Living evidence.	Identifier	MA-GE-01
date of issue	Date of issue of the information	Date (XSD)	MA-GE-01 MA-GE-08
issuing authority	A public organization with official authority in charge of issuing the domicile registration evidence.	Public Organization (CPOV)	MA-GE-01
data subject	The person who is subject to this information	Person (CPV)	MA-GE-02 MA-GE-03 MA-ML-01
unemployment data	Current unemployment data of the citizen.	Custom type	MA-ML-01
status	Status of the benefit (e.g., active, non-active, etc)	Enumeration (XSD)	MA-ML-07 MA-ML-09
period of time	It includes the effect date of the benefit and the date on which the benefit ends	Custom type	MA-ML-07

Figure 8 and Table 9 provide an overview of the Working Life Means of Living evidence.
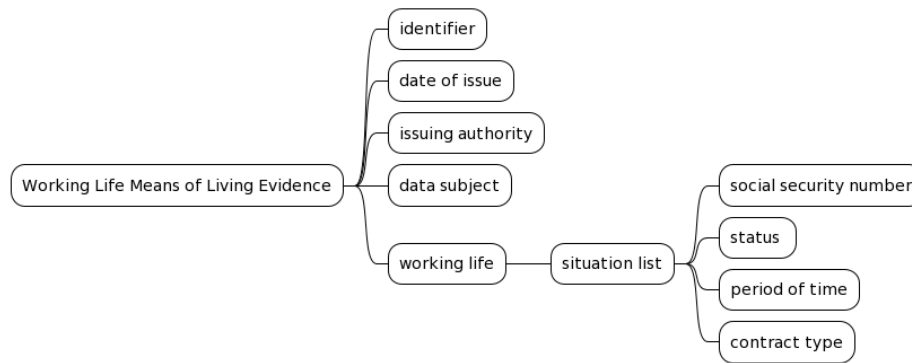
Figure 8: Working Life Means of Living Evidence - fields overview

Table 9: Working Life Means of Living Evidence – fields specification

Field	Definition	Data type	Relevant reqs
identifier	An unambiguous reference to the Means of Living evidence.	Identifier	MA-GE-01
date of issue	Date of issue of the information	Date (XSD)	MA-GE-01 MA-GE-08
issuing authority	A public organization with official authority in charge of issuing the domicile registration evidence.	Public Organization (CPOV)	MA-GE-01
data subject	The person who is subject to this information.	Person (CPV)	MA-GE-02 MA-GE-03 MA-ML-01
working life	Working life of the citizen.	Custom type	MA-ML-01
situation list	Contains the list of situations of the consulted citizen.	Custom type	MA-ML-10
social security number	Social security number of the situation returned.	Identifiers	MA-ML-11
status	Status of the benefit (e.g., active, non-active, etc)	Enumeration (XSD)	MA-ML-09 MA-ML-11
period of time	It includes the effect date of the benefit and the date on which the benefit ends	Custom type	MA-ML-11

Field	Definition	Data type	Relevant reqs
contract type	Identifier of the employment contract.	Enumeration (XSD)	MA-ML-11 MA-ML-12

4.2 Study Abroad Pilot Evidence

4.2.1 Higher Education Diploma Evidence

This type of evidence proves that an individual has acquired a higher education diploma. Figure 9 gives an overview of the appropriate fields, while Table 10 includes a specification of the fields, along with definitions, data types, and a cross-reference to the respective functional requirements specified in the deliverable D3.2 *"Requirements for Semantic Assets"*. The terms in parentheses in the "Data type" column indicate the third-party model that will potentially be adopted for representing the respective field: "EDCI" stands for the Europass Digital Credentials Infrastructure [21]; "XSD" stands for the XML Schema Definition [25], [26]. With regards to adopting EDCI, it was a recommendation by the DE4A Pilots to seek alignment with the Europass EDCI data model, although DE4A made some simplifications: (a) for DE4A pilots the large amount of data the full EDCI schema covers was not deemed necessary, and, (b) attributes were added for verifications, e.g., to verify evidence provided matches student authenticating at the issuer's end. At the same time, DE4A also considers the SDG data model for academic evidence, so the resulting model also includes some aspects from that model.
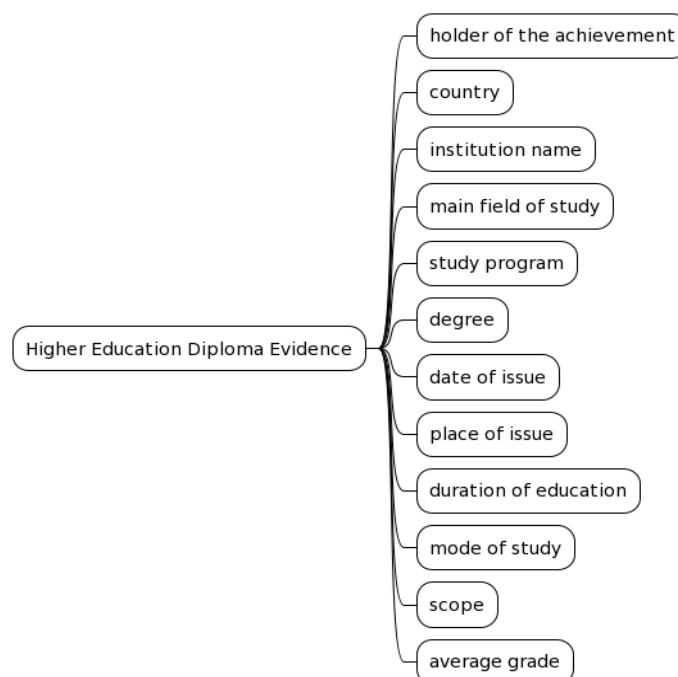
Figure 9: Higher Education Diploma Evidence - fields overview

Table 10: Higher Education Diploma Evidence - fields specification

Field	Definition	Data type	Relevant reqs
holder of the achievement	Person (student) that has obtained	Person (EDCI)	SA-HE-01 SA-HE-02

Field	Definition	Data type	Relevant reqs
	the academic title or degree		
country	Country where the study programme was completed by the student	Enumeration (EDCI)	SA-HE-01 SA-HE-03
institution name	The name of the higher education institution where the student obtained the degree	String	SA-HE-01 SA-HE-04
main field of study	Field of finished higher education	Enumeration (EDCI)	SA-HE-01 SA-HE-03
study program	Name of a study programme that the student finished at the higher education institution to obtain the degree	String	SA-HE-01 SA-HE-04
degree	An academic title or degree obtained by the student and proven by this diploma or certificate	String	SA-HE-01 SA-HE-04
date of issue	Date of issue of the certificate or diploma	Date (XSD)	SA-HE-01
place of issue	Place of issue (location) of the certificate or diploma	Location (EDCI)	SA-HE-01
duration of education	Official duration of education	Duration (XSD)	SA-HE-01 SA-HE-05
mode of study	Mode of study, e.g., full-time, part-time etc.	Enumeration (EDCI)	SA-HE-01 SA-HE-03
scope	The official workload of the study programme in ECTS credit points	Enumeration (EDCI)	SA-HE-01 SA-HE-03
average grade	The average grade awarded	Custom type	SA-HE-01 SA-HE-06

4.2.2   Secondary Education Completion Evidence

This type of evidence proves that an individual has completed their secondary education. Figure 10 gives an overview of the appropriate fields, while Table 11 includes a specification of the fields, along with definitions, data types, and a cross-reference to the respective functional requirements specified in D3.2 *"Requirements for Semantic Assets"*. As before, the terms in parentheses in the "Data type" column indicate the third-party model that will be adopted for representing the respective field.
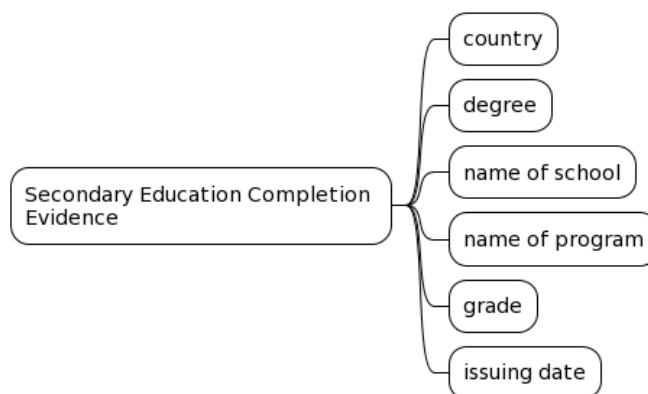
Figure 10: Secondary Education Completion Evidence - fields overview

Table 11: Secondary Education Completion Evidence - fields specification

Field	Definition	Data type	Relevant reqs
country	Country of completed secondary education	Enumeration (EDCI)	SA-SE-01 SA-SE-02
degree	Degree previously obtained (e.g., General upper secondary education)	String	SA-SE-01 SA-SE-03
name of school	Name of a secondary school that the person finished	String	SA-SE-01 SA-SE-03
name of program	Name of a secondary school programme that a person successfully finished (e.g., General secondary programme)	String	SA-SE-01 SA-SE-03
grade	Mark indicating a degree of accomplishment, accompanied by optional	Custom type	SA-SE-01 SA-SE-04

Field	Definition	Data type	Relevant reqs
	information specifying the grading scheme		
issuing date	Issuing date of the accomplishment	Date (XSD)	SA-SE-01

4.2.3   Non-Academic Information Evidence

This type of evidence provides additional non-academic information about an individual, i.e., household composition and income (e.g., for the purposes of awarding a scholarship or grant). The model proposed here is adopted from SDG, but within DE4A there is still an ongoing discussion for revisions to the model, as data evidence providing partners (SGAD) cannot provide evidence on household income and household composition. The final model will be made available at the respective DE4A repository on GitHub. Figure 11 gives an overview of the appropriate fields, while Table 12 includes a specification of the fields, along with definitions, data types, and a cross-reference to the respective functional requirements specified in D3.2 *"Requirements for Semantic Assets"*.
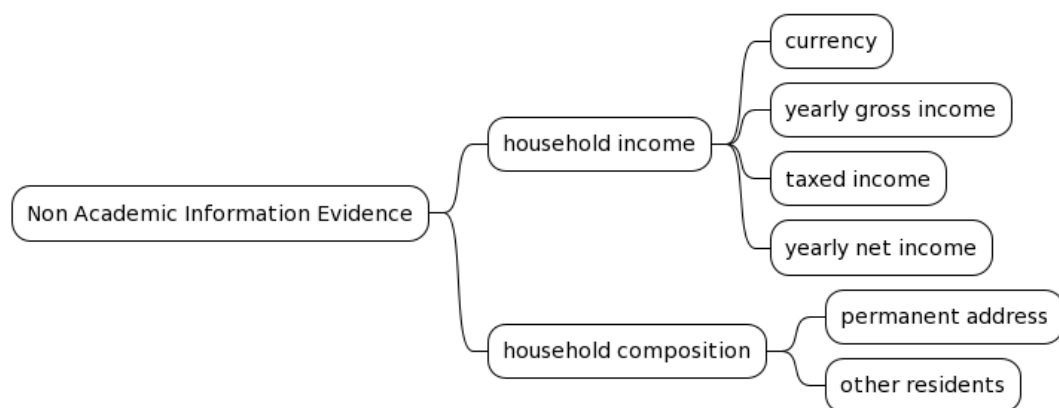
Figure 11: Non-Academic Information Evidence - fields overview

Table 12: Non-Academic Information Evidence - fields specification

Field	Definition	Data type	Relevant reqs
currency	The currency type	Enumeration (EDCI)	SA-NA-03 SA-NA-04
yearly gross income	The amount of yearly gross income of a household for that tax year	Number	SA-NA-02 SA-NA-03 SA-NA-04
taxed income	The amount of income taxed in that tax year	Number	SA-SE-01 SA-SE-03
yearly net income	The amount of yearly net income of a household for that tax year	Number	SA-SE-01 SA-SE-03

Field	Definition	Data type	Relevant reqs
permanent address	Address of the permanent residence of the citizen	String	SA-NA-05
other residents	The people they live with	Number	SA-NA-05

4.3 Doing Business Abroad Pilot Evidence

4.3.1 Company Registration Evidence

The company registration information is required by the pilot of doing business abroad to exchange the evidence of a company (c.f D3.2 *"Requirements for Semantic Assets"*.). Figure 12 gives an overview of the appropriate fields, while the concepts derived and their connection to the requirements elicited are tabulated in Table 13.
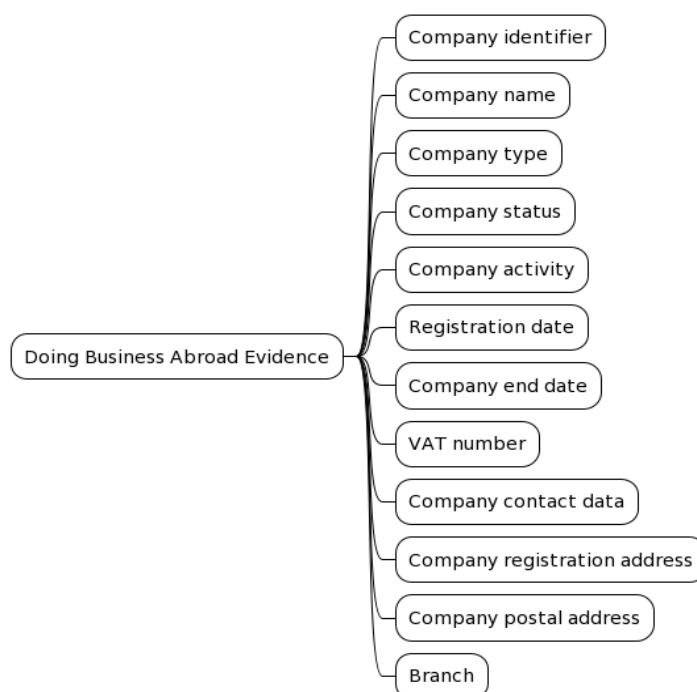
Figure 12: Company Registration Evidence - fields overview

Table 13: The specification derived concepts for the Company Registration evidence

Field	Definition	Data type	Relevant reqs
Company identifier	The unique identifier the company being identified	String	DBA_CRE_01 DBA_CRE_02
Company name	The primary name of the company	Text	DBA_CRE_10 DBA_CRE_09 DBA_CRE_07

Field	Definition	Data type	Relevant reqs
			~~SA-SE-01~~
			~~SA-SE-03~~
			~~SA-SE-01~~
			~~SA-SE-03~~
			~~SA-SE-01~~
			~~SA-SE-04~~
Company type	The type of the company	String	
Company status	The current status of the company as defined in BRIS	String	
CompanyActivity	The activity of a company as described by the codes and descriptions of NACE	Complex Type	
Registration Date	Date of registration of the company	Date	DBA_CRE_10 DBA_CRE_09
Company end date	The date the company is ended	Date	DBA_CRE_07 DBA_CRE_06
VAT number	The VAT registration number of the company	String	DBA_CRE_10 DBA_CRE_09 DBA_CRE_07
Company contact data	The contact information of the company (email and telephone number)	Complex type	
Company registration address	The address the legal entity is registered	Complex type	DBA_CRE_11 DBA_CRE_10 DBA_CRE_09 DBA_CRE_07
Company postal address	Physical address of the company	Complex type	
Branch	The branch information, which contains branch name and location	Complex type	DBA_CRE_10 DBA_CRE_09 DBA_CRE_07 DBA_CRE_05

5 The Information Desk

The Information Desk (IDK) is an information placeholder and key DE4A semantic asset for the actors -Data Evaluators, Requesters, Transferors and Owners- to obtain information that is required to build and send requests and responses between the requesting and providing sides. The IDK both aligns with and is an enabler of DE4A evidence-based approach (more details can be found in Section 5.1) and helps in the cross-border interoperability in full respect to the substance and availability of the participation of competent authorities. For example, actors can make the following queries to the IDK: i) *which cross-border authority is competent to issue the user's evidence?* or ii) *what are the semantics of this evidence type*?

This chapter provides a high-level view of the IDK design, which accommodates the wide range of realities in the evidence provision and procedure requirements according to the obligations under SGDR Art. 14, while a detailed description of its implementation is given in the deliverable D3.6 *"Semantic Toolkit – Final Version".*

The IDK has the following responsibilities with the corresponding components that cover them:

▶ Register and provide information on the available provisions - *Issuing Authority Locator (IAL)*:

- Available canonical evidence types provided by an issuing authority.
- Available canonical event catalogues provided by an issuing authority.
- Details on the type and particularities of each provision.
- Territorial scope of the issuing authorities' competences.

▶ Register and provide information to connect authorities - *Evidence Service Locator (ESL)*:

- Enable the interaction between cross-border competent authorities to obtain evidence corresponding to a canonical evidence type (and administrative level of issuing authority).
- Enable the interaction between cross-border competent authorities for the subscriptions to a canonical event catalogue.
- Provide competent authorities' information details about evidence services.

▶ Register and provide information on concepts and terms involved in the evidence exchange and support automatic generation of customizable user interfaces (explicit request, preview, additional parameters) that contain complex terms in any EU official language - *Multilingual Ontology Repository (MOR)*:

- Identification of canonical evidence types as complex terms.
- Identification of additional parameters of a data service as complex terms.
- Identification of code lists as a complex term of type enumeration.
- Syntax of complex and simple terms.
- Multilingual semantic description of complex and simple terms.

▶ Register and provide information on access authorization - *Cross-border Access Authorization Registry (CAAR)*:

- Agreements between data evaluators and data owners for consuming available provisions.

The information provided by the IAL, ESL and CAAR components can be represented by the following high-level diagram (Figure 13):
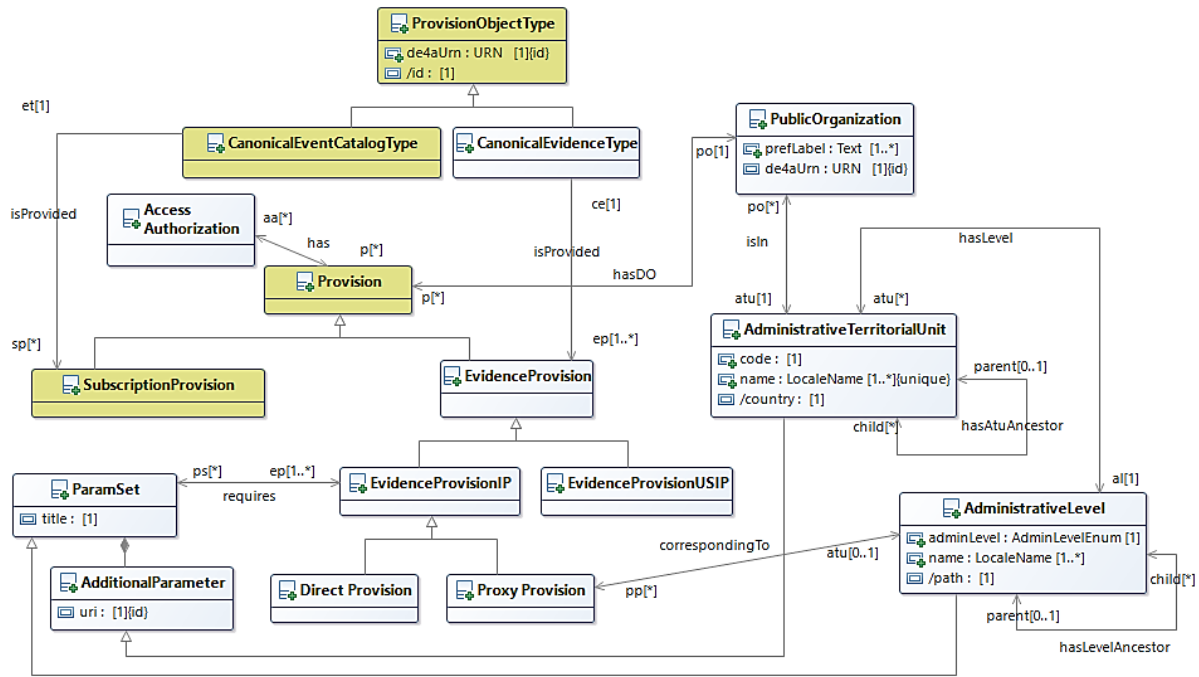
Figure 13: High-level overview of information provided by IAL, ESL and CAAR

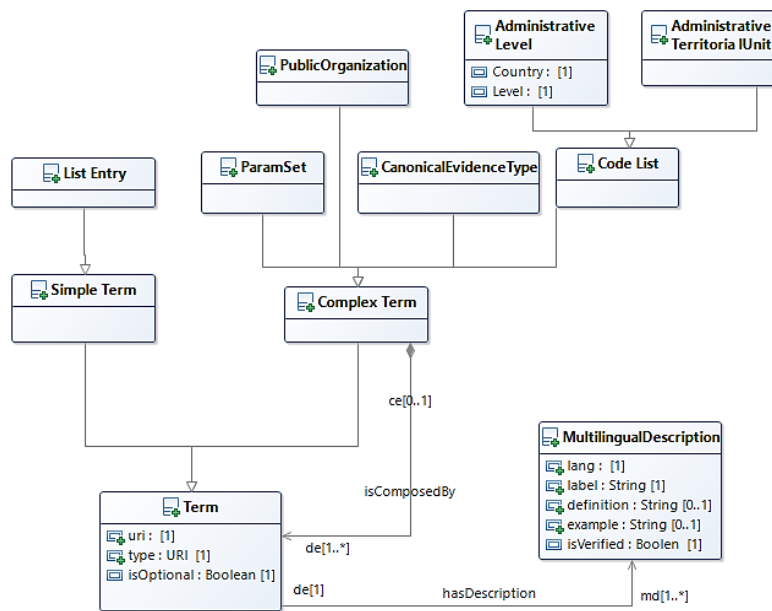The figure below illustrates the information provided by the MOR component:

Figure 14: High-level overview of information provided by MOR

The above mentioned IDK components are described in the subsequent paragraphs.

5.1 Issuing Authority Locator (IAL)

The Issuing Authority Locator (IAL) IDK component helps DCs to find out the competent issuing authority that can provide the evidence required by their procedures from a particular country.

The mapping between cross-border domestic evidence –evidence pieces nationally used with evidence pieces provided abroad- requires some interoperability agreements under either a criteria-based approach or an evidence-based approach. The former approach requires requesting and issuing competent authorities to work with domestic procedural requirements associated with domestic evidence pieces, as described in D2.4 *"Project Start Architecture"* [2] as well as interoperability agreements on procedural requirements from a country-agnostic perspective. On the other hand, both criteria-based and evidence-based approaches require requesting and issuing competent authorities to work with cross-border evidence so, without any country-agnostic interoperability agreement to provide common semantics, semantic and linguistic barriers can make the received evidence useless or wrongly processed. Finally, according to the GPDR and SDGR respectively, data protection measures require to identify the categories of dataset to process, and evidence types relevant to SDG procedures are to be identify; therefore, any system for the cross-border exchange of information as evidence requires to identify the evidence types to exchange with a common understanding of their purpose.

Consequently, DE4A has decided to use an evidence-based approach to minimize the cross-border agreements (since no agreements on procedural requirements are needed), to identify the evidence types to exchange abroad with a common understanding according to the GDPR and SDGR requirements, and to minimize linguistic and semantic barriers. Besides, the DE4A evidence-based approach also avoids competent authorities to specify and maintain the classification of their national domestic evidence types and to understand cross-border classifications.

DE4A evidence-based approach is based on a common classification of evidence types –canonical evidence types- to allow the matching between cross-border domestic evidence types, and some semantic and organizational agreements. This approach implies domestic evidence types to be associated by competent authorities to the canonical evidence types. Each canonical evidence type available through the system has a common understanding of the fact to be proven and the information to be provided. Besides, each canonical evidence type has associated a common data model aimed to provide a common understanding on the information provided by the associated domestic evidence type and to be automatically processed by any cross-border competent authority, regardless the semantic and linguistic particularities of the corresponding domestic evidence.

Accordingly to the mentioned above, to identify the corresponding issuing authority for a particular canonical evidence type, IAL requires the following preconditions:
1. The user has informed the DC that the evidence must be provided by another country.
2. The DC knows which is the correspondence between the evidence type required by the procedure and the available canonical evidence types in the system.
3. Each canonical evidence type is only provided by one competent authority within a certain territorial competence scope at some administrative level –national, regional, local or educational level. In the case of existing several issuing authorities at different administrative levels to issue the same canonical evidence type, only the provision at the higher administrative level is registered in the IAL. For instance, in Spain, the evidence that a person has a specific university degree resides in the registries of the corresponding university and the Ministry, but only the latter is registered in the IAL to provide a single point of access that facilitates the evidence location. This an organisational agreement achieved in the DE4A project to simplify the issuing authority location process.
4. Every canonical evidence type has been registered in IAL.
5. Every country has registered in IAL their issuing authorities and territorial competence distribution in several administrative levels, according to NUTS, LAU and a common identifiers policy for universities.

6. Every country has registered in IAL their provisions. Each *provision* is implemented by an available evidence service that provides a canonical evidence type issued by a competent authority with issuing competences at some territorial unit, and under some conditions such as the type of provision according to the exchange pattern –intermediation or user supported intermediation- implemented by the service, or any additional parameter required to properly located the evidence in the corresponding registry.

Additional parameters are defined with the help of the IDK Multilingual Ontology Repository (MOR), described below, to provide a common understanding of such parameters to both DCs and DPs. When an evidence service exists for different competent authorities at the same territorial level, e.g. for different municipalities, additional parameters may be used by an evidence service that acts as a *proxy provision*, to identify the proper competent territorial unit, so DCs are not required to interact with the several evidence services at subnational level, but only one. Thus, proxy provisions provide interoperability agreements between subnational issuing authorities for a canonical evidence type.

As the first step to build the cross-border evidence request, the DC consults IAL about the availability of some provision at the target country. Below are the possible flows to locate evidence provisions:

A. **Provision for a canonical evidence type at a specific territorial unit (Main flow):** DC queries the IDK about a specific canonical evidence type at a specific territorial unit, either a national, regional, local or educational unit. National and regional territorial units are identified by the NUTS code, local territorial units are identified by the LAU code and educational territorial units are identified by an URN. IDK will provide three possible outcomes:
R1 (Success)**:** a provision corresponding to the specified canonical evidence type, and territorial unit along with identification of the corresponding issuing authority at that unit.
R2 (Partial Success)**:** list of provisions at a territorial scope under the territorial unit specified.
R3 (Error)**:** error message because there is no provision for such canonical evidence type is available in such a territorial unit.

B. **Provisions for a canonical evidence type:** DC queries the IDK about a specific canonical evidence type. IDK will provide two possible outcomes:
R1 (Success)**:** list of provisions for the canonical evidence type at any territorial unit.
R3 (Error)**:** error message because there is no provision for such canonical evidence type is available.

Besides evidence provisions, IAL provides information on provisions to allow DCs to subscribe to event catalogues provided by base registries authorities, so subscription provisions are associated with services that implement the subscription & notification pattern. The functionality for locating subscription provisions has the same preconditions and flows than evidence provisions but regarding a canonical event catalogue instead of a canonical evidence type.

5.2 Evidence Service Locator (ESL)

Evidence Service Locator (ESL) helps DCs to locate the evidence service associated with an IAL provision, i.e., a canonical evidence type or event catalogue provided by a specific issuing authority.
To locate an evidence service, ESL requires the following preconditions:
1) DC knows the canonical evidence type to request and, after consulting the IAL, the corresponding issuing authority according to the provision located by the IAL consultation.
2) Every issuing authority has registered their service in the ESL for each IAL provision.
3) Each evidence service has a unique identifier and the required metadata to allow the connection between sending and receiving parties of the service.
DC consults the ESL for the evidence service corresponding to an evidence provision with the following possible consultation flows:

A. **Evidence Service Location (Main flow 1)**: DC asks for the evidence service for a certain canonical evidence type and issuing authority.

   R1 (Success): metadata connection details of the evidence service for the specified canonical evidence type and issuing authority.

   R3 (Error): there is no available evidence service that corresponds to the given query parameters, I.e., canonical evidence type and issuing authority.

ESL main flow is applicable to subscription provisions by specifying a canonical event catalogue instead of a canonical evidence type.

5.3   Multilingual Ontology Repository (MOR)

The main functionality of the **Multilingual Ontology Repository** (**MOR**) is to provide a common understanding of the semantics and syntax of canonical evidence types, additional parameters of provisions and code lists used for the cross-border evidence exchange, by describing all the terms that compose them. Table 14 introduces key MOR aspects, along with the corresponding Competency Questions (CQs) from D3.2 *"Requirements for Semantic Assets"* introducing the respective functional requirements.

Table 14: Multilingual Ontology repository functional requirements

Aspect	Description	Relevant reqs
MOR Term	A MOR term is a semantic element represented by an URI, syntax and multilingual meaning.	CQ20 CQ21
Types of MOR Terms	MOR terms can be simple and complex terms; complex terms are composed of other simple and/or complex terms. Simple terms are always part of a complex term. Canonical evidence types, sets of additional parameters and code lists are complex terms. Other complex terms are concepts defined by core vocabularies and domain ontologies that are reused for describing canonical evidence types and sets of additional parameters.	CQ23
Term Syntax	The syntax of a complex term is defined by the data type and cardinality of the terms that compose the complex term. The cardinality specifies if the term value is mandatory for composing the value of the higher term and how many values of that term can be used.	CQ20 CQ21
Term Multilingual Meaning	Each term is semantically described by a label, description and an example in every EU official language, but only the label is mandatory. These properties can be automatically translated from the English version to the rest of the languages, so the resulting version is marked as "non-verified" until a domain expert reviews the automatic translation, and it is then that this mark is changed to "verified".	CQ20 CQ21
Term Data Types	Simple terms correspond to simple data types, e.g., string, integer, token, etc. Complex terms correspond to complex data types that are identified by the URI of the complex term that defines the syntax and multilingual meaning of such a complex data type, so complex data types are also complex terms.	CQ23
Term URI	A complex term that is modelled as a tree hierarchy of terms, so each term is uniquely identified by a path that represents the position of that term within the hierarchy. If a complex term [X] is defined of type [Y], the [X] sub-terms have the same URI as the [Y] sub-terms except for the root element,	CQ20 CQ21

Aspect	Description	Relevant reqs
	so the root of [Y] term paths is replaced by the [X] URI. For example, the sub-term "Gender" of the complex term "*BirthEvidence/Child*" of type "*Person*", corresponds to the "*Person/Gender*" sub-term but with URI "*BirthEvidence/Child/Gender*"	
Code lists	A code list is a special complex term of data type "enumeration" whose sub-terms are of data type "token".	CQ22
Reusability	A complex term inherits the syntax and multilingual meaning of the corresponding complex type, unless the complex term explicitly specifies sub-terms that overload any part of the complex type syntax or multilingual meaning. For example, the complex term "*BirthEvidence/Child*" of type "*Person*", may overload the multilingual meaning -label and description- for new-born persons instead of persons in general.	CQ23

5.3.1   Building Customizable User Interfaces

Although the main functionality of the MOR is to provide a common understanding of the semantics and syntax of canonical evidence types, additional parameters and code lists, the MOR can also be used to automatically generate **customizable user interfaces** for any complex term in any EU official language. There are three cases where this functionality can be of help:

▸ The **explicit request** functionality should inform the user on the information to be requested as evidence, so the MOR can help to create a building block that generates such a user interface for any canonical evidence type and language.

▸ The **preview** functionality should show to the user the evidence to be incorporated to the procedure, so the MOR can help to create a building block that generates such a user interface for any canonical evidence type and language; audits can also use this building block to help auditors to understand any canonical evidence in any language. This is of special interest when the preview space is located at the evidence provider side, since the language on this side can be different from the language of the procedure that requires the cross-border evidence, and the user may not understand the provider's language. In this case, values of the canonical evidence attributes cannot be legally translated unless they are from a canonical code list, but most of such values are dates, proper names or numbers that do not require translation.

▸ The **additional parameters** functionality requires the user to request some fields through a form, so the MOR can help to create a building block that generates such a form for any set of additional parameters and language. In this case, the type of the terms is the key to generate the proper input field in the form (calendar, select list, text box, etc.) This is of special interest when the additional parameters have to be required at the evidence evaluator side, because the additional parameters are set by the evidence provider.

5.3.2   Reusability

In any case, the MOR building blocks have the advantage to be reusable and generic for any complex term and language, so parties in the evidence exchange do not need to develop their own equivalent components, and any modification in MOR is automatically available through the MOR building blocks. For a proper reusability of these building blocks and, in particular, of the customizable user interfaces, customizable cascade stylesheets (CSS) are used.

5.4 Cross-Border Access Authorization Registry (CAAR)

As part of the IDK, the Cross-border Access Authorization Registry (CAAR) stores access authorizations registered by the corresponding data owners to access their provisions. It helps to represent multi/bilateral agreements with Data Owner authorities for accessing their evidences or by-law authorisations. The CAAR is used by the Authorization Controller (AC)-deliverable D2.5 *"Project Start Architectures-Second Iteration"*- that allows checking access to a specific canonical evidence type or event catalogue provided by a specific data owner (DO) and requested by a specific data evaluator (DE) to be used in the scope of a specific procedure category. The pair issuing authority and canonical object type -canonical evidence type or event catalogue- identifies an IAL provision. Therefore, an authorization is a function of three parameters: requesting authority (DE), procedure category and IAL provision. The authorization could be extended to include legal grounds for requesting an evidence type.

5.4.1 Authorization Design Alternatives

According to Trusted Computer System Evaluation Criteria (TCSEC) [26], there are four divisions of criteria to assess system security policies:

D - Minimal protection (no security),

C - Discretionary protection,

B - Mandatory protection,

A - Verified protection (highest security level)

The AC is only a part of the system security policy to provide a mechanism to limit access to DO's canonical object types.

Different access control models can be identified:

▸ **Mandatory Access Control (MAC):**

- The strictest model. Each resource object is controlled by access settings defined by the administrator, so users cannot change these settings.
- Each resource object is assigned a security label with two properties: security classification (top secret, confidential, public, etc) and availability level category (department, project, user).
- Access permissions are controlled only by an administration.

▸ **Discretionary Access Control (DAC):**

- Every resource object has an owner controlling its access settings.
- Each resource object is associated with an Access Control List (ACL) that contains the list of users and groups with the level of access for each of them.
- Users or groups may control access permissions.

▸ **Role-Based Access Control or Non-discretionary Access Control**:

- Access is based on the user's role, i.e., their job function within the organization.
- Users may belong to several groups but are assigned to only one role.
- Users in a specific role may control access permissions.

▸ **Rule-Based Access Control (RBAC):**

- Access is based on a set of rules defined by the administration, which are stored in the ACL.
- When a user or group wants to access a resource object, the system checks the rules stored in its ACL.
- Access permissions are controlled only by an administration.

▸ **Attribute-Based Access Control (ABAC) or Policy-Based Access Control (PBAC) or Claims-Based Access Control (CBAC):**

- Access rights defined by policies, which combine attributes of any type (e.g., user, resource, environment, timing attributes).
- Example: The online store (resource owner) sells alcoholic beverages (resource) to consumers of a given age (attribute). The decision to grant a claim is made upon the user attribute.

▸ **Graph-Based Access Control (GBAC):**

- Access rights are defined using an organizational query language instead of total enumeration of roles or attributes.

The AC is using an Attribute-Based Access Control (ABAC) model for accessing DO's evidence types and event catalogues, with attributes from the IEM request that identifies the DO and canonical object type (provision), the DE, the category of the procedure and, in a potential extended version, the legal grounds of the request.

5.4.2   Authorization Controller (AC)

According to the AC architecture introduced in D2.4 *"Project Start Architecture (PSA)"* [2] - an updated version will be available in deliverable D2.5 *"Project Start Architectures Second Iteration"-,* there are two application components to enable the AC functioning: for checking authorisations for a particular IEM request and for managing the authorisations registered in the CAAR.

5.4.2.1   Authorisation Checking

The AC implements the authorisation checking process that requires the information from the CAAR and from the corresponding IEM evidence or subscription request messages. The authorisation is related to the functional parties (i.e., DE and DO), but the technical parties (i.e., data requester (DR) and data transferor (DT)) are the ones who check if the evidence request can be responded to. IEM evidence and subscription requests specify which Data Evaluator is requesting a canonical object type from which Data Owner in the scope of a procedure of a certain category. IEM evidence requests also include the grounds of the request. Therefore, the authorisation checking is to be incorporated into the system by its implementation in the DT's connector component to prevent unauthorized access; using the authorisation checking in the DR's connector component can avoid sending abroad authorized requests.

To know whether an IEM evidence or subscription request has appropriate authorisation, the following preconditions are required:

1. The IEM evidence or subscription request includes the URIs of the DE and DO involved.
2. The IEM evidence or subscription request includes the URIs of the requested object type -canonical evidence type or event catalogue- and the category of the procedure that requires such an object.
3. The IEM evidence request includes the grounds of the request.
4. Authorisations are stored in the CAAR regarding the DO included in the IEM request. Otherwise, it is understood that such a DO does not limit the access to its provisions.
5. A DO's authorisation is stored in the CAAR for the canonical object type, the DE and procedure category included in the IEM request, or some of these parameters are set to "any".

The authorisation checking could result in only **one main flow** for a specific IEM request. The flow can result in three possible outcomes:

> **R1 (Success)**: The IEM request is authorized to get the corresponding response.
> **R2 (Waiting for approval)**: Request for data access by a DO has not yet been processed.
> **R3 (Reject)**: The IEM request is not authorized to get the corresponding response.
> **R4 (Error)**: Technical error has happened during request processing.

The IEM request attributes used for defining authorisations are:

▸ DO's identifier

- /IEMRequestMessage/DataOwner/AgentUrn

- ▸ DE's identifier
    - /IEMRequestMessage/DataEvaluator/AgentUrn
- ▸ Canonical object type's identifier, one of:
    - /IEMRequestMessage/ExchangeRequestItem/CanonicalEvidenceTypeUri
    - /IEMRequestMessage/EventSubscripRequestItem/CanonicalEventCatalogUri
- ▸ Procedure Category (Table 11):
    - /IEMRequestMessage/Procedure/ProcedureCategory

In the extended version of the access control for IEM evidence requests, the authorisation may consider the request grounds "/IEMRequestMessage/ExchangeRequestItem/RequestGrounds".

5.4.2.2 Authorisation Managing

The CAAR stores authorisations to be used in the AC authorisation checking. A CAAR entry is an authorisation associated with an IAL provision, so the same user with permissions to manage IDK provision from a certain DO is also allowed to manage that DO's authorisations. An authorisation in CAAR is represented by the next properties:

- ▸ **IAL Provision**: Reference to the IAL provision that includes: (a) DO's URI according to the DE4A policy for identifiers; (b) Canonical object type URI, either a canonical evidence type or a canonical event catalogue according to the DE4A policy for identifiers.
- ▸ **DE's URI**, according to the DE4A policy for identifiers, or "**any**".
- ▸ **Procedure category**, according to the categories of administrative procedures considered by the SDG link repository and the directives mentioned in SDGR Article 14, or "**any**"

Table 15: Categorization of procedures

#	Cat. ID	Procedure Category	Proc. ID	Procedure
1	R	Birth	R1	Requesting proof of registration of birth (SDGR Annex II) [28].
2	S	Residence	S1	Requesting proof of residence (SDGR Annex II) [28]
3	T	Studying	T1	Applying for a tertiary education study financing, such as study grants and loans from a public body or institution (SDGR Annex II) [28].
4	T	Studying	T2	Submitting an initial application for admission to public tertiary education institution (SDGR Annex II) [28]
5	T	Studying	T3	Requesting academic recognition of diplomas, certificates or other proof of studies or courses (SDGR Annex II) [28].
6	U	Working	U1	Request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004 (SDGR Annex II) [28].
7	U	Working	U2	Notifying changes in the personal or professional circumstances of the person receiving social security benefits, relevant for such benefits (SDGR Annex II) [28].
8	U	Working	U3	Application for a European Health Insurance Card (EHIC) (SDGR Annex II) [28].
9	U	Working	U4	Submitting an income tax declaration (SDGR Annex II) [28].
10	V	Moving	V1	Registering a change of address (SDGR Annex II) [28]
11	V	Moving	V2	Registering a motor vehicle originating from or already registered in a Member State, in standard procedures (SDGR Annex II) [28]

#	Cat. ID	Procedure Category	Proc. ID	Procedure
12	V	Moving	V3	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 (SDGR Annex II)[28].
13	V	Moving	V4	Obtaining emission stickers issued by a public body or institution (SDGR Annex II) [28]
14	W	Retiring	W1	Claiming pension and pre-retirement benefits from compulsory schemes (SDGR Annex II) [28]
15	W	Retiring	W2	Requesting information on the data related to pension from compulsory schemes (SDGR Annex II) [28]
16	X	Starting, running and closing a business	X1	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 (SDGR Annex II) [28]
17	X	Starting, running and closing a business	X2	Registration of an employer (a natural person) with compulsory pension and insurance schemes (SDGR Annex II)[28].
18	X	Starting, running and closing a business	X3	Registration of employees with compulsory pension and insurance schemes (SDGR Annex II) [28]
19	X	Starting, running and closing a business	X4	Submitting a corporate tax declaration (SDGR Annex II) [28].
20	X	Starting, running and closing a business	X5	Notification to the social security schemes of the end of contract with an employee, excluding procedures for the collective termination of employee contracts (SDGR Annex II) [28].
21	X	Starting, running and closing a business	X6	Payment of social contributions for employees (SDGR Annex II) [28]
22	O	Other	O200536	Procedures under Directive 2005/36/EC [29] of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications. (Under the SDGR Article 14 scope)
23	O	Other	O2006123	Procedures under Directive 2006/123/EC [30] of the European Parliament and of the Council of 12 December 2006 on services in the internal market. (Under the SDGR Article 14 scope)

#	Cat. ID	Procedure Category	Proc. ID	Procedure
24	O	Other	O201424	Procedures under Directive 2014/24/EU [31] of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC. (Under the SDGR Article 14 scope)
25	O	Other	O201425	Procedures under Directive 2014/25/EU [32] of the European Parliament and of the Council of 26 February 2014 on procurement by entities operating in the water, energy, transport and postal services sectors and repealing Directive 2004/17/EC. (Under the SDGR Article 14 scope)
26	O	Other	BUSnoSDG	Procedures for business not included in SDGR Article 14(1) (IEM common types) [33].
27	O	Other	CITnoSDG	Procedures for citizens not included in SDGR Article 14(1) (IEM common types) [33].

In the extended version of the access control for evidence requests, the authorisation may include the grounds for the request:

▸ Request Grounds, one of:

- EventNotification (token)
- A LawELIPermanentLink (a valid link)
- ExplicitUserRequest type (token)

6 Information Exchange Model

The DE4A Information Exchange Model (IEM) is the payload specification of the messages to be exchanged across borders between competent authorities. IEM is agnostic to any technical implementation and business domain, according to the DE4A project specific pilot needs and architecture. The design of the IEM is based on TOOP EDM and other national models analysed by "WP3 Semantic Interoperability Solutions" in collaboration with the rest of technical work packages (architecture, pilots and common components) under the following basic assumptions:

▸ DE4A IEM allows automated message exchange between the DR and the DT.
▸ DE4A IEM allows evidence exchange communications between a DO and a DE according to the DE4A interaction patterns.
▸ DE4A IEM satisfies the specific needs of DE4A pilots and architecture.
▸ DE4A IEM satisfies the specific DE4A policy for identifiers and IDK model.
▸ A DT can automatically generate an IEM response according to the IEM requests of a DR.
▸ DE4A IEM is abstract to handle events and evidence in any business domain.
▸ DE4A IEM allows to handle several events and evidence types in the same message between a DE and a DO.
▸ DE4A IEM is based on existing international vocabularies and standards.
▸ DE4A IEM models general information to include in the messages as metadata about the transmission, data subject, data evaluator, data owner and exchange.
▸ DE4A IEM allows the representation of exchanged lawfully issued evidence as structured data according to the canonical evidence data model with or without attached domestic evidence in any format with the legal value, including unstructured data (PDFs).

IEM models all the information required to properly process requests and responses, as well as to log and audit the transmissions when required, from the public administrations' point of view.

IEM models information according to vocabularies, code lists, authoritative lists, etc. defined at European or international level.

DE4A IEM differs from TOOP IDM in the following aspects:

▸ Participation model:

- TOOP evidence exchange is a two-corner model: DC & DP.
- DEA4 evidence exchange is a four-corner model: DE/DR & DT/DO.

▸ Evidence matching approach:

- TOOP evidence request model is based on a criteria-based approach with two alternatives for the query request: on specific concepts defined in an agreed overall ontology and on some domestic evidence type associated to a specific common procedural requirement to return either the metadata of the corresponding domestic evidence documents or such documents in any form, format and language.
- DE4A evidence request model is based on an evidence-based approach (see section 5.1) to request a canonical evidence type from the available list, and the response is the requested canonical evidence according to an agreed XML schema and, optionally, the domestic evidences with legal value in any form, format and language, which are not aimed to be processed but to provide full legal guarantees if the semantic equivalence of the canonical evidence to the legal domestic evidence is required to be audited.

▸ DE4A IEM supports additional request parameters as required by the IAL provision of the corresponding evidence service.

6.1 IEM according to DE4A Patterns

As specified in the deliverable D3.2 "Requirements for Semantic Assets", the IEM models several DE-DO interaction patterns designed by DE4A:

Table 16: IEM interaction patterns

Pattern Type	Details
Intermediation Pattern (IM)	▶ An **ExchangeRequestItem** included in an IEM Request Message is sent by a DR on behalf of a DE to request a canonical evidence type provided by the addressed DO for the processing of a specific DE's administrative procedure, including where applicable optional additional parameters for record matching at the DO. As response, an **EvidenceResponseItem** included in an IEM Response Message is sent by the DT on behalf of the required DO to the corresponding DR with the requested canonical evidence optionally along with the domestic evidence, in its original form with legal value and, where applicable, the corresponding multilingual standard form according to the Public Documents Regulation 2016/1191[22].
User-Support Intermediation Pattern (USI)	▶ An **ExchangeUsiRequestItem** included in an IEM Request Message is sent by a DR on behalf of a DE to request a canonical evidence type provided by the addressed DO and to send the DE's redirection URL and request the DO's redirection URL. ▶ As response, an **UserRedirectionResponseItem** included in an IEM Response Message is sent by the DT on behalf of the required DO to the corresponding DR with the requested DO's redirection URL and with the requested canonical evidence optionally along with the domestic evidence, in its original form with legal value and, where applicable, the corresponding multilingual standard form according to the Public Documents Regulation 2016/1191 [22]. ▶ After obtaining the DO's redirection URL, an **ExchangeRequestItem** and the corresponding **EvidenceResponseItem** are exchanged regarding the required evidence.
Subscription Pattern (SO)	▶ An **EventSubscripRequestItem** included in an IEM Request Message is sent by a DR on behalf of a DE to subscribe to a canonical event catalogue provided by the addressed DO for the processing of a specific DE's administrative procedure. As explained in section 5.4.2.1, the Authorisation Controller checks that the DE is authorised to make subscription request. ▶ As response, subject to the mentioned authorisation process, a **SubscriptionResponseItem** included in an IEM Response Message is sent by the DT on behalf of the required DO to the corresponding DR with the subscription details.
Notification Pattern (NP)	▶ An **EventNotificationItem** included in an IEM Event Notification Message is sent by a DT on behalf of a DO to the DR associated with a DE that is subscribed to a DO's event catalogue regarding a

Pattern Type	Details
	certain data subject, when an event of that catalog that involves such a subject happens.
Look-up Pattern (LP)	▶ An **ExchangeRequestItem** and the corresponding **EvidenceResponseItem** are exchanged regarding the required evidence, in this case with the request grounds in reference to the event notification previously received.

6.2 Design of IEM Messages

There are three types of IEM messages:

▶ *IEM Request message*: sent by a DE to a DO through the DR to obtain a response. This type of message can include three types of requests:

- Requesting the subscription to a DO's canonical event catalogue regarding a particular data subject.
- Requesting a DO's canonical evidence type regarding a particular data subject based on certain grounds.
- Requesting a DO's redirection URL for a USI exchange, which includes the DE's URL to redirect back the user.

▶ *IEM Response message*: sent by a DO to a DE through the DT in response to an IEM Request message. This type of message can include four types of responses:

- Response to an event catalogue subscription request
- Response to an USI redirection URL request
- Response to a canonical evidence type request
- Error as response to any request

▶ *IEM Event Notification message*: sent by a DO to a DE to notify an event related to an event catalogue subscription.

6.2.1 IEM Request Message

The following figure provides a diagrammatic overview of the IEM request message, followed by a description of the elements.
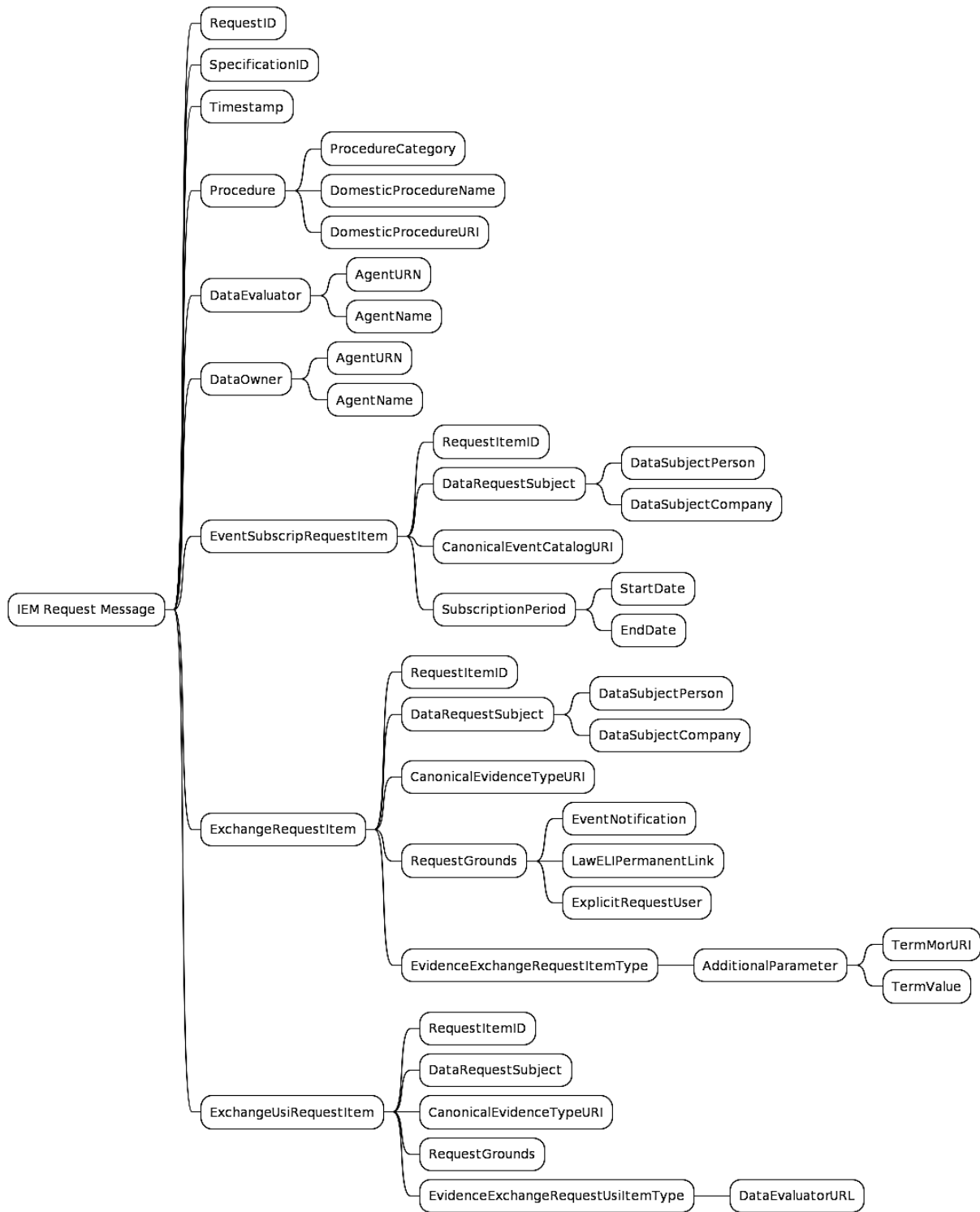
Figure 15: IEM request message overview

Description of elements:

▶ **RequestId**: Unique identifier of the Request Message (e.g., UUID).
▶ **SpecificationId**: Identifier of the IEM Request Message specification.
▶ **TimeStamp**: Day and time of the message sending.

- ▸ **Procedure**: Information about the DE's administrative procedure which processing requires the request. This information includes the category of the procedure according to the SDG regulation, the name of the procedure and, optionally, its URI.
- ▸ **DataEvaluator**: URN according to the DE4A policy of identifiers and, optionally, the organization name.
- ▸ **DataOwner**: URN according to the DE4A policy of identifiers and, optionally, the organization name.

Moreover, the following subsections describe the respective elements of any of the three request types.

6.2.1.1 EventSubscripRequestItem

Requesting the subscription to a DO's canonical event catalogue regarding a particular data subject:

- ▸ **RequestItemId**: Unique identifier of the request item within the request message (e.g., sequential number).
- ▸ **DataRequestSubject**: Either a physical or a legal person identifying data using the eIDAS profile attributes (eIDAS datasets) obtained at the DE during the authentication to the online procedure.
- ▸ **CanonicalEventCatalogUri**: Unique identifier of a canonical event catalogue according to the DE4A policy of identifiers.
- ▸ **SubscriptionPeriod**: Optionally, the starting date and time and/or ending date and time of the subscription.

6.2.1.2 ExchangeRequestItem

Requesting a DO's canonical evidence type regarding a particular data subject based on certain grounds:

- ▸ **RequestItemId**: Unique identifier of the request item within the request message (e.g., sequential number).
- ▸ **DataRequestSubject**: Either a physical or a legal person identifying data using the eIDAS profile attributes (eIDAS datasets) obtained at the DE during the authentication to the online procedure.
- ▸ **CanonicalEvidenceType**: Unique identifier of a canonical evidence type according to the DE4A policy of identifiers.
- ▸ **RequestGrounds**: Grounds of the request, either the reference of a former event notification or the link to a law according to the ELI specification or the physical person of the explicit request that justifies the evidence request.
- ▸ **AdditionalParameters**: Optionally, for Intermediation Pattern evidence provisions, the request may include values for the additional parameters specified in such provisions identified by URIs of MOR terms.

6.2.1.3 ExchangeUsiRequestItem

Previous step for requesting evidence under the User-Supported Intermediation Pattern and URL to redirect the user to the DO's portal and back to the DE's portal:

- ▸ **RequestItemId**: Unique identifier of the request item within the request message (e.g., sequential number).
- ▸ **DataRequestSubject**: Either a physical or a legal person identifying data using the eIDAS profile attributes (eIDAS datasets) obtained at the DE during the authentication to the online procedure.
- ▸ **CanonicalEvidenceTypeUri**: Unique identifier of a canonical evidence type according to the DE4A policy of identifiers.
- ▸ **DataEvaluatorURL**: DE's URL to redirect the user back to the DE's portal.

6.2.2   Response Message

The figure below gives a diagrammatic overview of the IEM response message, followed by a description of the elements that are common to any type of response.

Figure 16: IEM response message overview

Description of elements:

▸ **RequestId**: Unique identifier of the request message that this response message is responding to.

▸ **SpecificationId**: Identifier of the IEM Response Message specification.

▸ **TimeStamp**: Day and time of the message sending.

▸ **DataEvaluator**: URN according to the DE4A policy of identifiers and, optionally, the organization name. To be used as a safeguard for the matching between request and response messages besides de RequestId.

▸ **DataOwner**: URN according to the DE4A policy of identifiers and, optionally, the organization name. To be used as a guarantee of the correct matching between request and response messages besides de RequestId.

Moreover, the following subsections describe the respective elements of any of the four response types, three for each request type and a fourth type for error responses.

6.2.2.1   SubscriptionResponseItem

Response to an event catalogue subscription request:

▸ **RequestItemId**: Unique identifier of the request item within the request message that this response item is responding to.

▸ **DataRequestSubject**: Either a physical person or a legal person identifying data using the eIDAS profile attributes (eIDAS datasets). Same as the corresponding request item to be used as a safeguard for the matching between request and response items.

▸ **CanonicalEventCatalogUri**: Unique identifier of a canonical event catalogue according to the DE4A policy of identifiers. Same as the corresponding request item to be used as a safeguard for the matching between request and response items.

▸ **SubscriptionPeriod**: The starting date and time and, optionally, the ending date and time of the subscription finally granted.

6.2.2.2   EvidenceResponseItem

Response to a canonical evidence type request:

▸ **RequestItemId**: Unique identifier of the request item within the request message that this response item is responding to.

▸ **DataRequestSubject**: either a physical person or a legal person identifying data using the eIDAS profile attributes (eIDAS datasets). Same as the corresponding request item to be used as a safeguard for the matching between request and response items.

▸ **CanonicalEvidence**: the unique identifier of the requested canonical evidence type, according to the DE4A policy of identifiers -same as the corresponding request item to be used as a safeguard for the matching between request and response items- and the canonical evidence issued by the DO according to the request.

▸ **DomesticEvidence**: optionally, the domestic evidence as originally issued with legal value corresponding to the required canonical evidence type and, if needed in the case of the Public Document Regulation 2016/1191 [22], the corresponding multilingual standard form. A domestic evidence is represented by the issuing type (original or multilingual form), the MIME type of the evidence object, the language of the evidence information (at least one language), either a reference of the evidence object or the object itself represented in Base 64 encoding and, optionally, any additional information considered useful by the DO.

6.2.2.3   UserRedirectionResponseItem

Response in the previous step for requesting evidence under the User-Supported Intermediation Pattern to redirect the user to the DO's portal and back to the DE's portal.

▸ **RequestItemId**: Unique identifier of the request item within the request message that this response item is responding to.

▸ **CanonicalEvidenceTypeUri**: Unique identifier of a canonical evidence type according to the DE4A policy of identifiers. Same as the corresponding request item to be used as a safeguard for the matching between request and response items.

▸ **RedirectURL**: URL to redirect the user to the DO's portal.

6.2.2.4   ErrorResponseItem

Error as response to any request:

▸ **RequestItemId**: Unique identifier of the request item within the request message that this response item is responding to.

Object requested, one of:

▸ **CanonicalEvidenceTypeUri**: Unique identifier of a canonical evidence type according to the DE4A policy of identifiers. Same as the corresponding request item to be used as a safeguard for the matching between request and response items.

▸ **CanonicalEventCatalogUri**: Unique identifier of a canonical event catalogue according to the DE4A policy of identifiers. Same as the corresponding request item to be used as a safeguard for the matching between request and response items.

Error details:

▸ **Code**: There is an agreed error code list for common errors. For business errors that are particular for certain DOs, the domestic code errors need to specify at least the ID of the agency that assigns that code.

▸ **Message**: For common errors, associated messages are available in every EU language using functionalities of the MOR component; for domestic errors, associated messages need to specify the language of the text.

▸ **Description**: For common errors, associated descriptions are available in every EU language because of the MOR; for domestic errors, associated descriptions need to specify the language of the text.

▸ **AdditionalInfo**: For common errors, associated additional information is available in every EU language using functionalities of the MOR component; for domestic errors, associated additional information needs to specify the language of the text

6.2.3   IEM Event Notification Message

The following figure provides a diagrammatic overview of the IEM event notification message, followed by a description of the elements.
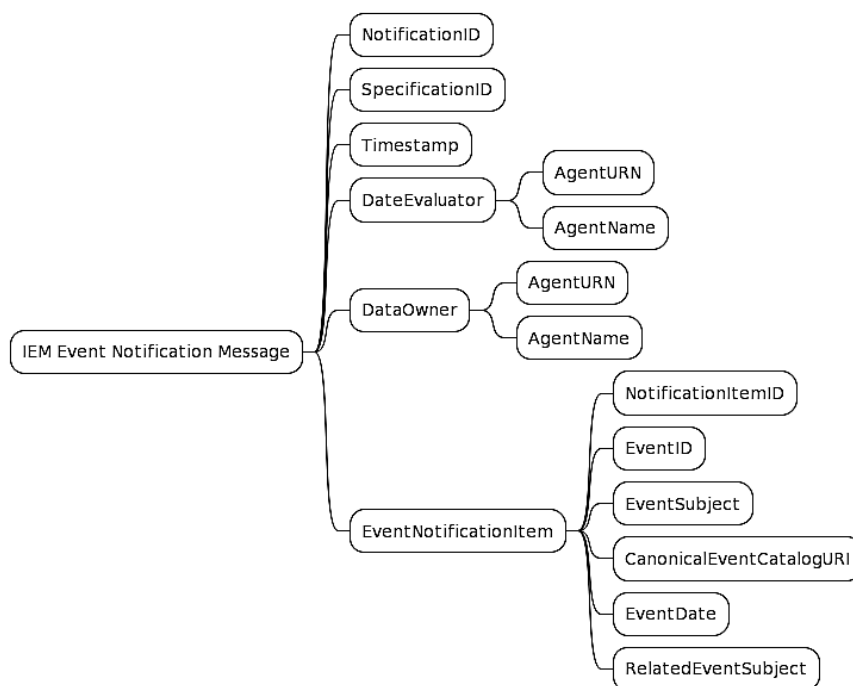
Figure 17: IEM event notification message overview

Description of notification message elements:

▸ **NotificationId**: Unique identifier of the Event Notification Message (e.g., UUID).
▸ **SpecificationId**: Identifier of the IEM Event Notification Message specification.
▸ **TimeStamp**: Day and time of the message sending.
▸ **DataEvaluator**: URN according to the DE4A policy of identifiers and, optionally, the organisation name. This is the addressee of the notification, who is subscribed to one of the DO's event catalogs.
▸ **DataOwner**: URN according to the DE4A policy of identifiers and, optionally, the organisation name. This is the notification sender.
▸ **EventNotificationItem**: list of notification Items that allow more than one event notification from the DO to the DE

Description of notification item elements:

▸ **NotificationItemId**: Unique identifier of the notification item within the event notification message (e.g., a sequential number).
▸ **EventSubject**: Either a physical person or a legal person identifying data using the eIDAS profile attributes (mandatory and optional datasets). Same as the corresponding date subject of the corresponding DE's subscription, to be used as a safeguard for the matching between the notification and the former subscription.
▸ **CanonicalEventCatalogUri**: Unique identifier of a canonical event catalogue according to the DE4A policy of identifiers. Same as the corresponding event catalogue of the corresponding DE's subscription, to be used as a safeguard for the matching between the notification and the former subscription.
▸ **EventId**: Token that identifies the event within the canonical event catalogue.
▸ **EventDate**: Date and time when the specified event happened.
▸ **RelatedEventSubject**: In some cases, the event not only involves the event subject but other subjects (e.g., companies merges).

7 Conclusions

This deliverable provides the final set of design guidelines for DE4ASem, the DE4A Semantic Framework, that ensures that the correct format and meaning of exchanged data and information are preserved and understood throughout exchanges between DE4A Member States, according to the requirements provided in D3.2 *"Final Requirements for the Semantic Assets"* needed to deliver integrated cross-border public services.

The basis of the DE4A Semantic Framework was set in D3.3 *"Semantic Framework - Initial Version"* [3], by first assessing existing data models of EU infrastructure, metadata efforts, and vertical systems for evidence exchange using semantic standards (e.g., ISA^2, and W3C). Based on those guidelines and taking into account new data models, semantic components, and requirements for the second iteration of DE4A pilots, the current deliverable proposes a final DE4A Semantic Framework, consisting of the **pilot-specific canonical evidence models** that provide the basis to develop common evidence data models, the **Information Desk final specification**, and the **Information Exchange Model final specification**. Conclusively, the key design guidelines provided here for the **semantic toolkit** lead to the implementation that is described in D3.6 *"Semantic Toolkit – Final Version"*.

References

[1] GitHub - SEMICeu/SDG-sandbox: The SDG Sandbox creates a space for the review of data models produced by WP4 - Data semantics, formats and quality - in the context of the preparatory work for the Single Digital Gateway Regulation. (2022). Retrieved 24 February 2022, from https://github.com/SEMICeu/SDG-sandbox

[2] DE4A Project Deliverable D2.4: Project Start Architecture, [online], available at: https://www.de4a.eu/_files/ugd/f739c2_fa17b6508b4744bf9872b59faa70cca3.pdf

[3] DE4A Project Deliverable D3.3: Semantic Framework- Initial version, [online], available at: https://www.de4a.eu/_files/ugd/f739c2_bbefa1524d5f4dc9917b049cee1c28f6.pdf

[4] TOOP Solution Architecture v2.1 – 2020 Edition, [online], available at http://wiki.ds.unipi.gr/display/TOOPSA210CEF, Accessed on 31 January 2022

[5] Core Person Vocabulary. Retrieved 31 January 2022, from: https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/solution/e-government-core-vocabularies/core-person-vocabulary

[6] Core Business Vocabulary. Retrieved 31 January 2022, from: https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/solution/e-government-core-vocabularies/core-business-vocabulary

[7] Core Location Vocabulary. Retrieved 31 January 2022, from: https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/solution/e-government-core-vocabularies/core-location-vocabulary

[8] Core public Organization Vocabulary. Retrieved 31 January 2022, from: https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/solution/e-government-core-vocabularies/core-public-organisation-vocabulary

[9] Core Criterion and Core Evidence Vocabulary. Retrieved 31 January 2022, from: https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/solution/e-government-core-vocabularies/core-criterion-and-core-evidence-vocabulary

[10] DCAT Application Profile specification. Retrieved 31 January 2022, from: https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/solution/dcat-application-profile-data-portals-europe

[11] Asset Description Metadata Schema – Application Profile (ADMS-AP). Retrieved 31 January 2022, from: https://joinup.ec.europa.eu/solution/asset-description-metadata-schema-adms/distribution/adms-ap-version-201-pdf, retrieved 2020/03/20.

[12] Base registries. Retrieved 31 January 2022 from: https://joinup.ec.europa.eu/collection/access-base-registries/about.

[13] Registered Organization Vocabulary. Retrieved 31 January 2022, from: https://www.w3.org/TR/vocab-regorg/

[14] Organization Ontology. Retrieved 31 January 2022, from: https://www.w3.org/TR/vocab-org/

[15] TOOP CERB- Criterion and Evidence Type Rule Base. Retrieved 31 January 2022, from: http://wiki.ds.unipi.gr/display/TOOPSA20/Criterion+And+Evidence+Type+Rule+Base, retrieved

[16] TOOP Data Service Directory. Retrieved 31 January 2022, from: http://wiki.ds.unipi.gr/display/TOOPSA20/Data+Services+Directory, Accessed on 15 August 2020

[17] TOOP Exchange Data Model. Retrieved 31 January 2022, from: https://wiki.ds.unipi.gr/display/TOOPSA210CEF/TOOP+Exchange+Data+Model

[18] TOOP Registry of Authorities. The Once-Only Principle Project. Retrieved 31 January 2022, from: http://wiki.ds.unipi.gr/display/TOOPSA210CEF/Registry+of+Authorities

[19] Verifiable Claims Data Model and Representations. Retrieved 31 January 2022, from: https://github.com/w3c/vc-data-model.

[20] Verifiable Credentials Data Model. Retrieved 31 January 2022, from: https://www.w3.org/TR/vc-data-model/.

[21] EDCI Data Model. Retrieved 14 February 2022 from: https://europa.eu/europass/en/european-digital-credentials-learning-interoperability

[22] EUR-Lex - 32016R1191 - EN - EUR-Lex. (2022). Retrieved 24 February 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R1191

[23] Canonical Evidence - DE4A. (2022). Retrieved 24 February 2022, from https://wiki.de4a.eu/index.php/Canonical_Evidence

[24] GitHub - de4a-wp3/moving_abroad: Repository of canonical evidences of Moving Abroad Pilot. (2022). Retrieved 24 February 2022, from https://github.com/de4a-wp3/moving_abroad

[25] W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures. (2022). Retrieved 24 February 2022, from https://www.w3.org/TR/xmlschema11-1/

[26] W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes. (2022). Retrieved 24 February 2022, from https://www.w3.org/TR/xmlschema11-2/

[27] Tasker, P.S., Shadle, W.F., Anderson, J.P., & Lipner, S.B. (2001). Trusted Computer System Evaluation Criteria (Orange Book) December.

[28] SDG Regulation. EUR-Lex Document 32018R1724. Annex II. Retrieved 4 February 2022 from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1724#d1e32-36-1

[29] SDG Regulation. Procedures under Directive 2005/36/EC. Retrieved 4 February 2022 from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0036.

[30] SDG Regulation. Procedures under Directive 2006/123/EC. Retrieved 4 February 2022 from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0123.

[31] SDG Regulation. Procedures under Directive 2014/24/EU. Retrieved 4 2022 February from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0024

[32] SDG Regulation. Procedures under Directive 2014/25/EU. Retrieved 4 February 2022 from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0025

[33] IEM Common Types. Retrieved 4 February 2022 from: https://github.com/de4a-wp3/IEM/blob/main/iteration2/common-types.xsd

[34] Application profiles - EU Vocabularies - Publications Office of the EU. (2022). Retrieved 24 February 2022, from https://op.europa.eu/el/web/eu-vocabularies/application-profiles

[35] Controlled vocabularies - EU Vocabularies - Publications Office of the EU. (2022). Retrieved 6 February 2022, from https://op.europa.eu/en/web/eu-vocabularies/controlled-vocabularies

[36] Code lists - Eurostat. (2022). Retrieved 6 February 2022, from https://ec.europa.eu/eurostat/data/metadata/code-lists

[37] SDGR, 14401/1/17 REV 1, Brussels, 28 November 2017, Article 3(1). Retrieved 6 February 2022 from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0001.01.ENG&toc=OJ:L:2018:295:TOC#003

[38] Data Model | Glossary | SCOOP4C. (2022). Retrieved 15 February 2022, from https://scoop4c.eu/glossary

[39] Documentation eDelivery. (2022). Retrieved 24 February 2022, from https://ec.europa.eu/digital-building-blocks/wikis/display/CEFDIGITAL/Documentation+eDelivery

[40] DE4A Project deliverable D2.1: Architecture Framework, page 55, 8.1 Intermediation Pattern. [online], available at https://www.de4a.eu/project-deliverables

[41] Once-Only Principle. Retrieved 6 February 2022 from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN

[42] Formal ontology - EU Vocabularies - Publications Office of the EU. (2022). Retrieved 9 February 2022, from https://op.europa.eu/en/web/eu-vocabularies/concept/-/resource?uri=http://publications.europa.eu/resource/authority/asset-classification/c_89b4bdb7

[43] DE4A Project Deliverable D4.1: Studying Abroad- Use Case Definition and Requirements. Glossary. [online], available at: https://www.de4a.eu/_files/ugd/2844e6_cd8abc5ce50048fa8fc32bb283775bc9.pdf

[44] Proof. Retrieved 7 February from : https://dictionary.cambridge.org/dictionary/english/proof

[45]Proof. Retrieved 7 February from: https://www.merriam-webster.com/dictionary/proof

[46] Public Service. Glossary of summaries - EUR-Lex. (2022). Retrieved 25 February 2022, from https://eur-lex.europa.eu/summary/glossary/public_service.html

[47] Taxonomy - EU Vocabularies - Publications Office of the EU. (2022). Retrieved 9 February 2022, from https://op.europa.eu/en/web/eu-vocabularies/concept/-/resource?uri=http://publications.europa.eu/resource/authority/dataset-type/TAXONOMY

[48] The Once-Only Principle Project | TOOP.EU. (2022). Retrieved 10 February 2022, from https://toop.eu/info

[49]Ontologies - W3C. (2020). Retrieved 24 February 2022, from: https://www.w3.org/standards/semanticweb/ontology