D2.8 Beyond interoperability: One Network for Europe (ONE)

Document Identification			
Status	Final	**Due Date**	28/02/2023
Version	1.0	**Submission Date**	22/03/2023

Related WP	WP2, WP4	**Document Reference**	D2.8
Related Deliverable(s)	D2.8 builds upon D2.5, D2.7 and D4.1, D4.5, D4.9 and forthcoming pilot results	**Dissemination Level (*)**	PU
Lead Participant	MinBZK/ICTU	**Lead Author**	Alexander Bielowski (MinBZK/ICTU)
Contributors	Mavi Cristache (MinBZK/ICTU), Carl-Markus Piswanger (BRZ/BMF)	**Reviewers**	Muhamed Turkanović (UM)
			Harold Metselaar (MinBZK/ICTU)

Keywords:
Architecture, Once-Only Technical System, European Digital Identity, Wallet, eDelivery, Interoperability, Digital Decade, People-centricity, Sovereignty, eGovernment, Digital Single Market, European Digital Identity Wallet, Policy

Document Information

List of Contributors	
Name	Partner
Alexander Bielowski	MinBZK/ICTU
Mavi Cristache	MinBZK/ICTU
Carl-Markus Piswanger	BRZ/BMF

List of Interview Partners	
Name	Organisation
Alberto Crespo	Atos Research & Innovation
Hans Graux	TIMELEX
Ana Rosa Guzmán Carbonell	General Secretariat for Digital Administration, Spain
Fredrik Linden	MyData Sweden
Thashmee Karunaratne	Stockholm University
Prof. Dr. Robert Krimmer	University of Tartu
Dr. Peter Kustor	Federal Ministry of Finance, Republic of Austria
Gérard Soisson	Ministry for Digitalisation - Luxembourg

Document History			
Version	Date	Change editors	Changes
0.0	01/09/2022	Alexander Bielowski, Mavi Cristache (ICTU)	Tables of contents and references
0.1	13/10/2022	Alexander Bielowski, Mavi Cristache	Review of document concept and structure
0.1.1	14/10/2022	Alexander Bielowski	Drafted first outline
0.1.2	16/10/2022	Alexander Bielowski	Drafted first outline
0.1.3	17/10/2022	Alexander Bielowski	Drafted first outline
0.1.4	18/10/2022	Alexander Bielowski	Drafted first outline
0.1.5	20/10/2022	Carl-Markus Piswanger	Review first outline
0.1.6	02/11/2022	Alexander Bielowski, Mavi Cristache	Literature review (Chapter 1.3) Review of references
0.1.7	09/11/2022	Alexander Bielowski, Mavi Cristache	Literature review (Chapter 1.3) Review of references

Document History			
Version	Date	Change editors	Changes
0.1.8	16/11/2022	Alexander Bielowski, Carl-Markus Piswanger (BRZ)	Aligned ToC with Interview guide
0.1.9	30/11/2022	Alexander Bielowski	Literature review (Chapter 1.3)
0.1.10	03/12/2022	Alexander Bielowski	Literature review (Chapter 1.3)
0.1.11	04/12/2022	Alexander Bielowski	Literature review (Chapter 1.3)
0.1.12	07/12/2022	Alexander Bielowski	Literature review (Chapter 1.3)
0.1.13	09/12/2022	Alexander Bielowski	Literature review (Chapter 1.3)
0.1.14	11/12/2022	Alexander Bielowski	Literature review (Chapter 1.3)
0.1.15	16/01/2023	Alexander Bielowski	Literature review (Chapter 1.3)
0.1.16	18/01/2023	Alexander Bielowski	Literature review (Chapter 1.3)
0.2.0	22/01/2023	Alexander Bielowski	Introduction to chapter 1.3
0.2.1	26/01/2023	Alexander Bielowski Carl-Markus Piswanger	Introduction to chapter 1.3 Consolidation of interview responses
0.2.2	27/01/2023	Alexander Bielowski, Carl-Markus Piswanger	Section 2.1 Consolidation of interview responses
0.2.3	28/01/2023	Alexander Bielowski	Section 2.2, structuring 2.3 and 2.4
0.2.4	29/01/2023	Alexander Bielowski	Section 2.3, 2.4, 2.5, structuring 2.7
0.2.5	30/01/2023	Carl-Markus Piswanger	Analysis of interview responses (Chaper 3)
0.2.5	01/02/2023	Alexander Bielowski Carl-Markus Piswanger	Complete draft chapter 1.3 Analysis of interview responses (Chaper 3)
0.2.6	03/02/2023	Alexander Bielowski	Finalize chapter 1.3
0.3	06/02/2023	Carl-Markus Piswanger	Chapter 3 elaborated and included
0.3.1	08/02/2023	Alexander Bielowski	Outline of chapter 4
0.3.2	09/02/2023	Alexander Bielowski	Introduction of chapter 4 and Section 4.5, Annex I & II
0.3.3	10/02/2023	Alexander Bielowski Carl-Markus Piswanger	Sections 4.1, 4.2 and 4.3 Annex III
0.4	11/02/2023	Alexander Bielowski	Complete draft of chapter 4
0.4.1	12/02/2023	Alexander Bielowski	Chapter 5, Addition of 4.5.5, Execution Summary
0.4.2	13/02/2023	Alexander Bielowski	Reference List List of Interview Partners

Document History			
Version	Date	Change editors	Changes
0.5	15/02/2023	Carl-Markus Piswanger Alexander Bielowski	Update Chapter 3and Annex IV and V, List of Acronyms, Final Edit
0.6	06/03/2023	Alexander Bielowski	Internal review results
0.9	09/03/2023	Alexander Bielowski	Final Edits
0.91	20/03/2023	Julia Wells (ATOS)	Update for conformity to template, final quality review for submission
1.0	22/03/2023	Ana Piñuela Marcos (ATOS)	Final for submission

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Alexander Bielowski (MinBZK/ICTU)	09/03/2023
Quality manager	Julia Wells (ATOS)	20/03/2023
Project Coordinator	Ana Piñuela Marcos (ATOS)	22/03/2023

Style Disclaimer

References to generic third persons are made by means of the singular '*they*' (and its variants *them, their, themself*).

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AAA	Authentication, Authorization and Accounting
API	Application Programming Interface
BB	Building Block
BPM	Business Process Model
BRIS	Business Register Interconnection System
CEF	Connecting Europe Facility
Connect / (DG) CNECT	The European Commission's Directorate-General for Communications Networks, Content and Technology
DE4A	Digital Europe for All
DIGIT / (DG) DIGIT	The European Commission's Directorate-General for Informatics
DRL	Digital Read Legislation
DSM	Digital Single Market
Dx.y	DE4A formal Deliverable x.y (e.g. D2.5)
E2E	End-to-end
EBSI	European Blockchain Services Infrastructure
EC	European Commission
EESSI	Electronic Exchange of Social Security Information
eID	Electronic identity
eIDAS	EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. It was established in EU Regulation 910/2014.
EIF	European Interoperability Framework
EIRA	European Interoperability Reference Architecture
EAA	Electronic Attestation of Attributes
EUDIW	European Digital Identity Wallet
EUID	European Unique Identifier
ICT	Information and communications technology
IEB	Interoperable Europe Board
IOP	InterOPerability
ISA(^{2})	Interoperability Solutions for Public Administrators programme
LSP	Large scale pilot
MS	European Union Member State(s)
MOR	Multilingual Ontology Repository
ONE	One Network for Europe
OOTS	Once-Only Technical System
PoR	Powers of Representation
PSA	Project Start Architecture
RBAC	Role-based Access Control

Abbreviation / acronym	Description
REST	Representational state transfer
SDG	Single Digital Gateway
SDGR	Single Digital Gateway Regulation
SLA	Service level agreement
SSI	Self-sovereign identity
Tn.m	DE4A formal project Task n.m (e.g. T2.3)
VC	Verifiable Credential
VP	Verifiable Presentation
WP	Work Package

Executive Summary

European digital policy and recent developments, such as the European Digital Identity Framework, show a first outline of a future that goes beyond eGovernment Interoperability. A thorough analysis of current EU policy documents reveals an underlying vision of a seamless Digital Single Market (DSM) ecosystem - One Network for Europe ONE, exhibiting the following eight aspects:

- Overcoming the Boundaries Between Public, Private and Third Sector
- A European Ecosystem Instead of Interconnecting National Silos
- People-centricity and Sovereignty
- Inclusion
- Free Flow of Data
- Secure and Trusted Environment
- Increasing role of the government
- Cross-sectoral Governance on European Level

Expert interviews were used to collect insights into practical steps towards this vision, exploring what would be needed to create a European DSM ecosystem that will maximise the growth potential of our European Digital Economy, provide an optimal breeding ground for digital start-ups and at the same time be people-centric and preserve our privacy and sovereignty as EU citizens.

From the interviews we see confirmed that **harmonization** cannot stop on the legal level but needs to include the level of organisational and technical specifications while being mandatory for both EU and Member State level. This requires strengthened **governance** of the digitization of Europe. The proposed Interoperable Europe Act [9] is seen as a very important step in the right direction with the expectation that the Interoperable Europe Board will evolve over time to the central governance body, with an even stronger mandate than defined in the first proposal. The insight gained for the interviews concerning the future **architecture** confirmed the importance of the EUDIW and the central role of harmonized semantics allowing automated reuse of information across the Union. Interestingly the second focus of architecture related responses are closely related to the harmonization and governance, calling for the use of standards, the use of common description languages, improved cartography of ready-to-use toolboxes. A very concrete focus was put on **data** in enabling the data-driven economy: data should be easily available across the Union with a data access logic managed on EU-level.

On the basis of the interview results, the literature analysis and the insights gained in from de DE4A project, a functional architecture landscape was derived, consisting of 6 functional areas, containing 21 architecture elements (or components) of which only some highlights are summarized here.

In the **User** area, we found that the EUDIW is a very powerful basis for two people-centric components: that we called the human Digital Twin and European Passepartout. The human Digital Twin will need to consist of multiple, separate personas in order to be privacy preserving. The European Passepartout is a universal, yet not uniform, “master key“ that must support both full as well as pseudonymous identification to allow separate personas to behave independently from each other.

Legally valid, harmonized structured data that can be directly reused in a fully automated way (cf. canonical evidence or electronic attestation of attributes) is the most prominent element in **Data and Sources**. Other important element is a catalogue (or catalogue of catalogues) of roles (and professions and rights) and data services and a multilingual ontology repository. These catalogues and repositories must allow automated querying and validation against them (cf. trust lists).

The elements of the **Usage and Functionality** area draw a picture of loosely coupled business services that break open the national and sectoral silos an can be used irrespective of the origin within the Union or ownership (public or private) of the service. These services would build on standard protocols and as far as possible on ready-to-use building blocks.

The above builds on **Horizontal Functions**, namely a Multi-pattern Exchange Architecture and an Attestation-based Access Management System. The latter is expected to use validation against the catalogue of roles and the ontology repository.

Some elements that are required for the preparation and initialization of the ecosystem are compiled in the **Prerequisites**. Digital ready legislation and the availability of interoperability skills fall in this area, as does the need for a DSM value model.

Not of the least importance is the area of **Governance**, which is structured top-down, from the need to be stronger involved in international governance to the need to anchor operational governance in a permanent interoperability agency.

Overall, we see that current developments, such as the OOTS [12] [13], the EUDIW[16][17][9] as well as regulatory measures such as the Interoperable Europe Act are all moving Europe towards the ONE vision. There are, however, nine points that require further attention research:

1. Legal validity of structure data should be established on European Level.
2. There is an apparent need to interoperability agreements that are binding across the Union and applicable for both the public as the private sector, yet less rigid than laws.
3. Our governments should claim their role in the Governance of an interoperable Europe that extends from the eGovernment domain to cover the entire DSM, hence including private actors. This requires establishing strong European digital governance bodies.
4. Member states and the Commission should take a proactive and coordinated stance in international governance bodies concerning questions of the digital economy, including international standardization bodies.
5. The Wallet should be a European Passepartout supporting pseudonymous identification and allowing the user to manage the different personas of their human Digital Twin in a privacy-enhancing way.
6. The management of semantics should be recognized as a European endeavour, including the creation of multilingual ontology repositories and a semantic elicitation approach to create and maintain ontologies on European level.
7. The creation of an attestation-based access management logic that must be highly decentralized, yet applicable across the Union and across different channels requires further research and development, as it is crucial for the success of the DSM.
8. The OOTS and EUDIW provide a good basis for establishing a muti-pattern exchange architecture, but establishing such a horizontal, multi-pattern architecture should be recognized as an overarching goal and managed consistently.
9. A value model of the DSM should be developed to mitigate the risk of value dissipating from budget financed services to commercial enterprises.

Concluding, we can establish that attaining the ONE-vision of a seamless Digital Single Market Ecosystem does depend more on conceptual and governance challenges than the lack of technological capability. Using our specific strength and trusting in "*the best of Europe - open, fair, diverse, democratic, and confident*" [3] we should indeed be able to achieve the goal that "*Europe must lead the transition to a [..] a new digital world.*" [10].

1. Introduction

1.1. Purpose of the Document

One objective of DE4A is to envision different target architecture states at different time horizons that provide guidance to the further development of European governmental interoperability solutions and platforms. This deliverable presents a consolidated architecture vision for the long-term time horizon, specifically the time beyond this Digital Decade [4]. The starting hypothesis is that the digital transformation of European administrations, national governments and public authorities has a profound impact on the development of the data-driven economy and the social and economic reality of the single market and its global competitive position.

The objective of D2.8 is to provide guidance and focus for architects and policy makers both on Union and Member State level. The authors attempt to put forward a positive, ambitious, yet attainable, architecture vision of the future of interoperability that transcends both national boundaries and classical roles of public administration, private and third sector. This vision for One Network for Europe (ONE) builds on insights and direction derived from current EU policy documents and regulations and covers a range of legal, semantic, organizational, and technical solution elements or approaches. These key solution elements are derived, following an inductive approach, from semi-structured interviews with renowned European experts in the area of cross-border eGovernment interoperability and the digital economy.

1.2. Research Method and Structure of the Document

The research consists of two mayor parts. First, a literature review of recent EU policy documents and regulations uses a deductive approach, to validate the starting hypothesis: Current EU policy is directed towards the vision of a seamless Digital Single Market (DSM) ecosystem. This analysis resulted in 8 aspects of the ONE vision described in **chapter 2**.

Second, a series of semi-structured interviews was performed with European experts to collect ideas on actionable "solution elements" that would need to be put in place to attain the ONE vision. Current policy focusses approximately 10 years into the future – the Digital Decade – and does so from a strategic, goal-setting perspective. The interviews aimed to look beyond this decade and were set up to collected thoughts, ideas and dreams that usually life in the margins of the daily work and mostly remain undocumented. The responses are analysed in **chapter 3**.

In **chapter 4**, the authors apply inductive reasoning based on the policy insights, interview results and insights gained in the course of the DE4A project to derive a landscape of functional architecture elements that are required for attaining the general vision outlined in chapter 2.

The document concludes in **chapter 5** with a summary of the main findings.

1.3. Relation to other DE4A Deliverables

D2.8 builds upon insight from the DE4A Project Start Architectures D2.5 [26], insight obtained from the pilots as well as the insights from the mid-term target architecture description brought forward in D2.7 (Interoperability Architecture for Cross-border Procedures and Evidence Exchange in light of the Single Digital Gateway Regulation). Alignment meetings where held with WP6 "Sustainable impact and new governance models" and WP7 "Legal and ethical compliance and consensus building" as their deliverables were written in parallel. D2.8 is an externally directed report and has no directly dependent deliverables in DE4A.

2. Long-term EU Policy Perspective on the Digital Single Market and European Interoperability

The European Commission (EC) defined the Digital Single Market (DSM) in 2015 as "[..] one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence." [1] The importance of achieving a DSM is highlighted as it "will ensure that Europe maintains its position as a world leader in the digital economy, helping European companies to grow globally." [1] One way in which this is happening is, because a DSM "[..] can create opportunities for new start-ups and allow existing companies to grow and profit from the scale of a market of over 500 million people." [1] in an environment where "[..] most economic activity will depend on digital ecosystems, integrating digital infrastructure, hardware and software, applications and data." [1]

The notion that "Digital technologies are profoundly changing our daily life, our way of working and doing business, and the way people travel, communicate and relate with each other […]" [3] was reconfirmed by the EC in 2020 and thought to be "as fundamental as [the transformation] caused by the industrial revolution." [3]. The unchanged or even increased importance of the DSM for "Shaping Europe's Digital Future" is expressed in the 2nd key objective for "A fair and competitive economy: A frictionless single market, where companies of all sizes and in any sector can compete on equal terms, and can develop, market and use digital technologies, products and services at a scale that boosts their productivity and global competitiveness, and consumers can be confident that their rights are respected." [3]

This continued focus on the DSM is also mirrored in the 2030 Digital Compass: "Digitalisation endows people with new sources of prosperity, allowing entrepreneurs to innovate, set up and grow their business wherever they live, opening markets and investments across Europe and globally, and creating new jobs at a time when an increasing number of Europeans feel threatened in their economic security or environment."[4] and in the Berlin Declaration that put forward the objective to "Foster resilience and sustainability by strengthening the Digital Single Market that reaps the economic and social benefits of digitalisation and connectivity for citizens in all countries and regions;" [5]

Among all achievements that were attained along the tree pillars of the Digital Single Market Strategy [1] we would like to mention especially the EU regulatory achievements that were concluded by "A new Digital Services Act [that upgrades] our liability and safety rules for digital platforms, services and products, and complete our Digital Single Market." [10]: The Open Data Directive [7], the Digital Markets Act [6] and the European Declaration of Digital Rights and Principles [8]. Additionally, the ongoing investment in the Single Digital Gateway (SDG) [12] and the Once-Only Technical System (OOT) [13] must be highlighted as essential for the DSM. They build on the important investments made is context of CEF [14] and ISA^2 [15]. However, and without disesteem for the great achievements of creating a DSM in period from 2015 to 2021, we clearly can observe a broad consensus for the importance of further fostering the DSM [3] [4] [5] in the decade(s) ahead: "our stated ambition is more relevant than ever: to pursue digital policies that empower people and businesses to seize a human centred, sustainable and more prosperous digital future." [4]

Europe also has specific strengths that gives confidence for the long-term future of the digital economy where the DSM will not only "maintains its position as a world leader in the digital economy" [1] but can develop into the leading digital economy: "an open and competitive single market, strong rules embedding European values, being an assertive player in fair and rule-based international trade, its solid industrial base, highly-skilled citizens and a robust civil society." [4] And leadership in the digital economy goes beyond economic strength: "This digital Europe should reflect the best of Europe - open, fair, diverse, democratic, and confident" [3] In more practical terms this means: "putting people at the

centre of the digital transformation; underlying solidarity and inclusion; restating the importance of freedom of choice; participation in the digital public space; safety, security and empowerment; and sustainability" [8] in pursuit of the goal that "Europe must lead the transition to a healthy planet and a new digital world." [10].

Summarizing, "The European way to a digitalised economy and society is about solidarity, prosperity, and sustainability, anchored in empowerment of its citizens and businesses, ensuring the security and resilience of its digital ecosystem and supply chains." [4] One required property of this DSM ecosystem is interoperability across Europe; The barriers in the DSM are not only regulatory in nature and exist on all levels of the European Interoperability Framework [EIF] [2]: legal, organisational, semantic and technical. The EIF provides extremely valuable insights and direction for achieving and governing cross-border interoperability and the authors highly recommend the application of its recommendations and principles. Whether we use the definition of interoperability from EIF[1] or the proposed Interoperable Europe Act[2] [9], however, interoperability in this context focusses on eGovernment and public services. This is in stark contrast with the much wider long-term aspiration of the DSM outlined above. If the DSM ecosystem is to be an environment "where individuals and businesses can seamlessly access and exercise online activities" [1], then we ought to move beyond the public service centred understanding of interoperability and envision a consistent and seamless, digital environment. Breaking down the barriers that exist in the DSM on all EIF layers, we can see "One Network for Europe" (ONE) emerge. This chapter outlines eight aspects of the ONE-vision that can be derived from current EU policy documents and regulations.

2.1.Overcoming the Boundaries Between Public, Private and Third Sector

As shown in the introduction above, the DSM ecosystem is about "individuals and businesses [that] can seamlessly access and exercise online activities" [1] and it is clear that "The public sector has an important role in stimulating digital transformation." [10]. Digital public service and government regulated services will be crucial in "ensuring the security and resilience of its digital ecosystem"[4] in which "consumers can be confident that their rights are respected." [3] This means in a long-term perspective, we will need to overcome the boundaries between public, private and third sector digital services, having them build onto each other and reusing each other in a seamless manner.

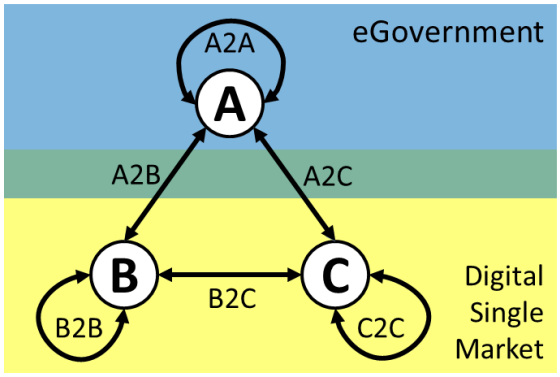

Figure 1: Types of Transactions between Administration, Business and Citizen in eGovernment and the Digital Single Market

[1] For the purpose of the EIF, interoperability is the ability of organisations ['Organisations' here means public administration units or any entity acting on their behalf, or EU institutions or bodies.] to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems. [1]

[2] Article 2 (1) 'cross-border interoperability' means the ability of network and information systems to be used by public sector bodies in different Member States and institutions, bodies, and agencies of the Union in order to interact with each other by sharing data by means of electronic communication; [10]

The objective of the new EIF "to steer European interoperability initiatives contributes to a coherent European interoperable environment, and facilitates the delivery of services that work together, within and across organisations or domains" [2] expresses exactly what is needed, except that their definition of organisation restricts its applicability to the public administration. The scope only "covers three types of interactions: A2A (administration to administration), [..] A2B (administration to business), [..] A2C (administration to citizen)" [1], whereas ONE would need to support another three types to facilitate the next level of the DSM, as shown in Figure 1: B2B (business to business), B2C (business to consumer) and C2C (consumer to consumer, or rather citizen to citizen) transactions. In the remainder of the document, insights and principles from the EIF are consequently treated as best practice guidance beyond the public administration domain.

Recommendations of EIF on interoperability governance are an exception of the above: They cannot be that simply extrapolated across all 6 types of transactions because the government plays very diverse roles in these transactions (cf. section 2.3). The notion that the boundaries between public and private sectors are being overcome in de digital economy, however, is undeniable. Very practical examples are the emergence of GovTech companies and the development of the European Digital Identity Wallet (EUDIW) [16][17]. The latter is explicitly designed to serve the user (natural or legal person) in transactions with both, public and private service providers, hence covers five of the six types of transactions: A2C, A2B, B2C, B2C and C2C. As argued in the DE4A deliverable D2.7 [18], the aforementioned OOTS [13] is a solid basis to evolve into a multi-pattern architecture, fully supporting the sixth type, A2A, in support of A2C and A2B services.

2.2.A European Ecosystem Instead of Interconnecting National Silos

Currently, the eGovernment sector is mostly structured in 'national silos', closely integrated information systems, catering exclusively to the needs of national public service provisioning. Additionally, these silos are often further compartmentalized per sector. This is not at all surprising, as this mirrors the administrative structures on Union and on National Level as depicted in Figure 2. EIF rightfully advocates that "[…], efforts to digitise the public sector should be well coordinated at European and national levels to avoid digital fragmentation of services and data, and help the EU's digital single market to work smoothly" [2], but the efforts of cross-border interoperability, these last decades were mostly focussed on interconnecting national silos with European (sectoral) systems. eDelivery [19], which is a crucial building block in Digital Europe, championed the 4-corner model [20]. This model did not as much advocate a hub-and-spoke architecture of national access points as it enable it to become a dominant implementation model [21], e.g. BRIS[22] and ESSII[23]

This less than optimal situation is clearly recognized by the EC: "Too many European citizens feel like they have different opportunities in certain parts of Europe than they do in others. We need use all the tools at our disposal to put this right." [10] and a more seamless, fully interoperable, digital ecosystem is seen as one of these tools: "Digitalisation can become a decisive enabler of rights and freedoms, allowing people to reach out beyond specific territories, social positions or community groups, and opening new possibilities to learn, have fun, work, explore and fulfil one's ambitions. This will enable a society where geographical distance matters less, because people can work, learn, interact with public administrations, manage their finance and payments, make use of health care systems, automated transport systems, participate to democratic life, be entertained or meet and discuss with people anywhere in the EU, including in rural and remote areas." [4] The Member States recently declared in Berlin their "[…] common political commitment regarding the stated priorities with a view to ensuring high quality, user-centric and seamless cross-border digital public services for citizens and businesses in developing a future-oriented European Single Market." [5]

More specifically, the Berlin Declaration commits to "Strengthen Europe's digital sovereignty and interoperability by establishing common standards and modular architectures;" [5], which is perfectly in line with EIF Recommendation 35: "Decide on a common scheme for interconnecting loosely

coupled service components and put in place and maintain the necessary infrastructure for establishing and maintaining European public services." [2] and EIF Recommendation 36: "Develop a shared infrastructure of reusable services and information sources that can be used by all public administrations." [2] This call for a modular, loosely coupled architecture also resonates in the regulatory provisions of the Open Data Directive [7] that in Article 5 commits to the availability of data "via suitable APIs" and "in formats that are open, machine-readable, accessible, findable and re-usable, together with their metadata. Both the format and the metadata shall, where possible, comply with formal open standards."

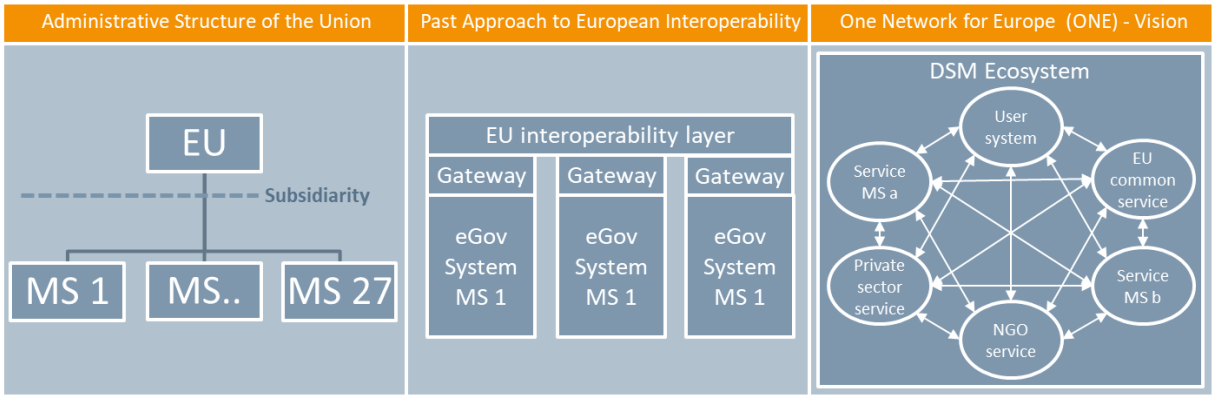

Figure 2: Emergence of a European Ecosystem

These policy and regulatory advancements clearly envision ONE seamless, modular, standards-based, loosely coupled, European ecosystem that dissolves the existing national silos as shown in Figure 2. The EC in their 2030 Compass also sites potential projects under the Recovery and Resilience Fund that would constitute very promising, concrete steps toward that vision: "Building a common and multi-purpose pan-European interconnected data processing infrastructure, to be used in full compliance with fundamental rights developing real-time (very low latency) edge capacities to serve end-users' needs close to where data are generated (i.e. at the edge of telecom networks), designing secure, low power and interoperable middleware platforms for sectoral uses, and enabling easy exchange and sharing of data, notably for Common European Data Spaces;" [4]

2.3. People-centricity and Sovereignty

A third aspect of the long-term ONE vision is people-centricity. The Declaration of Digital Rights and Principles headlines "Chapter I: Putting people at the centre of the digital transformation" [8] and explicitly stated that "The EU vision for digital transformation puts people at the centre, empowers individuals and fosters innovative businesses." [8] several times in the overall text. This is mirrored by the Lisbon Declaration, that calls "for a model of digital transformation that strengthens the human dimension of the digital ecosystem with the Digital Single Market as its core." [24] The assertion that "Citizens no longer feel in control over what happens with their personal data […]." [3] fuels the vision of a "[..] the human-centred, secure and open digital environment [that] should comply with the law, but also further enable people to enforce their rights, such as the rights to privacy and data protection, freedom of expression, the rights of the child and consumer rights.[4] This means that "In the digital space, we need to make sure that the same rights that apply offline can be fully exercised online." [4]

A central notion of the people-centricity appears to be digital self-determination, sometimes also referred to "sovereignty" on the individual level (cf. Self-Sovereign Identity (SSI)). The basic rational is that "Trust in the online world also means helping consumers take greater control of and responsibility for their own data and identity." [3]. According to the Berlin Declaration, for example, "Every citizen and business in Europe should be able to navigate the digital world with confidence and in a self-determined manner. Users should be further empowered to manage their digital identity and to

protect their personal data and privacy online." [5] because "the people of Europe [should] maintain autonomy by keeping control over their data and its use." [5] The idea of self-determination is also picked up and further detailed in the Declaration of Digital Rights, stipulating that "That [the] right [of personal data protection] includes the control on how the data are used and with whom they are shared." [8] The proposed EUDIW [16][17] is a very concrete operationalization of this ambition for self-determination, providing both the functionality for electronic identification and for the sharing of data in form of Electronic Attestations of Attributes (EAA) under full control of the user.

The aspect of self-determination is closely linked with the aspect of sovereignty at the strategic level. This is crucial for attaining the ONE vision, because "Digital sovereignty is key in ensuring the ability of citizens and public administrations to make decisions and act in a self-determined manner in the digital world." [5]. Stated differently: if the means of the DSM are predominantly controlled by companies and governments outside the European Union, then the individual self-determination is at the mercy of powers beyond the democratic control of the people of Europe. Consequently, the EC plans to "carefully assess and address any strategic weaknesses, vulnerabilities and high-risk dependencies which put at risk the attainment of its ambitions and will need to accelerate associated investment. That is the way for Europe to be digitally sovereign in an interconnected world by building and deploying technological capabilities in a way that empowers people and businesses to seize the potential of the digital transformation, […]." [4]

2.4.Inclusion

Inclusion is one European value that is prominently represented in current policy documents on the digital. "A new digital divide has also emerged, not only between well-connected urban areas and rural and remote territories, but also between those who can fully benefit from an enriched, accessible and secure digital space with a full range of services, and those who cannot." [4] Inclusion is hence an aspect that is best treated in its two facets: personal and economic inclusion.

Personal inclusion in the objectives of the EC for 2030 means that "[...] that democratic life and public services online will be fully accessible for everyone, including persons with disabilities." [4] An objective shared by the Member States in the Berlin Declaration that feel that "What is at stake is true digital empowerment of our citizens who want to benefit from a digitalised world. Everyone should be able to seize the opportunities offered by digitalisation. No one should be left behind." [5] and culminating in the commitment to "[...] a digital transformation that leaves nobody behind. It should notably include elderly people, persons with disabilities, or marginalised, vulnerable or disenfranchised people and those who act on their behalf." [8] in the interinstitutional Declaration of Digital Right and Principles.

In the business arena, inclusion means the "support [of the] digital transformation of both innovative and non-digital SMEs [..]. The objective is to achieve a high level of digital intensity, leaving no-one behind." [4] To do so, companies, especially SME need skilled experts, investment in innovation and "a frictionless single market, unhampered by diverging local or national regulations that increase administrative burdens for smaller companies in particular." [3]

2.5.Free Flow of Data

The ONE vison cannot ignore the aspect of the data-driven economy. The Open data principle of EIF from 2017 that focuses on "releasing machine-readable data for use by others to stimulate transparency, fair competition, innovation and a data-driven economy." [2] has matured into the Open Data Directive that stipulated that data owned by public bodies "shall be re-usable for commercial or non-commercial purposes." [7] The economic logic of this development is described by the EC as follows: "For the development of many products and services, data needs to be widely and easily available, easily accessible, and simple to use and process. Data has become a key factor of production, and the value it creates has to be shared back with the entire society participating in providing the

data. This is why we need to build a genuine European single market for data - a European data space based on European rules and values. [3]

From the above follows that it appears sensible for the ONE vision to fully embrace EIF Recommendation 42: "Publish open data in machine-readable, non-proprietary formats. Ensure that open data is accompanied by high quality, machine-readable metadata in non-proprietary formats, including a description of their content, the way data is collected and its level of quality and the licence terms under which it is made available. The use of common vocabularies for expressing metadata is recommended." [2]

2.6.Secure and Trusted Environment

That ONE must be built as in a secure and trusted online environment might appear obvious and the already Digital Market Strategy summarized this very concisely: "The Digital Single Market must be built on reliable, trustworthy, high-speed, affordable networks and services that safeguard consumers' fundamental rights to privacy and personal data protection while also encouraging innovation." [1] More recent policy documents confirm and further detail this notion. The Member States, for example established the "need to ensure that the European Union further strengthens its pioneering role in the research on secure and trustworthy technology design and that the opportunities of Emerging Disruptive Technologies (EDT)" [5] and that "to ensure a free, open and safe digital domain and enhance social trust, fundamental rights and security should be integrated in all policies with a digital dimension." [5]

As matter of fact, security-by-design and privacy-by-design are today widely accepted principles for the digitization of the public sector and are dissipating increasingly also to the private sector to the degree that European citizen may consider this part of their Digital Rights:

- "Everyone should have access to digital technologies, products and services that are safe, secure, and privacy-protective by design." [8]
- "Everyone has the right to the confidentiality of their communications and the information on their electronic devices, and no one shall be subjected to unlawful online surveillance or interception measures." [8]

In addition, the declared Digital Right clearly show that the vision of a secure and trusted environment goes far beyond technical question, like E2E encryption, to the functional aspects and the rules engrained in the digital environment:

- "Everyone has the right to freedom of expression in the online environment, without fear of being censored or intimidated." [8]
- "Everyone should have the means to know who owns or controls the media services they are using." [8]

It is in this context of trust, in addition to people centricity (cf. section 17), that highlights how fundamental the EUDIW [16][17] proposition is considered to be for the long-term benefits of a seamless DSM ecosystem. In the words of the Berlin Declaration, it is required to "Strengthen trust through security in the digital sphere by […] taking steps to make widely usable, secure and interoperable electronic identification and trust services for electronic transactions available for each European resident and providing trustworthy, user-centric, accessible and reliable public services and information;" [5]

Trust and security, however, also present a polarity to privacy and self-determination (cf. section 17). Fake news, the application of targeted advertising to political propaganda, internet trolls and online grooming are all symptoms of a free online environment that point to the legitimate interest to know who said/wrote/published what and when. The Berlin Declaration, for example, states that "European democracy must be protected from both disinformation and outright attacks on elections with due respect for the freedom of expression. All citizens should be able to verify the authenticity of online

information, websites and applications. Everyone, especially children and young people, needs the best possible protection from malicious cyber activity like cyber bullying, mobbing or grooming." [5] Balancing the "due respect" for freedom of expression and privacy in general with the requirement to prevent "malicious cyber activity" targeting individuals and our democratic society as a whole, will be a central challenge in attaining ONE vision of the Digital Europe.

2.7.Role of the government

The long-term vision that emerges from the analysis of current policy documents implies a transformation in the role played by government and public administration. New roles are emerging and existing roles are slowly changing.

This starts with the fundamental role of the **government as regulator** that we see reconfirmed and widened in a Digital Europe. A DSM ecosystem that is secure-by-design and privacy-by-design, is non-discriminatory and seamless across Europe and adheres to European norms and values, respecting our Digital Rights [7] is a rule-based sociotechnical system that demands regulation at a very detailed, even technical level.

Examples of this are Implementing Acts (IA) that put forward the "organisational and technical specifications" of actual information systems, like the OOTS [13] or the long list of IAs that are mentioned in the proposed eIDAS revision [16]. We observe some level of struggling to come to terms with this new, detailed level of regulating sociotechnical systems, i.e. to find the right balance of what needs to be enforced by law (incl. IAs), and what can be covered by different governance approaches, including, but not limited to standards. An example of the latter is recital 96 of the Digital Markets Act: "The implementation of some of the gatekeepers' obligations, such as those related to data access, data portability or interoperability could be facilitated by the use of technical standards." [6]

These same dynamics apply to the **executive function of government**, if ensuring a level playing field in the DSM implied "that rules applying offline – from competition and single market rules, consumer protection, to intellectual property, taxation and workers' rights – should also apply online. Consumers need to be able to trust digital products and service just as much as they would any other." [3]. Information system are, by their very nature, rule-bases systems. For a seamless DSM ecosystem to function, they will need to be become 'rule of law'-based systems. This amounts to the automation of parts of the executive function of government, because much of the behaviour of our information systems is fully automated, without direct intervention or control of a human. It is worth mentioning that this includes "public interests that go beyond competition or economic considerations." [3] Very far beyond, if we consider that we are looking at a vision where "European values and ethical rules and social and environmental norms must apply also in the digital space."[3]

A novel and much more operational role is the **stewardship of the DSM infrastructure**, which follows from the commitment to "fostering responsible and diligent action by all digital actors, public and private, for a safe and secure digital environment;"[8] The majority of the systems making up the DSM, as well as the majority of the organisation providing them will not be part pf the public administration. The interoperable, save and secure functioning of all systems making up the DSM ecosystem cannot be ensured by juridical means alone for two reasons: first, reaction time and second, a much wider scope of compliance than the distinction between legal and illegal behaviour. Stated differently, a service level overrun and even a data breach is by no means always a legal question, but nevertheless requires corrective action. As a consequent, government must assume a role in the operational governance of the ecosystem that extends well beyond the systems that are operated by the public sector.

Another, quite obvious, role is the role as **provider of digital key services**. "People are free to work and relocate and businesses are free to trade and operate in all EU Member States. In doing so, they inevitably have to interact electronically with Member State public administrations." [2] The reason to restrict this to 'key' services if very well explained by EIF principle 10: "Where possible, public

administrations should seek to […] eliminating any [administrative processes] that does not provide public value." [2] This means not only to cut bureaucratic red band, but also to concentrate on services that provide public value.

Some of these key services are associated with the role of the **government as trusted party**. This role is increasingly import and cannot be overstated: "For Europe to truly influence the way in which digital solutions are developed and used on a global scale, it needs to be a strong, independent and purposeful digital player in its own right. In order to achieve this, a clear framework that promotes trustworthy, digitally enabled interactions across society, for people as well as for businesses, is needed. Without this focus on trustworthiness, the vital process of digital transformation cannot succeed." [3] One specific key service that government provides in their role as trust party is the digital identity, which will receive a major update with the EUDIW [16][17]. The DSM will greatly benefit, if participants in digital interactions and especially digital economic transactions can trust in the identity of their counterpart because it is guaranteed by their government.

Next to regulation and taxation, subsidies are considered the third important means available to government for steering societal developments. "In an ever-shrinking world where technology is gaining in importance, Europe needs to continue to act and decide independently and reduce over-reliance on digital solutions created elsewhere." [3] This means that for the digital transformation of Europe to succeed and to safeguard our strategic sovereignty, **government acts as co-investor in digital innovation**: "The Commission will pursue the EU's digital ambitions for 2030 through […] multi-country projects combining investments from the EU, Member States and the private sector" [10]

One specific aspect of investment in innovation in the information economy is that this investment goes beyond technological innovation to include operational expenses in the starting phase of an enterprise. This upfront investment in operation is required to create the critical mass so that positive network externalities grow beyond a value threshold that can sustain the underlying operation. It is this logic [25] that leads to the new type of natural monopolies that are also known as "very large platforms"[6]. The investment in providing every European citizen with an EUDIW, including the investment in public services to provide attestations to these wallets and to use these attestations in public service encounters must be seen as a market-level, up-front investment in such critical mass. This should benefit European start-ups and SME by enabling them to offer innovative digital service and products in the DSM.

The above-mentioned investment in the EUDIW can be understood as one example in which "The public sector has an important role in stimulating digital transformation." [10] The stimulation of the digital transformation, however, goes much further than that and hinds to the role of the **government as community leader**. The Member States in the Berlin Declaration "[.] acknowledge the public sector as an essential element for the European Single Market and a driving force for new and innovative technological solutions for public services and societal challenges. Public authorities at all levels must lead by example to strengthen the tenets of the European Union by adopting the following cornerstone principles in the digital sphere" [5].

2.8.Cross-sectoral Governance on European Level

The eighth aspect of the ONE vision that we can derive from current policy documents is the emergence of a cross-sectoral governance. EIF states that "Historically, applications and information systems in public administrations were developed in a bottom-up fashion, trying to solve domain-specific and local problems." [2] A solution to counter this development is described in EIF Recommendation 32 and builds on the role of the government as community leader: "Support the establishment of sector-specific and cross-sectoral communities that aim to create open information specifications and encourage relevant communities to share their results on national and European platforms."[2]

The emergence of a cross-sectoral governance is additionally fuelled by realisation that the regulatory means available today struggle to deal with the level of governance required to develop, evolve and operate a sociotechnical ecosystem, as mentioned at the beginning of section 2.7 above. The proposed Interoperable Europe Act would to be a very important step in establishing such a governance. It "[..] lays down measures to promote the cross-border interoperability of network and information systems which are used to provide or manage public services in the Union by establishing common rules and a framework for coordination on public sector interoperability, with the aim of fostering the development of interoperable trans-European digital public services infrastructure." [9] For the ONE vision to succeed, this path ought to be followed further to extend this governance beyond the public service domain as a mechanism to relieve the legislative process from regulating technical and operational details and to support government in the stewardship of the DSM ecosystem.

3. Analysis of Interview Results

3.1.Interview and Analysis Approach

Additional to literature research in chapter 2, eight European experts, from the areas of eGovernment, Interoperability, European law and SSI have been interviewed to gather individual views on ONE Network for Europe. The interviews have been conducted along the five EIF IOP layers – Legal, Technical, Semantical, Organisational and Governance (for definition, please refer to Annex II).

In each interview the interviewee was asked to highlight three solution elements per layer, which are seen as essential for future shape and content of the network. As the results show, most of the interviewees named three topics, in rare cases only one or even four topics. Furthermore, each interviewee was asked to highlight the most important points with a ranking and extra points over all named topics in all five layers. This has been included in the interview sheets as such (and as one result) and this interview sheets are available in the Annex IV, nonetheless they are not part of the public results.

Within the process of evaluation, it appeared that it was of main importance to get the wide variety of answers in concise core exclamations, executed in a multi-step concretion. Therefore, the following six steps have been executed in the evaluation:

1. Merging of all answers within the EIF layer structure – all answers with priorities visible
2. Categorisation within the EIF layer structure within subcategories
3. Summarising of the meanings off all individual statements
4. Creation of five mind maps of all summarised meaning for visualisation, incl. subcategories
5. Merging within one combined mind map, incl. further condensed grouping
6. Deduction of core sentences out of the condensed grouping in the combined mind map

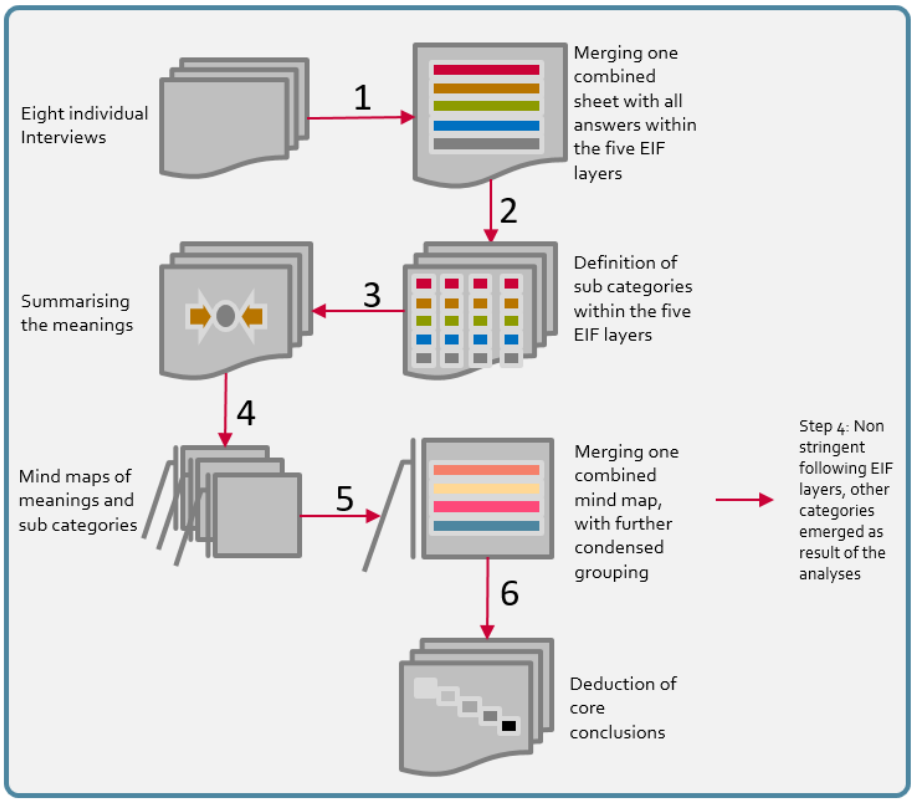

Figure 3: Visualisation of the analysis steps

In the next sections (3.2 to 3.4) the steps for analysis are included as follows:

- *Step 1* results are explained in chapter 3.2 and the questionnaires with all the information are included in Annex IV
- *Step 2* results are explained in chapter 3.2; the results of step 2 are included in the results of step 4
- *Step 3* results are explained in chapter 3.2; the results of step 3 are included in the results of step 4
- *Step 4* results are explained in chapter 3.2 and the five regarding mind maps following the EIF layer categorisation are included in Annex V
- *Step 5* results are depicted in chapter 3.3
- *Step 6* results are included in chapter 3.4

3.2.Explanation of Steps 1 to Step 4 of the Analysis

Step 1

In the first step of the analysis the pure answers of the eight questionnaires have been structured within the five EIF layers and coloured for a better readability and comparability. The colour code of the header sections of each answer area serves for the identification of the related questionnaire (in random order):

Interviewed Person 1
Interviewed Person 2
Interviewed Person 3
Interviewed Person 4
Interviewed Person 5
Interviewed Person 6
Interviewed Person 7
Interviewed Person 8

The structured answers of the questionnaire itself exhibits a substantive and autonomous result.

Step 2

In the second step of the analysis subcategories have been deducted from the answers within each EIF layer, which resulted in first content-related clusters. This step was conducted as a preparatory work to the following step 3 (and consecutive step 4).

Step 3

In the third step of the analysis a summary (of the meaning) to each answer within the subcategories (of step 2) have been included. For the further analysis these summaries have been taken instead of the long versions of the answers. This step was conducted as a preparatory work to the following step 4.

Step 4

In the fourth steps of the summaries and subcategories have been depicted in mind maps following the EIF layer structure as a preparatory work to the following step 5. This “visualisation” itself exhibits a substantive and autonomous result.

3.3. Analysis of the interviews, step 5: Merged Mind Map with further condensed grouping of meanings and subcategories

As shown in the depiction above the EIF layer categorisation shifted into another categorisation, which is shown in the following mind map. A recirculation into the EIF layer categorisation is possible in the following way:

- **Legal IOP** is covered in Governance, especially in Legal Governance / EU Governance
- **Organisational IOP** is interwoven in all categories, also in the new category Harmonisation
- **Semantical IOP** id covered in Architecture, especially in Semantics / Automation / AI
- **Technical IOP** is covered in Architecture and Data
- **Governance IOP** is covered in Governance

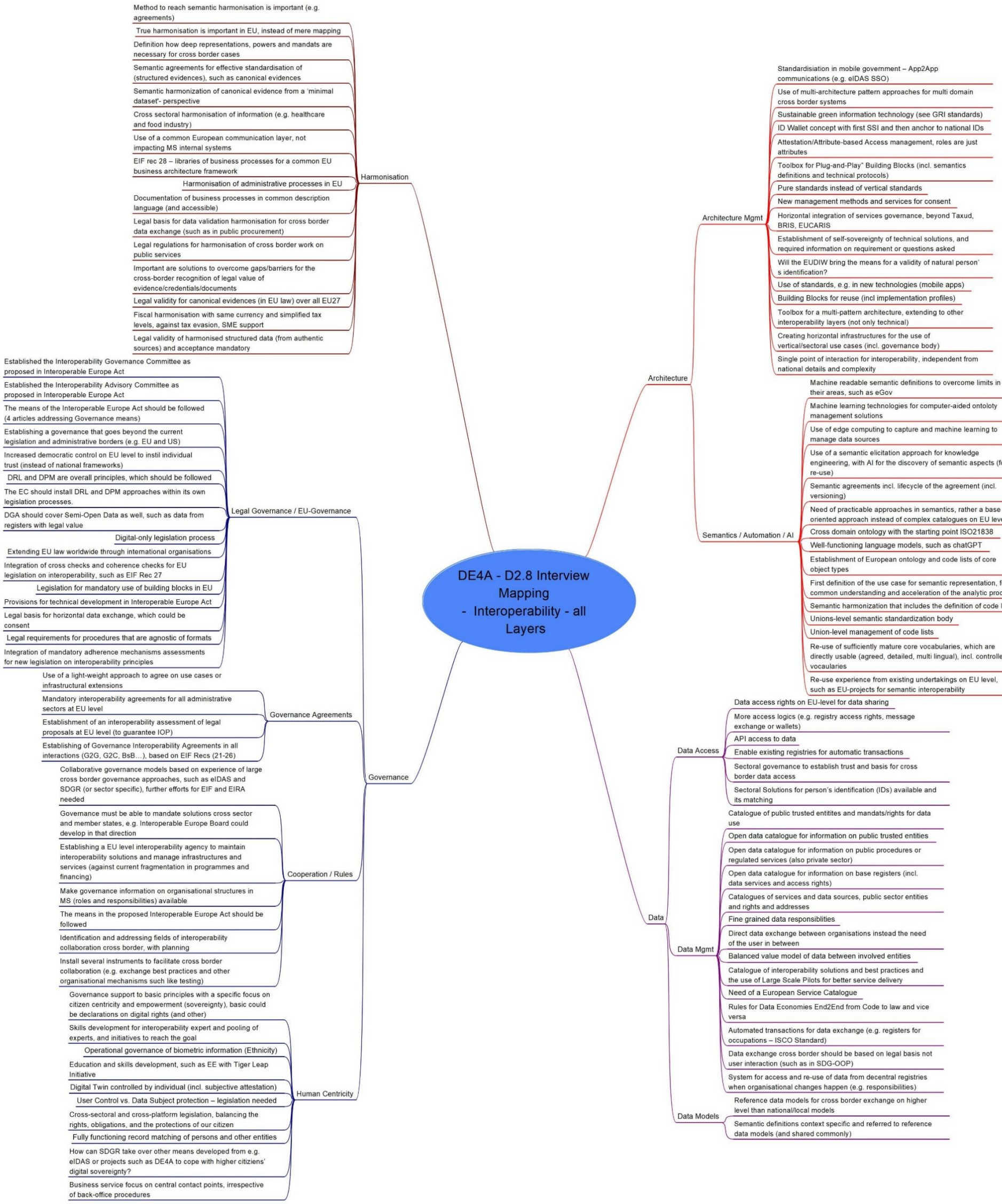

Figure 4: Deducted Mind Map (non EIF Layer Structure)

3.4. Analysis of the interviews, step 6: Deduction of core conclusions in the given categories

The following section represents the last analysis step of the interview results, in which core conclusions have been deducted from the findings depicted in the combined mind map.

3.4.1. Category Harmonisation

Data and its legal validity should be harmonised (on EU level) and made mandatory for information exchange both for EU and MS. The EU should provide instruments to overcome the gaps and barriers.

From the harmonisation [1] of the legal regulations to the [2] administrative processes to [3] the cross-border services from MS and [4] to the harmonisation of Semantics and [5] data with legal valid canonical evidences and to overcome the problem with mapping

- This should be mandatory for all parties – EU and MS
- For the harmonisation a common description language should be used
- Harmonisation on EU level that the MS can use without altering their own systems
- Harmonisation of data and documentations, use of common libraries; furthermore, documentation of processes
- The use of specific instruments should help to overcome gaps and barriers in cross border recognition of data (in this meaning evidences/documents and credentials)
- Moreover, fiscal harmonisation is important, overall with simplified tax systems, for support of SME in cross-border business

3.4.2. Category Governance

Open up information on Governance within the EU. The IEA should support governance in Europe with its instruments. A clear and simple organisation on EU level on governance (and IOP) should foster European enforcement. Experts are important, and in this case the development of skills on IOP. User centricity is important as well as well as a working record matching, with a focus on European undertakings.

Legal Governance/EU-Governance

- The IOP Governance Committee (and IOP Advisory Committee) as proposed in IOP Europe Act should be established, and also the means in the four governance-related articles, furthermore, should the IEA cover technical provisions
- Governance should be extended internationally together with international organisations and under stronger democratic control
- European legislation should include use of building blocks, semi-open data (DGA) and horizontal data exchange (consent?), and should be generally extended to digital-only legislation
- DRL/DPM should be followed, also for EU legislation processes
- Legislation on interoperability should follow coherence checks following EIF[2] Rec 27 and mandatory adherence mechanisms assessments for new legislations on IOP
- Legal requirements on data agnostic on formats

Governance Agreements

- More agreements: on governance on IOP and mandatory IOP on administrative level (EU), incl. assessment and on light-weight use case definitions

Cooperation and Rules

- National governance information on organisational structures should be made public and fields of IOP for cross border collaboration should be identified and planned
- Experience in establishing governance models from EU-projects and legislations should be used (also EIF and EIRA) and the means of the IEA should be followed

- Formal system to mandate MS to common governance rules and a governance structure – [1] Interoperable Europe Board and [2] agency for maintaining interoperability governance (solutions, infrastructure, programmes, financing)

Human Centricity

- Fostering skills and education to create experts for interoperability and expert pools
- Citizen and user centricity and empowerment (sovereignty, digital rights declaration), also for the Digital Twin; incl. cross sectoral/platform legislation and data protection – also in existing European undertakings such as SDGR
- Necessity of governance rules for the use of biometrics
- Record matching for persons (natural and legal)

3.4.3. Category Architecture

Fostering the use of pure standards (e.g. mobile) and the provision of toolboxes for re-use of services and easy to use services. EUDIW should focus on self-sovereignty and then on national eIDs.. Methods for access management, incl. roles/attributes are required. Horizontal infrastructures should support vertical/sectoral services.

Establishment of an EU level semantic standardisation body. Semantics should be built up bottom up for better understanding and on basis of experience. Machine readability could support the semantic definitions; machine learning could be used for the creation of ontologies and the elicitation in the knowledge engineering process. Cross domain ontologies and EU level ontologies, which are agreed and based on controlled core vocabularies (for code lists and core object types).

Architecture Management

- Use of standards [1] in mobile App2App communications (e.g. eIDAS SSO) and [2] use of pure standards instead of vertical standards
- Toolboxes for plug-and-play building blocks for re-use (incl. implementation profiles) and for multi pattern architecture (also for other interoperability layers)
- Establishment of horizontal infrastructures for the use of vertical/sectoral use cases
- EUDIW, [1] with SSI and then with anchor on national eIDs and [2] the means for validation of person identification, also new methods and services for consent
- Attestation/Attribute-based access management and inclusion of roles as attributes
- Use of sustainable green IT
- Single contact points for cross-border management instead of national complexity of responsibilities

Semantics / Automation / AI

- Machine learning for computer aided ontologies management solution, and use of edge computing
- Machine readability of semantic definitions
- Bottom up semantics for practical use, semantic agreements (incl. life cycle mgmt.), and first a definition of use cases for common understanding and accelerating the analytic process, and the re-use of experience for semantic interoperability
- Use of a semantic elicitation approach for knowledge engineering, with AI for the discovery of semantic aspects (for re-use)
- Establishment of a European semantic standardisation body
- Cross domain ontologies and EU level ontologies for code lists (with a EU level management) and core object types
- Well-functioning language models and re-use of agreed and controlled core vocabularies

3.4.4. Category Data

Data access should be managed on EU level with more logic and governance rules and following reference data models; registries should open up for automatic exchange without user interaction and should manage organisational changes (incl. responsibilities). More open data and catalogues for entities and procedures (and other data).

Data Access

- Data access rights should be valid across EU-level, with more access logics (channels) and also API access.
- Governance rules for data exchange for cross border exchange
- Registries should open for automatic exchange

Data Management

- Open data on public trusted entities, on public procedures and on base registries (data services)
- Catalogues on trusted entities (incl rights for data use), services and data sources, public entities, rights and addresses, as well as of interoperable solutions and best practices (e.g. LSPs), and also EU services
- Direct data exchange instead of user interaction and on legal basis
- System for access and re-use of data from decentral registries when organisational changes happen (e.g. responsibilities – which are fine grained)
- Balanced value model of data between involved entities

Data Models

- Reference data models for data exchanges on EU-level and semantic definition of this models

4. Elements of ONE Digital Single Market Ecosystem

This chapter applies inductive reasoning to describe functional architecture elements of ONE Digital Single Market Ecosystem that jointly exhibits the eight aspects derived from current EU policy documents in chapter 2. The main basis for this inductive approach is the knowledge collected in the eight expert interviews that are analysed in chapter 3 supplemented with insights gained by the authors while working in the DE4A project, especially on deliverables D2.7 (Interoperability Architecture for Cross-border Procedures and Evidence Exchange in light of the Single Digital Gateway Regulation) [18] and D2.5 (Project Start Architecture (second iteration)) [26], based on the requirements [27][28][29] and forthcoming results of the DE4A pilots.

As a first step of this inductive approach, we defined the ONE Architecture Canvas depicted in Figure 5 below. It consists of six functional areas that helped to focus the analysis on the interview results and policy insights when identifying more concrete, well delimited architecture elements. Therefore, the resulting functional architecture elements correspond more or less directly to main insights from the interviews: some translating nearly on-to-one from interview responses, others combining aspects of different responses or focussing on a specific aspect that seems specifically important in achieving the overall vision.

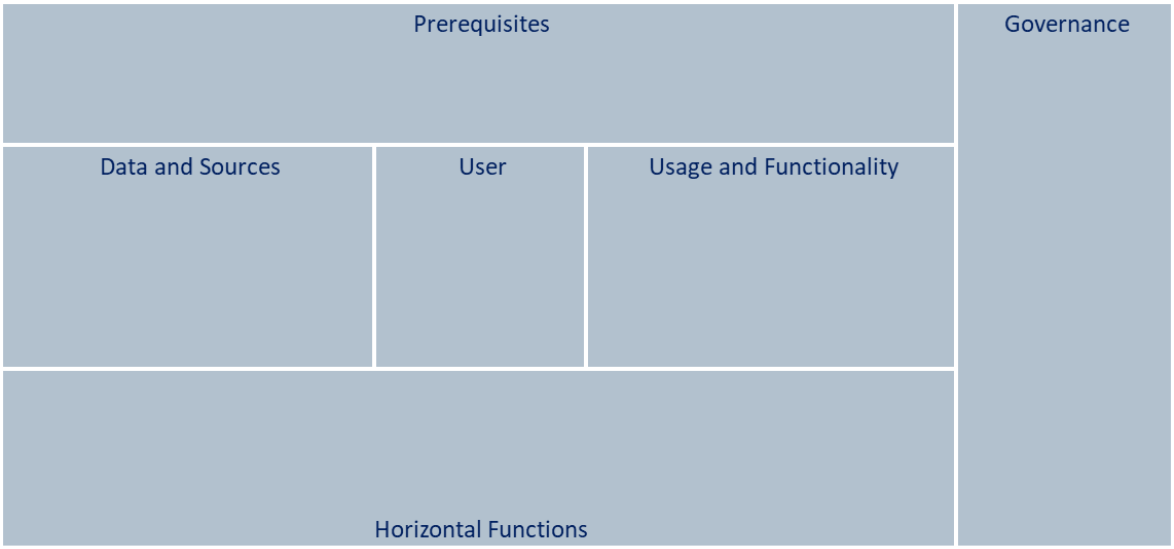

Figure 5: ONE Architecture Canvas

The six functional areas of the One Architecture Canvas are:

- The **User** area is the central area of the canvas, paying tribute to the prominence of people-centricity in current policy making (cf. 2.3) and the frequent mentioning of the EUDIW [16][17] in the interview responses (cf. 3.4.3).
- The **Data and Sources** area, to the left of the user, focuses on how different sources of data are made available. It reflects the relative importance of data-related topics in the interview responses (cf. 3.4.4) and the notion of a data driven economy enabled by the free flow of data (cf. 2.5).
- The **Usage and Functionality** area, to the right of the user, directs the reasoning to elements involved in using this data in providing different functionalities and (both public and private sector) services. It completes the three core functional areas that can vaguely be read from left to right.
- The three core functional areas build on the foundation of **Horizontal Functions** that are positioned at the bottom of Figure 5. This area collects functional elements that are closely intertwined with and reach across the elements of Sources, User, Usage.

- The **Prerequisites** area across the top of Figure 5 concerns elements that play a role in the preparation and initialization of the overall architecture. Here you will find mostly "design time" elements.
- The sixth area, connecting the three layers alongside the right side of Figure 5, is **Governance**. The elements in this area are involved in steering the creation and operation of ONE Digital Market Ecosystem.

This Canvas was used iteratively, area by area, to define functional architecture elements from the interview responses focussing in a second and third iteration on aspects of the responses that were not covered by already defined elements. In a final iteration, the completeness of the resulting long-term ONE architecture was validated against the eight aspects derived from current EU policy. The resulting Functional ONE Architecture Landscape of the Digital Single Market Ecosystem consists of 21 architecture elements and is depicted below in Figure 6.

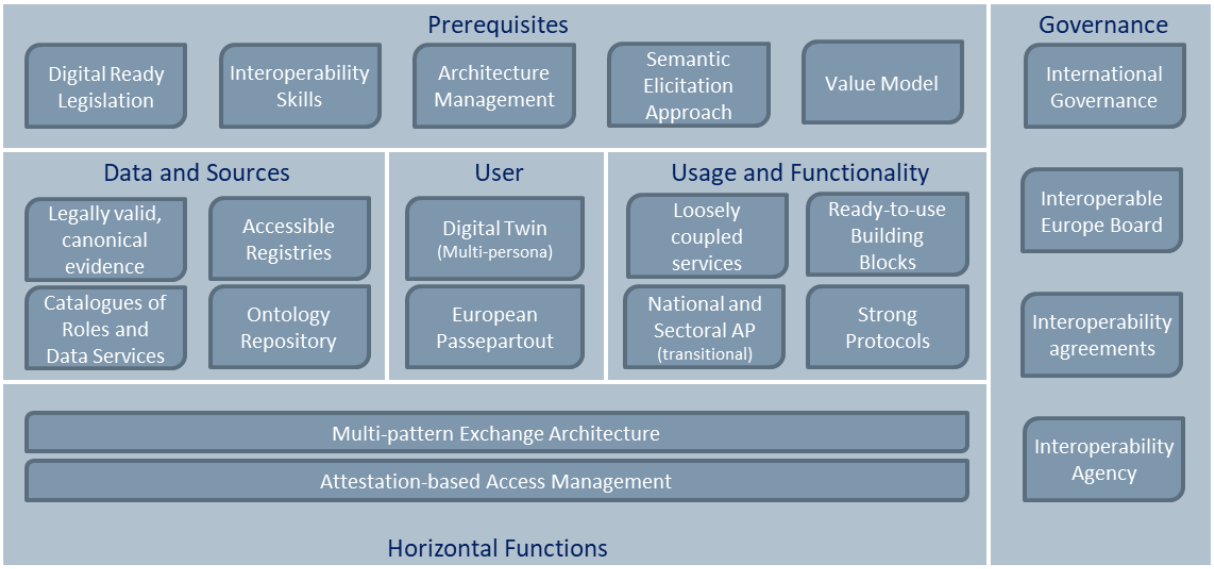

Figure 6: Functional ONE Architecture Landscape of the Digital Single Market Ecosystem

The remainder of this chapter is structured along the lines of the canvas and describes each functional architecture element.

4.1. User

It would be simple to focus this section exclusively on the EUDIW [16][17] as the central functional element of the user area, subdividing it further into its three core functions: identification, attribute attestations and electronic signature. This would also fit its immediate importance for the DSM as shown in chapter 2: It is crucial for overcoming the boundaries between public and private sector (2.1), it is a central enabler for digital self-determination (2.3), a cornerstone in the creation of a secure environment (2.6) and the token that makes government instilled trust a portable commodity of the DSM (2.7). Some interviews, however, pointed out that this restriction would be too narrow to adequately cover people-centric functionality in the ONE Architecture Landscape.

4.1.1. Digital Twin

One interview partner called for the creation of a conceptual, human Digital Twin under control of the natural person; meaning bringing together the multitude of data that represents each of us individually in the digital world and to hand the full control to the natural person. It is important to realize that this is broader than the attestations that one would carry in an EUDIW: The footprint of our Digital Twin is much larger. Consider for example that a big part of the digital economy is advertising-driven; fuelled

by the data generated though our online behaviour. The current situation means that the user, looking into the digital mirror, merely sees a shadow of their Digital Twin, whereas large platforms gain detailed insight into our lives through that looking glass. Would all the data that represents an individual person, related together, create the ultimate looking glass though which the all-seeing eye of Big Brother [32] is watching all of us? It would, if the data can be correlated by any single participant in the ecosystem, other than the user.

Another interview respondent explained that for the ONE vision to succeed, we ought to accept and aptly represent the difference between a natural person and their multiple administrative personas: the taxpayer, the inhabitant, the patient, the student, the voter, the convict etc. This might point to a way to mitigate the risk of the Digital Twin becoming the ultimate surveillance and control mechanism; if we generalize this notion to digital personas and include the 'subscriber to online service A or B', the 'online shopper on platform X and Y' and the 'author of a political essay on social platform Z'. True people centricity and digital self-determination would require keeping these personas separate, applying concepts like data minimization and pseudonymous identification. To keep with the metaphor: Our Digital Twin must exhibit an aggravated form of virtual multiple personality disorder and go by many names.

4.1.2. European Passepartout

This section is concerned with the online/remote (via the internet) and on-site/proximity identification function currently under discussion as one of the three main functions of the EUDIW [16][17] which should leady to "80% of citizens using digital ID" [by 2030] [33]. The ID function of the wallet is mentioned repeatedly and nearly by every interview partner as a crucial enabler of the people-centric DSM, highlighting specific aspect, like the need to imbue the identification with legal value[3] and the need to have it accepted across the Union, including the problem of record matching. Its central importance is also sustained by the Declaration of Digital Rights, that commits to "ensuring that all Europeans are offered an accessible, secure and trusted digital identity that gives access to a broad range of online services." [8]

What is curious, is that the central element of people-centricity is defined from an administration perspective: from the need to identify a citizen in a service encounter. The Berlin Declaration provides a somewhat more human-centric formulation: "Everyone should be able to navigate the digital world safely, authenticate and be digitally recognised within the EU conveniently." [5] If we really take the perspective of the user, then the EUDIW represents a means to navigate the digital world safely; it is a universal key to unlock and log-into things in the physical and the virtual world; literally, the digital equivalent of a European Passepartout, "allowing each citizen to control their own online interactions and presence. Users can make a full use of online services easily and throughout the EU while preserving their privacy."[4]

To favour one implementation option over another is beyond the scope of this paper, but the authors understand the call for "SSI first" by one of the interview partners (cf. 3.4.3), as highlighting that a European Passepartout must be non-traceable, privacy-preserving and resilient against attack or control of a central infrastructure. This, taken together with the need to function for all types of transactions in the public and private sector (cf. 2.1), means that **the universal key must not be uniform**. It should build on the concept of pseudonymous identification that is emerging in the negotiations of the revised eIDAS regulation and it should strictly adhere to the principle of data minimization (cf. selective disclosure and Zero-Knowledge-Proof (ZKP)). As a result, identification is not **one** functionality, but provides very different levels of unlocking or logging into something. One could for example, and without prejudice to a thorough analysis, distinguish between:

[3] The EUIDW[17] is presently defined as an eID means of Level of Assurance (LoA) high[34]. This means that even if the EUDIW would be secure enough to serve as legal means of identification, the revised eIDAS regulation [16] is not giving it the same legal validity yet as current identification means, such as passports or ID cards.

1. Logging into an account at a private online service provider, using only a service-specific pseudonym and not sharing any other personal data (you can log-in with different pseudonyms to manage different accounts that seem unrelated for the service provider)
2. Logging into a virtual ballot box to cast a vote with a pseudonym that enforces uniqueness (you cannot login with different pseudonyms to cast multiple votes for one election), without sharing any personal information other than a proof of citizenship (national elections) or a proof of residence (municipal elections). Please consider that a similar logic might enable the user to perform financial online transactions in a privacy-enhancing manner, compared to the status-quo of the offline an online world.
3. Unlock the access to a venue or purchase in the physical world by proving a specific attribute attestation of the natural person (e.g. legal age, membership of a football club) without disclosing the full identity.
4. Unlocking the physical access to secure areas or boarding an international flight, revealing one's full identity as rightfully required by law or company policy.
5. Logging into procedure platforms of trusted institutions (e.g. governments or banks), revealing ones full identity, to securely perform critical transactions (e.g. change of address, name, civil status; or authorization of payment or confirm transfer of ownership)

One specific aspect of the passepartout is that it must support the ability provide representatives with the ability to access specific services on behalf of the user. This is needed to fulfil the requirement of inclusion (cf. 2.4) of people who are not (including: not yet, not anymore and temporarily not) able to participate fully in the digital society. The second important type of representation is the representation of legal persons in the digital economy. Presently, legal persons do usually act through human representatives, making the support for Powers of Representation (PoR) a crucial element of the European Passepartout for the functioning of the DSM. What both types of representation have in common, is that it is usually not the complete universal key that one hands to a representative but rather specific keys to specific services, places, or rights. And yes, there are places and services that require two keys (joint representation).

4.2. Data and Sources

4.2.1. Legally valid, canonical evidence

If we would need to choose the single most prominent point raised in the interviews, it would be the use of structured data (cf. 3.4.4)., that is sufficiently harmonized (cf. 3.4.1) and has legal validity to be directly used in fully automated processes (cf. 3.4.3). It amounts basically to mandate the adherence to EIF Recommendation 9: "Ensure data portability, namely that data is easily transferable between systems and applications supporting the implementation and evolution of European public services without unjustified restrictions, if legally possible." [2] the combined voice of the interview partners says: Make it possible! This requires more than defining a specific data set as carrying legal validity. In the world of public administration, which is defined by national legal frameworks making data portability possible will in some cases also require farther reaching legal harmonization.

This element is not only about structured, machine-readable data that can readily be reused. The DE4A pilots were focussing on 'evidence' in line with the terminology of the SDGR [12], while the eIDAS revision [16] uses the term Electronic Attestation of Attributes (EAA) (see Annex I for a comparison of terminology). Whether called evidence or attestation, the important feature they are sharing is that they are not merely data, but that they are data combined with an explicit (EAA) or implicit (OOTS) proof of correctness, supported by a trusted party. Whereas not all attestations in the DSM Ecosystem will require legal validity, attestations based on data from authentic sources surely should.

4.2.2. Ontology Repository

Using the canonical evidence described above in real processes requires an understanding of the meaning of each attribute and value. This was mentioned in different contexts during the interviews (cf. 3.4.1, 3.4.3). How to engineer (4.5.4) and govern (4.6.3) the semantic harmonization is covered at different place in this chapter. The ontology repository caters for the need to provide machine-readability of semantic definitions and labels. Especially where legal validity is required, and consequently automatic translations are not sufficient, such an ontology repository must be multilingual to be a valid choice for Europe. The Multilingual Ontology Repository (MOR) [35] developed for the limited universe of the DE4A pilots is a concrete example of this concept.

4.2.3. Catalogues of Roles and Data Services

The need to have a catalogue of trusted administrative entities (3.4.4) that can automatically be queried in run-time is apparent from the interviews. For a DSM Ecosystem this need clearly extends further to catalogues of professions or more generally to roles holding specific rights to provide or request information. Ursula van der Leyen, stated in her Agenda for Europe she believed "[..] Europe can successfully manage the transformation into the digital age, if we build on our strengths and values." [10] One such strength is that many such catalogues already exist on national level and are well maintained either by the public administrations or by recognized professional associations, such as catalogues of public administrations, companies, medical professionals, notaries, etc. The difficult bit of establishing such catalogues and the governance around them is mostly done. What is lacking, is to activate these catalogues for automated querying, e.g. for runtime validation of attestation providers or relying parties.

Extending from this is the need to have catalogues of genuine data services and authentic sources. This finding from the interviews is also fully supported by policy declaring "Everyone should have the means to know who owns or controls the media services they are using."[8] We see different approaches taken in this regard, like the Data Service Directory of the OOTS [13] or the obligation of Article 9.1 and 9.2[4] of the Open Data Directive[7]. Also the EUDIW [17] will require different (trust) lists to become operational. For ONE Architecture to be practical, a hierarchical approach of catalogues of catalogues must be established that supports both human navigation as well as automated querying and validation at runtime and makes maximum reuse of existing catalogues including their governance.

4.2.4. Accessible Registries

The fourth functional element are registries open for automated data exchange (cf. 3.4.4). This is defined as a separate functional element to finding them and being able to judge the validity of the information contained in them (see 4.2.3 above) and requires that they are accessible by a suitable, standardized interface.

4.3. Usage and Functionality

4.3.1. Loosely coupled services

The call of EIF Recommendation 36 to use loosely coupled service on a common infrastructure to break up organisational, sectoral and national silos is clearly mirrored by the interview respondents,

[4] Article 9.1. Member States shall make practical arrangements facilitating the search for documents available for re-use, such as asset lists of main documents with relevant metadata, accessible where possible and appropriate online and in machine readable format, and portal sites that are linked to the asset lists. Where possible, Member States shall facilitate the cross-linguistic search for documents, in particular by enabling metadata aggregation at Union level.
Article 9.2. Member States shall, in cooperation with the Commission, continue efforts to simplify access to datasets, in particular by providing a single point of access and by progressively making available suitable datasets held by public sector bodies with regard to the documents to which this Directive applies, as well as to data held by Union institutions, in formats that are accessible, readily findable and re-usable by electronic means. [7]

especially for the provision of data services. It should not matter where the service consumer and provider reside, or whether they belong to the public or private sector, to be accessible across the Union. Access rights must be managed in a different way (see 4.4.2 below).

4.3.2. National and Sectoral Access Points (transitional)

The transition to a more loosely coupled architecture, even if we are considering coarse grained services, is not happening overnight and the respondents also voiced the expectation that European Harmonization should not alter MS systems (cf. 3.4.1). The predominant integration pattern so far was to establish national or sectoral Access Points (AP) and to shield the complexities of closely integrated national systems. And some of these AP-based cross-border integrations are just being implemented recently. Even if location and organisation independent, loosely coupled services are becoming the dominant structure in the future, they are perfectly able to coexist (at least temporarily) with bubbles of closely integrated systems, accessible via AP.

4.3.3. Ready-to-use Building Block

The concept of European Building Blocks was championed by the Connecting Europe Facility (CEF) and is well received by the member state respondents. What they wish for in the future is a more comprehensive toolbox of ready-to-use technical, open-source building blocks that already contain the implementation profile. The motivation behind this stems from the experience that building blocks that are too generic, can be implemented and configured in different ways, leading to non-interoperable solutions. The second motivation is concerned with the time and specific skills required to implement and configure these building blocks.

4.3.4. Strong Protocols

Related to the need for technical building blocks is the use of horizontal standards (3.4.3) (as opposed to domain specific) that are well documented and detailed to the level of implementable protocols and minimize the room for interpretation, hence ensure interoperability. Each core function required for the functioning of the DSM ecosystem should be specified and standardized to this level of detail, preferrable with at least one ready-to-use building block available.

4.4. Horizontal Functions

4.4.1. Multi-pattern Exchange Architecture

As stated in the introduction of chapter 2, the authors recommend the adoption of the EIF for all transaction types in the DSM, including B2B, B2C and C2C. This is especially true for the requirements for transfer mechanisms:

- **registered and verified**, so that both sender and receiver have been identified and authenticated through agreed procedures and mechanisms;
- **encrypted**, so that the confidentiality of the exchanged data is ensured;
- **time stamped**, to maintain accurate time of electronic records' transfer and access;
- **logged**, for electronic records to be archived, thus ensuring a legal audit trail. [2]

DE4A defined the concept of a multi-pattern architecture in the PSA [36] for three pilots, covering five of the life/business-events mandated by the SDGR [12]. The requirements of different sectors, participants and procedures are too heterogenous to be resolved by a single exchange pattern. Instead of developing different systems for different needs, the multi-pattern architecture proposes as consistent set of components that are jointly able to support different patterns. The interview respondents reconfirmed the need for such a multi-pattern exchange architecture that is established as a horizontal infrastructure to be used for a multitude of sectoral requirements and solutions.

In deliverable D2.7 [18], we explored the concept further and were able to show that the infrastructure of OOTS [13], designed for one specific interaction pattern can in be easily leveraged to support a the

multi-pattern architecture, including the EUDIW, in the mid-term future. This would support such disparate requirements as self-determination of the user and, where applicable, pro-active eGovernment procedures.

4.4.2. Attestation-based Access Management

The respondents clearly "Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved" [2], in line with EIF Recommendation 30 and also subscribe to EIF Recommendation 37: "Make authoritative sources of information available to others while implementing access and control mechanisms to ensure security and privacy in accordance with the relevant legislation." [2]. With the small, but relevant difference that we need to strive for one consistent access logic on EU level that cuts across different channels (cf. 3.4.4), which means that the access control mechanism should apply across the entire multipattern architecture, irrespective of the pattern used.

The authors are fully aware that establishing such an access logic is all but trivial. We cannot pull a AAA-server off the shelf and configure a standard Role-Based Access Management (RBAC) logic – the current, centralized, approaches are unable to cater for the complexity of an entire DSM ecosystem; They are reaching their conceptual boundaries already in larger corporate settings. An EU-level access logic would need build on a highly decentralized and flexible approach to be practicable.

One respondent pointed to a possible avenue for such an approach: an attestation-based access management (cf. 3.4.3). Others cited the evolution of RBAC to attribute-based access control. Cryptographically signed attestations of access rights to particular (types of) data that can be provided from a wallet or communicated through other channels of the multi-pattern architecture (e.g. included in an eDelivery message) could be a concept for a decentralized and flexible access management approach. The missing elements would be the a) availability lists of trusted issuers of such attestations and b) a mapping of the attestations to the (types of data) they unlock. Please note that the logic could possible also hold for issuing/providing data, not only for the access of it.

The hierarchical catalogue of catalogues described in section 4.2.3 should be able to provide the required (a) trust list of issuers, while the Ontology Repository described in section 4.2.2 should provide the definitions of (types of) data to which the 'access attestations' would need to be mapped. Therefore, an Attestation-based Access Management would primarily need to provide the mapping logic between issuers of attestations, attestation type and types of data an attestation allows to access (or issue). It is, hence, part of the horizontal functions of the ONE architecture.

Please consider this example from the eHealth for the functioning of an attestation-based access management. The example holds both for a physical service encounter and a (presently impossible) fully online, via the internet scenario. It is included as an attempt to fill the envision DSM ecosystem a bit with life:

- Imagine you need medical assistance. The (alleged) physician requires access to your medical record. To receive access, they present an electronic attestation issued in MS X that confirms that they are an active physician
- The patient system (can be a wallet but could equally use a different interaction pattern) validates the attestation, including the validation 1) against the respective catalogue (4.2.3) - the register of medical professions of MS X - that the issuer of the attestation is indeed the right party to issue such attestation and 2) that the attestation allows access to medical data (4.2.2).
- The (validated) physician performs a medical examination and determines that medication is required and issues an ePrescription
- Again, the patient system would check that the attestation of the physician is valid and provides the right to issue valid ePrescriptions (technically, an attestation in its own right).
- You take the valid ePrescription and visit an (online) pharmacy. The pharmacy provides an attestation that it is a pharmacy (it's license) issued in MS Y, allowing access to prescription data

(and effectively allowing to dispense prescription medication, which is nice to know when purchasing medication online).

- The patient system validates the attestation 1) against the respective the catalogue of pharmacies of MSY and 2) that this attestation indeed provides access to the patient's prescription data.

4.5. Prerequisites

The sections 4.1 to 4.4 explained the main operational functionalities of the envisioned DSM Ecosystem. This section dives into the prerequisites, the things that are needed to prepare and initiate such an ecosystem. Followed by section 4.6 on how to steer and control it.

4.5.1. Digital Ready Legislation

The EIF identifies a number of legal interoperability barriers: […] "sectoral or geographical restrictions in the use and storage of data, different and vague data licence models, over-restrictive obligations to use specific digital technologies or delivery modes to provide public services, contradictory requirements for the same or similar business processes, outdated security and data protection needs, etc." [2]. A prerequisite for a well evolving DSM ecosystem is to remove these barriers in existing laws, and to develop approaches to write new laws that are digital ready.

This call for Digital Ready Legislation (DRL) is well represented in the interview results (cf. 3.4.2) and it appears logic that if we […] "need to make sure that the same rights that apply offline can be fully exercised online." [4], then we need to pass laws that are designed to apply online and offline. One approach cited in the interviews are mandatory interoperability check or digitization checks as part of the legislative process. Such checks are current practice in some member states, e.g. Esthonian, but should become common practice both on Member States and on European level.

4.5.2. Interoperability Skills

The challenge to find suitable interoperability experts for digitization projects, specifically in the eGovernment domain, and the overdemand on experts is a challenge that returned explicitly in several interviews. A prerequisite for attaining the ONE vision is the availability of sufficient and sufficiently skilled experts. Two approaches mentioned that can contribute to skills being available when and where needed, are 1) reviving the Interoperability Academy, which had a promising start prior to the COVID-19 pandemic and 2) pooling experts that can contribute to projects across the Union. Increasing the focus on basic - "which should become a right for all" [4] - and advanced digital skills development and including specific European interoperability skills in the regular education curricula could be an approach to resolve this challenge in the long run.

4.5.3. Architecture Management

One element of the ONE Architecture is the need to establish an Architecture Management function as such. In the interviews we collected statements about harmonization of description languages for processes and other architecture artefacts (cf. 3.4.1) and the (standardized) availability of organisation and responsibility information (cf. 3.4.2) across the Union and the creation of toolboxes of reusable solutions (cf. 3.4.3). One expert explicitly referred to the Cartography [30] of EIRA [31] as a good start for the latter. The Architecture Management approach for ONE would need to go further in that direction and cover a wider range of solutions, also from MS-level and from private sector providers. Great effort is invested in maintaining organisational and technical architectures within the scope of our organisations. What we envision, is European Architecture Management that makes these architecture descriptions usable for the alignment and integration across national and organisational borders.

4.5.4. Semantic Elicitation Approach

The complexity of semantic harmonization on European Level is enormous and reaching semantic agreements that are valid across 27 Member States is painstaking work. Five aspects make this

especially challenging: 1) Meaning is context specific, often defined within the confines of a specific sector or professional culture. 2) Concepts are language dependent, meaning that building ontologies in the multilingual environment of Europe goes beyond “simple” translation. 3) True interoperability requires deep semantic definitions that do not merely define objects and attributes, but also the attribute domain (the values an attribute can take), resulting in extensive refence data models (cf. 3.4.4) that are in itself difficult to navigate and manage (even within one langue and sector). 4) The described universes of discourse are not static, meaning that maintaining ontologies is an ongoing effort. 5) In the world of public administration, the universe of discourse is defined by laws, originating from 27 different legal frameworks, and resulting in possibly incompatible or even contradicting “facts of nature”.

As a result of the above, interviewed semantics experts did not only highlight the need for semantic harmonization, but emphasised especially the need for an information engineering method that consistently yields actionable results in different context (cf. 3.4.3). This semantic elicitation approach could be in the future supported by machine learning technology, however, not replaced. The resulting models and definitions must be able to carry legal validity if they are to be instrumental part of an DSM ecosystem. Machine learning could especially support the elicitation process and simplify the navigation of existing ontologies for reuse.

4.5.5. Value Model of the DSM

The Digital Single Market (DSM) ecosystem and the data driven economy that it supports, should not require sustained budgetary funding, much like a mycelium does not require its own source of nutrients, but is sustained by the trees that profit from their synergetic relationship. The infrastructure and public data services of the ecosystem should be allowed to capture part of the value that they create form the businesses participating in the DSM. This will not happen automatically. To the contrary, the value created through the existence of the ecosystem could easily dissipate to commercial participants that are able to monetize it through their services, while the ecosystem requires increasing public funding.

Stated differently, we should apply EIF Recommendation 30: “Perceive data and information as a public asset that should be appropriately generated, collected, managed, shared, protected and preserved.” [2] and extend its asset logic to also include fundamental infrastructure services.

We need a value/business model (cf. 3.4.4) that regulates the value creation across all participants in the DSM ecosystem, including a monetarisation logic. Monetarisation of the added value of the DSM ecosystem must allocate a fair share of the proceeds to the providers of the core infrastructure, irrespective of their origin (EC, Member State or even from outside of the Union) or ownership (public administration or commercial entity).

4.6. Governance

4.6.1. International Governance

The interview respondents pointed out that for “Europe [to] lead the transition to [..] a new digital world.” [10], the Member States and the Commission would need to engage proactively in international governance of digitisation. It is worth emphasizing that this includes both governance on the political level, i.e. in governance bodies like the UN, OECD or WTO, and governance on the technical level through international standardization bodies, like ISO or ITU. Active participation in these standardization bodies should be fostered.

4.6.2. Interoperable Europe Board

The Interoperable Europe Board (IEB) [9] is explicitly mentioned as an important development, but several respondents maintained that it is merely a first step. “In the ‘Interoperable Europe Board’, Member States and representatives from the Commission, the Committee of the Regions and the

European Economic and Social Committee set the strategic goals and agree on concrete measures that can ensure the cross-border interoperability of their network and information system providing or managing digital public services." [9] Similarly to scope of the EIF, the responsibility of the IEB would need to extend beyond the domain of public services to serve as a governance body of the entire DSM ecosystem. It could develop in a permanent governance body that issues interoperability agreements that are binding across the EU.

4.6.3. Interoperability Agreements

The call for interoperability agreements was pervasive through most of the interviews, specifically highlighting that these agreements would require to be mandated and binding for everybody across the Union, including EU institutions, MS administration and the private sector. We adopt the notion of interoperability agreements from EIF, which makes clear that agreements are to be reached on all levels of the interoperability. "At semantic and technical levels, but also in some cases at organisational level, interoperability agreements usually include standards and specifications. At legal level, interoperability agreements are made specific and binding via legislation at EU and/or national level or via bilateral and multilateral agreements." [2] The above mentioned IEB should play a central role in forging these multilateral agreements, providing the required level of binding agreements that are more flexible than legal provisions and allow regulation at the detailed level required for strong protocols that can readily be implemented.

4.6.4. Interoperability Agency

The DSM ecosystem is too important for the future of Europe to rely on cyclical programme funding and organisation. Several of the elements of the ONE architecture landscape require a stable organisational home on the operational level, giving rise to the idea of a European Interoperability Agency (cf. 3.4.2). The agency should for example be responsible:

- to maintain the body of interoperability agreements,
- to check compliance to these agreements
- to test or providing means to test interoperability
- to maintain oversight over the functioning of the overall ecosystem
- to manage overarching issues and their resolution
- to manage a cartography and a toolbox of ready-to-use building blocks
- to operate common components of the ecosystem, such as for root level catalogues
- to serve as semantic standardisation body on EU-level that develops and maintains (or coordinates the development and maintenance) of European ontologies
- to manage interoperability knowledge, potentially including an Interoperability Academy and pools of European experts

This neither prescriptive nor exhaustive list shows that the ONE vision requires an operational-level governance anchored in a permanent organisation on EU-level. Stated differently, the journey towards a DSM that started in 2015 on Policy level with the Digital Single Market Strategy [1] and was established through EU-level regulations in the years since then, will require also EU-level administrative means beyond programme financing to become an operational reality.

5. Conclusions

European digital policy and recent developments, such as the European Digital Identity Framework, show a first outline of a future that goes beyond eGovernment Interoperability to overcome the boundaries between national systems, as well as those between public sector and private sector services. Also, the role of Governments is changing in this transformation: On the one side, reconfirming classical roles, like their role as regulator that is increasingly extending to the detailed level of operational and technical specifications. On the other side, emerging roles in a wider governance, beyond classical regulatory means, like the stewardship of the overall ecosystem.

A thorough analysis of current EU policy documents revealed an underlying vision of a seamless Digital Single Market (DSM) ecosystem - One Network for Europe ONE. Expert interviews were used to collect insights into practical steps towards this vision, exploring what would be needed to create a European DSM ecosystem that will maximise the growth potential of our European Digital Economy, provide an optimal breeding ground for digital start-ups and at the same time be people-centric and preserve our privacy and sovereignty as EU citizens.

From the interviews we see confirmed that **harmonization** cannot stop on the legal level but needs to include the level of organisational and technical specifications while being mandatory for both EU and Member State level. This requires strengthened **governance** of the digitization of Europe. The proposed Interoperable Europe Act [9] is seen as a very important step in the right direction with the expectation that the Interoperable Europe Board will evolve over time to the central governance body, with an even stronger mandate than defined in the first proposal. The insight gained for the interviews concerning the future **architecture** confirmed the importance of the EUDIW and the central role of harmonized semantics allowing automated reuse of information across the Union. Interestingly the second focus of architecture related responses are closely related to the harmonization and governance, calling for the use of standards, the use of common description languages, improved cartography of ready-to-use toolboxes. A very concrete focus was put on **data** in enabling the data-driven economy: data should be easily available across the Union with a data access logic managed on EU-level.

Based on the interview results, the analysis of EU policy documents and the insights gained in from de DE4A project, a functional architecture landscape was derived, consisting of 21 architecture elements (or components), in 6 functional areas. Overall, we see that current developments, such as the OOTS [12] [13], the EUDIW[16][17][9] as well as regulatory measures such as the Interoperable Europe Act are all moving Europe towards the ONE vision. There are, however, nine points that require further attention research:

- Legal validity of structured data should be established on European Level.
- There is an apparent need to interoperability agreements that are binding across the Union and applicable for both the public as the private sector, yet less rigid than laws.
- Our governments should claim their role in the Governance of an interoperable Europe that extends from the eGovernment domain to cover the entire DSM, hence including private actors. This requires establishing strong European digital governance bodies.
- Member states and the Commission should take a proactive and coordinated stance in international governance bodies concerning questions of the digital economy, including international standardization bodies.
- The Wallet should be a European Passepartout supporting pseudonymous identification and allowing the user to manage the different personas of their human Digital Twin in a privacy-enhancing way.

- The management of semantics should be recognized as a European endeavour, including the creation of multilingual ontology repositories and a semantic elicitation approach to create and maintain ontologies on European level.
- The creation of an attestation-based access management logic that must be highly decentralized, yet applicable across the Union and across different channels requires further research and development, as it is crucial for the success of the DSM.
- The OOTS and EUDIW provide a good basis for establishing a muti-pattern exchange architecture, but establishing such a horizontal, multi-pattern architecture should be recognized as an overarching goal and managed consistently.
- A value model of the DSM should be developed to mitigate the risk of value dissipating from budget financed services to commercial enterprises.

Concluding, we can establish that attaining the ONE-vision of a seamless Digital Single Market Ecosystem does depend more on conceptual and governance challenges than the lack of technological capability. Using our specific strength and trusting in "the best of Europe - open, fair, diverse, democratic, and confident" [3] we should indeed be able to achieve the goal that "Europe must lead the transition to a [..] a new digital world." [10].

References

[1] A Digital Single Market Strategy for Europe, European Union: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 6 May 2015, COM(2015) 192 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 (Accessed: 9 November 2022)

[2] European Union: European Commission, The New European Interoperability Framework (2017) ISA² - European Commission. Available at: https://ec.europa.eu/isa2/eif_en/ (Accessed: 2 November 2022).

[3] Shaping Europe's Digital Future, European Union: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Shaping Europe's Digital Future", 19 February 2020, COM(2020) 67 final. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020DC0067 (Accessed: 2 November 2022).

[4] 2030 Digital Compass: the European way for the Digital Decade, European Union: European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "2030 Digital Compass: the European way for the Digital Decade", 9 March 2021, COM(2021) 118 final. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118 (Accessed: February 2nd 2023).

[5] Berlin Declaration on Digital Society and value-based Digital Government (2020) Federal Ministry of the Interior and Community. Federal Ministry of the Interior and Community. Available at: https://www.bmi.bund.de/SharedDocs/downloads/EN/eu-presidency/gemeinsame-erklaerungen/berlin-declaration-digital-society.html?__blob=publicationFilev%3D6 (Accessed: 2 November 2022).

[6] Digital Markets Act, European Union: THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, Available at: https://eur-lex.europa.eu/eli/reg/2022/1925/oj

[7] Open Data Directive, European Union, Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) (2019) Official Journal L 172, 26.6.2019, p. 56–83. In force. Available at: http://data.europa.eu/eli/dir/2019/1024/oj (Accessed: 2 November 2022).

[8] European Declaration on Digital Rights and Principles for the Digital Decade, European Union: European Commission, Proposal, Brussels, 26.1.2022, COM(2022) 28 final, Available at: https://ec.europa.eu/newsroom/dae/redirection/document/82703

[9] Interoperable Europe Act, European Union: European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures for a high level of public sector interoperability across the Union, Brussels, 18.11.2022, Available at: https://commission.europa.eu/publications/interoperable-europe-act-proposal_en

[10] Ursula von der Leyen, President of the European Commission, A Union that strives for more - My agenda for Europe. Available at: https://op.europa.eu/en/publication-detail/-/publication/43a17056-ebf1-11e9-9c4e-01aa75ed71a1 (Accessed: 22.01.2023).

[11] Digital Services Act, European Union: THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, REGULATION (EU) 2022/2065, 19 October 2022, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN (Accessed: 22.01.2023)

[12] European Parliament and the Council, "Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012", https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R1724&from=EN , accessed on 12/02/2023.

[13] COMMISSION IMPLEMENTING REGULATION (EU) /... setting out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the "once-only" principle in accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council; C/2022/5628 final; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282022%295628&qid=1658925262468

[14] Connecting Europe Facility (CEF), https://ec.europa.eu/inea/en/connecting-europe-facility (Accessed via archice-it on 12/02/2023)

[15] ISA² - Interoperability solutions for public administrations, businesses and citizens, https://ec.europa.eu/isa2/home_en/ (Accessed 12/02/2023)

[16] Revised eIDAS Regulation, European Union: European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, Brussels, 3.6.2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0281 (Accessed: 10.02.2023)

[17] The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework - The European Digital Identity Wallet Architecture and Reference Framework, Version 1.0.0, European Union: European Commission, January 2023, Available at: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework (Accessed 10.02.2023)

[18] D2.7 Interoperability Architecture for Cross-border Procedures and Evidence Exchange in light of the Single Digital Gateway Regulation, https://www.de4a.eu/project-deliverables (Accessed: 27.01.2023)

[19] eDelivery, European Union: European Commission: Digital Europe, https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery (Accessed: 28.01.2023)

[20] eDelivery 4-corner Model, CEF Telecom, Marcio Sapiano, 16th May 2017, https://wayback.archive-it.org/12090/20221204073504/https://ec.europa.eu/inea/sites/default/files/7._ms_edelivery_2017-05-16_inea_edelivery_presentation_v1.0.pdf (Accessed: 28.01.2023)

[21] eDelivery Implementation Models, https://edelivery.digital/implementation-models (Accessed: 28.01.2023)

[22] Business Registers Interconnection System (BRIS) , https://e-justice.europa.eu/content_business_registers_at_european_level-105-en.do (Accessed: 28.01.2023)

[23] Electronic Exchange of Social Security Information (EESSI), fhttps://ec.europa.eu/social/main.jsp?catId=1544&langId=en#:~:text=EESSI%20is%20an%20IT%20system,the%20EU%20rules%20on%20social (Accessed: 28.01.2023)

[24] Lisbon Declaration "Digital Democracy with a Purpose" https://www.lisbondeclaration.eu/learn-more/

[25] Carl Shapiro and Hal R. Varian, Information Rules, 1999, Harward Business School Press, ISBN 0-87584-863-X

[26] DE4A Deliverable D2.5 Project Start Architecture (PSA), second iteration, can be consulted via https://www.de4a.eu/project-deliverables

[27] DE4A Deliverable D4.1 Studying Abroad - Use Case Definition & Requirements, can be consulted via https://www.de4a.eu/project-deliverables

[28] DE4A Deliverable D4.5 Doing Business Abroad - Use cases definition and requirements, can be consulted via https://www.de4a.eu/project-deliverables

[29] DE4A Deliverable D4.9 Moving Abroad - Use cases definition and requirements, can be consulted via https://www.de4a.eu/project-deliverables

[30] Cartography Tool (CarTool©), https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira/solution/cartography-tool

[31] European Interoperability Architecture (EIRA), https://joinup.ec.europa.eu/collection/european-interoperability-reference-architecture-eira

[32] George Orwell, Nineteen Eighty-Four, 8 June 1949, Secker & Warburg

[33] Europe's Digital Decade: Digital targets for 2030, European Union: European Commission, Europe's Digital Decade: Digital targets for 2030 (2022) European Commission. Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (Accessed: 2 November 2022).

[34] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, European Union: European Commission, 8 September 2015, Available at: http://data.europa.eu/eli/reg_impl/2015/1502/oj (accessed 10/02/2023)

[35] SlavkoŽitnik, KarmenKernPipan, MihaJesenko, DejanLavbič, Semantic reusable webcomponents: A use case in e-government interoperability; 17.10.2022, Uporabna informatika, Available at:

Multilingual Ontology Repository (MOR) Available at: https://uporabna-informatika.si/ui/article/view/189/149 (accessed 13/02/2023)

[36] DE4A Deliverable D2.5 Project Start Architecture (PSA), second iteration, can be consulted via https://www.de4a.eu/project-deliverables

Annexes

Annex I: Comparison of Terminology in Relevant Communities

Table 1: Comparison of Terminology in Relevant Communities

DE4A and TOOP	SDGR OOTS	EUDI-Wallet	W3C Verifiable Credentials
Data Provider (DP)	Evidence Provider (EP)	(Q)EAA Provider	Issuer
Data Consumer (DC)	Evidence Requestor (ER)	Relying Party (RP)	Verifier
Evidence	Evidence	(Qualified) Electronic Attestation of Attributes ((Q)EAA)	Verifiable Credential (VC) / Verifiable Presentation (VP)

Annex II: Definition of EIF-Layers

Legal interoperability

Legal interoperability is about ensuring that organisations operating under different legal frameworks, policies and strategies are able to work together. This might require that legislation does not block the establishment of European public services within and between Member States and that there are clear agreements about how to deal with differences in legislation across borders, including the option of putting in place new legislation. [2]

Organisational Interoperability

Organisational interoperability also aims to meet the requirements of the user community by making services available, easily identifiable, accessible and user-focused. [2]

Semantic interoperability

Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words 'what is sent is what is understood'. [2]

Technical Interoperability

This covers the applications and infrastructures linking systems and services. Aspects of technical interoperability include interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocols. [2]

Interoperability governance

Interoperability governance refers to decisions on interoperability frameworks, institutional arrangements, organisational structures, roles and responsibilities, policies, agreements and other aspects of ensuring and monitoring interoperability at national and EU levels. [2]

Annex III: Tabular relation between Chapters 2, 3 and 4

Table 2: Tabular relation between Chapters 2, 3 and 4

	Elements	Chapter 2 and 3 results reference
Prerequisites		
	Digital Ready Legislation	2.7 Role of the Government 3.5.2 Category Governance: *Legal Governance/EU-Governance*
	Interoperability Skills	2.3. Citizen-centricity and Sovereignty 2.4 Inclusion 3.5.2 Category Governance: *Human Centricity*
	Architecture Management	2.6 Secure and Trusted Online Environment 3.5.3 Category Architecture: *Architecture Management*
	Semantic Elicitation Approach	2.2 A European Ecosystem Instead of Interconnecting National Silos 2.5 Free Flow of Data 3.5.3 Category Architecture: *Semantics / Automation / AI*
	Value Model	2.1 Overcoming the Boundaries Between Pubic, Private and Third/Forth Sector 3.5.4 Category Data: *Data Management*
Data and Sources		
	Legally valid, canonical evidence	2.2 A European Ecosystem Instead of Interconnecting National Silos 2.5 Free Flow of Data 3.5.1 Category Harmonisation 3.5.3 Category Architecture: *Semantics / Automation / AI* 3.5.4 Category Data: *Data Models*
	Ontology Repository	2.2 A European Ecosystem Instead of Interconnecting National Silos 2.5 Free Flow of Data 3.5.1 Category Harmonisation 3.5.3 Category Architecture: *Semantics / Automation / AI*
	Catalogues of Rules and Rights	2.2 A European Ecosystem Instead of Interconnecting National Silos 2.5 Free Flow of Data 3.5.4 Category Data: *Data Management*

	Catalogues of Data Services	2.2 A European Ecosystem Instead of Interconnecting National Silos 2.5 Free Flow of Data 3.5.4 Category Data: *Data Access* 3.5.4 Category Data: *Data Management*
User		
	Digital Twin	2.3. Citizen-centricity and Sovereignty 2.4 Inclusion 3.5.2 Category Governance: *Human Centricity*
	European PassePartout	2.2 A European Ecosystem Instead of Interconnecting National Silos 2.3. Citizen-centricity and Sovereignty 2.4 Inclusion 3.5.2 Category Governance: *Human Centricity* 3.5.4 Category Data: *Data Access*
Usage and Functionality		
	Loosely coupled services	2.2 A European Ecosystem Instead of Interconnecting National Silos 3.5.4 Category Data: *Data Management*
	Ready-to-use Building Blocks	2.6 Secure and Trusted Online Environment 3.5.3 Category Architecture: *Architecture Management*
	National and Sectoral AP	2.6 Secure and Trusted Online Environment 3.5.1 Category Harmonisation 3.5.3 Category Architecture: *Architecture Management*
	Strong Protocols	2.6 Secure and Trusted Online Environment 3.5.3 Category Architecture
Governance		
	International Governance	2.8 Cross-sectoral Governance on European Level 3.5.2 Category Governance: *Legal Governance/EU-Governance* 3.5.2 Category Governance: *Governance Agreements* 3.5.2 Category Governance: *Cooperation and Rules*

	Interoperable Europe Board	2.1 Overcoming the Boundaries Between Pubic, Private and Third/Forth Sector 2.8 Cross-sectoral Governance on European Level 3.5.2 Category Governance: *Legal Governance/EU-Governance*
	Interoperability agreements	2.1 Overcoming the Boundaries Between Pubic, Private and Third/Forth Sector 2.8 Cross-sectoral Governance on European Level 3.5.1 Category Harmonisation 3.5.2 Category Governance: *Governance Agreements*
	Interoperability Agency	2.1 Overcoming the Boundaries Between Pubic, Private and Third/Forth Sector 2.8 Cross-sectoral Governance on European Level 3.5.1 Category Harmonisation 3.5.2 Category Governance: *Legal Governance/EU-Governance* 3.5.2 Category Governance: *Governance Agreements* 3.5.2 Category Governance: *Cooperation and Rules*
Horizontal Functions		
	Multi Pattern Exchange Architecture	2.6 Secure and Trusted Online Environment 3.5.3 Category Architecture: *Architecture Management*
	Attestation-based Access Management	2.6 Secure and Trusted Online Environment 3.5.3 Category Architecture: *Architecture Management* 3.5.4 Category Data: *Data Access* 3.5.4 Category Data: *Data Management*

Annex IV: Questionnaires

Legal IOP

Table 3: Questionnaire: Legal IOP

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Cross-border legal basis for exchange of information "in the public interest"	A legal trust anchor is requirement. The "user involvement" in SDG OOTS is essentially a "work around" for this lack.	1	X	Low	High	High
Clearer data subject protection legislation in view of decentral data sharing (cf. wallet)	A problem with the concept of user control and user sovereignty and the ability and power of the citizen to their interest as a data subject	3		High	Low	Low
Cross-sectoral and cross-platform legislation, balancing the rights, obligations, and the protections of our citizen		4		Low	High	Low
Legislation on the EU level to harmonize the legal validity of data across borders	e.g. public procurement	2		Low	High	High

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
European Regulations	European regulations are required to bring harmonisation on the main barriers to the cross-border collaborative provision of public services.	1	Maximum	70%	Depending on the matter	Depending on the matter
Multi-identity matching for natural	Into Digital identity is now considered in	1	Maximum	70%	Low for legal persons	Low for legal persons with the ELI. High

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
person taking "sectoral" identities (or "personas" into account, cf. private sector) - based on sectoral legal provisions.	abstract, without considering that it is partly resolved in sectoral solution (e.g. unique identifiers for companies from BRIS, EESSI, etc.). One natural person has several administrative personas.				with the ELI. High for natural persons.	for natural persons that can be eased eIDAS2 implementing regulations and IOP solutions.
The legal validity of the identification as a natural person must be defined on EU level	What the legal value of EUID Wallet identification?	2	Maximum	70%	Low	Medium, if eIDAS2 includes attestation attributes with legal value for national identities, issued by matching them to the ID linked to the EUDIW. Then, it is up to Member States to implement identity matching procedures.

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Digital Ready Legislation and	This represents the overall principle, which is recommended to be followed.	1	x			

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Digital Policy Making						
Digital Ready Legislation and Digital Policy Making for EU Legislation	The Commission itself should be the addressee of Digital Ready Legislation and Digital Policy Making. In the context of the proposal for the Interoperable Europe Act, there are approaches (in article 3) in this direction. But, beyond these efforts it is important that the EC thinks and acts in this sense for its own legislation, means to implement all instruments as proposed in the Interoperable Europe Act and beyond that. In an operative perspective a technical and organizational definition for an implementation should be developed upfront, and the feasibility of such implementation as well as the interoperability aspects should be scrutinized in advance. Only after these steps, the legal framework definitions and the new lesgilative act should be drafted, proposed and negotiated.	2				

Solution Element	Description	Ranking (1-3)	Extra priority	Probability (high/low)	Complexity	Level of Barriers and Resistanc
Assessment of Once-Only related legal instruments (SDGR) vis-à-vis other instruments (eIDAS2) that focus more on citizens' digital sovereignty (also EU technological and data sovereignty) and VCs and extending legislation in the future to address "advanced topics" that have been relevant in DE4A: powers of representation, evidence/credentials revocation, S&N for automated	Explicit legal linkage may be needed between SDGR and eIDAS 2 or adding of SDGR governance mechanisms that integrate wallets into SDG architecture	1	+1	Dependin g On "advanced Topic" High for SDGR vs eIDAS2	Hig h	Dependin g On "advanced Topic"

Solution Element	Description	Ranking (1-3)	Extra priority	Probability (high/low)	Complexity	Level of Barriers and Resistanc
data updates without prior request/preview, deregistration, interrupted procedures. Cross-sectoral and cross-platform legal alignment	or amending SDG….					
Fully developing provisions in Interoperable Europe Act (e.g. Interoperable Europe Board, policy implementation support projects, regulatory sandboxes)	(cf. WP7)	2		Low	High	High according to ambition / complexity
Solutions to overcome gaps/barriers for **the cross-border recognition of legal value** of evidence/credentials/documents	Recognized repeatedly in DE4A	3	+1	High	High	Can be High depending on national legislation
Guidelines to identify and address legal interoperability barriers through "interoperability and digital checks" for new EU legislation screening (EIF recommendation 27) **including coherence checks between (potentially overlapping) legislation.** Also exchange of best practices in this regard between MS and EC DGs.	Q: public/private	4		High	High	Low to undertake but high to apply in each case
Extending Open Data re-use to semi-open data (certain categories of protected data held by public sector bodies) sharing c.f. provisions in Data Governance Act (**creating single information points with registers of available information searchable at EU level**)	Q: imbue registers with legal value for automated transactions A: Yes, example of the transaction system of Notaries in Spain.	5		Low	High	High if not prioritised / made mandatory

Solution Element	Description	Rank (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Legal requirements for procedures that are in agnostic of formats		2		low	high	high
Legal validity of canonical evidence in union law	Contract/agreement based trust works for bilateral exchanges today, but it has his barriers in an EU of 27	1		high	high	low

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Legal basis for horizontal data exchange	Could be consent					
Increased democratic control on European Level to instil individual trust	Trust of citizen and administrators presently anchored in national administrative frameworks					
Make legislation technology independent (no paper or technology specifics)	Reduce “paper dependency” of legislaton					

Solution Element	Description	Ranking (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Rules and Ethics for the Data Economies	From Code to law and law to code	1		high	high	high
Legal frameworks that are not primarily bound to geographical borders (digital citizenship)	Use supranational bodies like OECD to further the EU/MS agendas. Maybe even the WHO regions can help sometimes as they maybe more natural.	2		low	high	high
Fiscal harmonization	Same currency, same simplified tax levels. Globally for dApp stores (via WTO) and within EU.	3		low	low	high

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Interoperability checks	Systematic assessment of new legal proposal for adherence to interoperability principles. The Interoperability check must be mandatory for each legal proposal on national and Union level.					
Mandatory building blocks at sufficient level of specificity	Building blocks should become mandatory to use across the Union. Currently, BB are not specific and standardized enough and mandatory in their us, leading to lack of interoperability (e.g. multiple, non-interoperable eDelivery configuration).					
Legal validity of harmonized, structured data from authentic sources and the obligation to accept this data	Harmonized structured data definitions that facilitate communication throughout the Union need to be imbued with legal validity their acceptance as evidence made mandatory.					

Organisational IOP

Table 4: Organisational IOP

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Catalogues of trusted entities (i.e. public administrations) and their mandates and (information) rights	We need a clear understanding who is able to request what data ana for what purpose	1	X	Low	High	High

Solution Element	Description	Ranking (1-3)	Extra priority	Probability	Complexity (high/low	Level of Barriers and Resistances
Public organisation Catalogues as open data	**Catalogues** under common open data APIs to provide information on the **organisation of competent authorities** in each Member State	1	Max	60%	High	High because of complexity
Administrative procedure catalogues as open data	**Catalogues** under common open data APIs to provide information on available administrative procedures provided by the competent authorities of each Member State Note that an administrative procedure is not automatically a public service, they can be also regulated services executed by private organisations. This can extend to professions.	1	Max	60%	Medium	High because of scarce human resources
Base registries catalogues as open data	**Catalogues** under common open data APIs to provide information on base registries, their data services and access constraints in each Member State	1	Max	60%	Medium	High because of scarce human resources

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
IOP Act	The means in the proposed Interoperable Europe Act should be followed.					

Solution Element	Description	Ranking (1-3)	Extra priority	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Alignment of digital transformation processes within MS and **between MS** (where necessary) for areas identified as priorities for cross-border collaboration (or which must be addressed within given timeframes according to existing or new approved legislation) => how? **Exchange of architectural blueprints?**	The problem of process alignment between MS. More bottom-up alignment on organisational level. Example: insights gained in OOTS working groups and DE4A between MS	1		Low	High	High: diversity of national approaches, maturity in digital transformation, cultural and legal differences, low awareness of administrative organisation across MS.
Best practices and mechanisms to facilitate coordination and collaboration between diverse groups especially for cross-border collaboration, in particular with coordinating teams per MS and multi-month phase for establishing alignments, priorities, ensure financing and resources… for complex undertakings. E.g.	MS alignment team/node (split alignment within MS and between MS) Strategic alignment (goal alignment) as a separate phase, taking into account the available resources Best practice coordination tools for execution phase	2	+1	High (as seen in DE4A)	High (but necessary)	High depending other priorities. Requires enhanced exchanges and multidisciplinary experts availability, availability of collaboration tools, access to good documentation, etc.

Solution Element	Description	Ranking (1-3)	Extra priority	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
projectathons, iterative scoping and Agile methods, agreeing over UI/UX through wireframes, use of online messaging tools for developers and integrators, availability of good technical documentation, training over common building blocks…						
Libraries of business processes relevant for cross-border integrated public service delivery modelled under a common methodology / expressed with commonly agreed artifacts for business architects (use of Archimate, etc.) c.f. EIF recommendation #28	Common EU business architecture framework	3		Low	High	High due to diversity of approaches and effort involved

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Harmonization or best practice on the level of administrative processes	Today the same type of service is provided in very different ways across the Union with very different requirements	2		low	high	high
Access and re-use of decentral registries to increase the scope on which this information can be used	How can we manage and react best to changes in organisation responsibilities, e.g. as result of government changes in a way that is fit for automated used?	1		high	high	high

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Responsibility for data at the leaf-level (The organisational unit itself, not some higher administrative responsibility)		2		low	high	high

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Refocus on organisation to organisation integration	Instead of handing data to the user					
Solving the record matching problem	Identification and matching of subjects across borders (users, businesses, buildings, cars, etc.)					
Education and skills development	e.g. Tiger Leap initiative of Estonia					

Solution Element	Description	Ranking (1-3)	Extra priority	Probability	Complexity	Level of Barriers
"Digital Twin" of the citizen controlled by the individual	Including "Subjective attestation" (value ascribed to traits by society and/vs. the individual)	2		High	low	high
Value-model of the data economy	That is "fair" between government, business, and private person	1	2	low	high	high
Enabling existing registers (i.e. for skills and professions) for automated transactions	ISCO Standard from ILO as example all the way to certificate for Online education	3		high	low	high

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Loose coupling of business services	Focus of the contact points and interactions, irrespective of back-office					

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
	procedures (not to be too intrusive internal processes technology of organisations					
Registers of services and data sources	Directory of public sector bodies and their responsibilities and the way to address them.					
Business Process documentation	Common description language and accessibility of documented processes / business services					

Semantic IOP

Table 5: Semanic IOP

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Model/Methodology for semantic agreements	The method how to come to semantic harmonization is important and needs to be backed by the right governance, e.g. company representation remains unresolved.	2		High	High	Low
European harmonization of semantics	Not merely mapping, but true harmonization	1	X	Low	High	High

Solution Element	Description	Ranking (1-3)	Extra priority	Probability	Complexity (high/low)	Level of Barriers and Resistances (high/low
Reference data models (incl. definitions and data domains)	Reference data models for the cross-border exchange of information, providing clear and unambiguous definition, semantic and syntaxis of data attributes. These should be higher-level models than the national/local operational models. This is more about semantic than syntax.	1	Max	60%	High	Medium-high: Barriers due to legacy data, data diversity and scarce human resources
Sematic definitions in sectoral and temporal context (different universe of discourse)	Models and definitions are context specific and apply for a given use-case. These should be referred to reference data models and shared in an open common repository of semantic assets.	1	Max	90%	Medium	High because of the little openness of sectoral environments and little human resources

Solution Element	Description	Ranking (1-3)	Extra priority	Probability	Complexity (high/low)	Level of Barriers and Resistances (high/low
Semantic elicitation approach	A knowledge engineering approach that is consistently applied to come repeatedly to actionable results in different context. It should be a live IOP solution publicly available. AI can help in this context for discovery of semantic aspects for reusability.	1	Max	40%	Low (a lot of background)	High, because it is wrongly seen as not necessary

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Complexity	Semantic is always an important topic, but: It is hard to close the "circle"; the practitioners are coming from the base with its own tools and tasks (challenges), but the frameworks or available elaborations do not fit; so the two worlds are not coming together. For example: the "EC catalogues" for semantics are very comprehensive but much too complex and therefore often not practicable for real world challenges.	1				
Use Case orientation	It is important to consider and question what the use case for semantics represents (knowledge and estimation). This should be the starting point for a step by step definition and deepening. This would accelerate a common understanding, quick wins and could accelerate the whole analytical process. This is recommended instead of the definition and consideration of large bundles of definitions/catalogues, which cannot be implemented in due time.	2				

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Representations, powers and mandates	It is important to define (on common ground), how deep representations, powers and mandates can be implemented for cross-border cases in a useful manner; In this sense same as before: first the easy achievable realisations to cover the most challenges and afterwards the more granular definitions (if necessary).	3				

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Approaches that enable **effective standardisation** of (structured) evidences, DE4A has proven the advantages of using harmonised semantic models (canonical evidence types for evidence exchange) but effort should be oriented to enable correspondence of domestic evidences driven by national regulations towards canonical evidence types and new knowledge creation through **semantic agreements.**		2	+1	High if mapping prioritised on certain domains of evidences and procedures	High	Low if supported from EC and MS
Common ontologies and **European harmonisation** rules to identify properly concepts/meanings/syntaxis, to preserve meaning across borders and across contexts and	This includes the methodological approach for semantic harmonization	3	+1	Low	High (multiple elicitation challenges, heterogeneous	

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
to represent information to exchange cross-border as pre-condition to design evidence types required in exchange use cases with participation of **domain experts in communities of practice** from numerous authorities in different MS.					communities of practice)	
Promote experience and benefits achieved on semantic interoperability from DE4A (toolkit comprising Information Desk -IAL, **ESL-MOR**, Information Exchange Model) as several aspects can be relevant for future projects		1	+1	High (if interest confirmed)	Low (documentation available from DE4A)	Low (good collaboration with SDG semantic experts)

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Semantic harmonization of canonical evidence from a 'minimal dataset'-perspective	Legal and semantic are closely related	1		high	high	high
Sematic harmonization that includes the definition of code lists	Have choices rather than free text attribute domains. Harmonization needs to go beyond data models.	1		high	high	high
Dynamic data model creation	Data models (canonical evidences) are created dynamically by the requirement of the procedure	1		low	high	high

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
European Service Catalogue	Not only limited to the public services					
European ontology and code lists of core object typers	Example (one registry for streets..); Picture of a digital twin of the union.					
Enable existing registries for automatic transactions						

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Combination of sectoral harmonization	Example of healthcare information and food industry	3		high	high	high
Cross-domain Ontology	Top-level ontology (ISO21838) as starting point	1	3	high	high	low
Well-functioning language models	chatGPT	2	XXX (helps all other parts)	high	high	High

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Harmonization to the level of fully automated reuse of structured data though the use of re-use of sufficiently mature core vocabularies	Core vocabularies must be directly useable and detailed to have agreed, multi-lingual terms and definitions that are fit to be directly used in projects, otherwise we continue to use project-specific dialects. This should include controlled vocabularies (code lists / defined attribute domains).					

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Semantic harmonization for a common, European communication layer	The internal working of transactional systems in MS should not be impacted					
Maintained, cross-sectoral repository and discovery of semantic definitions	Semantic assets can only be used if they are easily accessible and understandable				high	

Technical IOP

Table 6: Technical IOP

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
EU-level data access management (data sharing rights)	Personal information management perspective (**not** purely consent management!)	1		High	Low	Low
Data access not strictly bound to one exchange logic	Direct registry access, message exchange, wallets, etc…	2		Low	High	High

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Reusable EU building blocks	Accompanied with specific implementation profiles (concrete configurations)	2	Medium	60%	Medium	High due to technology rate evolution
Toolbox for a multi-pattern architecture	Multi-pattern extends to the other interoperability layers (not only technical)	1	High	70%	Low	High due to the current fragmentation and isolation of approaches
Function abstraction layer driving the integration	Example of the DE4A Connector that is too specific for a one implementation. As opposed to use abstract classes.	1	High	60%	Low	High due to the extra effort required to design the abstract layer

Solution Element	Description	Rating (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Mobile Government	Standardisation for interoperability in mobile applications are important; this could be seen	1	x			

Solution Element	Description	Rating (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
	especially in cross-border App2App communications (e.g. for eIDAS-compliance); overall SSO should be considered in this field.					
Standards	The technical realisations should be based on standards, this is more important when it comes to new technologies, such as mobile applications.	2				

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Multi-architecture pattern approaches can be adequate for multi-domain cross-border systems to support different public admins and end user requirements.		1	+1	High	High	High (depending on understanding of cost-benefit, level of "open-mindedness")
Grouping of technical functions under a common single point of interaction or proxy (e.g. DE4A Connector) can enable large savings in effort and time for MS	Will be required to enable a hybrid situation between federated and decentralized also on a	2	+1	High when benefits are understood based on real cross-border operations	Low (compared to alternatives)	Can be lower for MS with previous experience with such solutions and higher for others, depends on

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
when integrating /inter-communicating digital services, also hiding national details and complexity not needed for the agreed protocols for cross-border interoperability.	long-term perspective					organisational culture too
Easy access to catalogue of interoperability solutions (e.g. improved EIRA CarTool) and working examples of cross-border implementations (with adequate support for common building blocks under DEP, ISA2…) and large-scale piloting bringing together the public **administration stakeholders with the businesses and citizens** that will benefit from cross-border services **to ensure solutions such as EUDI Wallets are properly validated** before	The next level of cartography of the solution space. Cross-sectoral and public/private validations (i.e. LSPs)	3	+1	High (due to necessity)	High (efforts, funding and resources need to be mobilised)	High depending on other priorities

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
their deployment (overcoming language barriers, reaching high levels of usability, etc.)						

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Machine readable semantic definitions	Expectation that these are mostly human-managed ontologies in t=4; Emerging ontologies might have still their limits to be used in areas like eGov. (garbage in/out problem)	1		high	high	high
Computer-aided ontology-management solution	Probably driven by machine learning technology. Already today that could greatly help to navigate and understand distributed semantic repositories	2		high	high	high
Use of edge computing to capture and machine learning to manage registries/code lists etc.	e.g. responsibilities of organisation and within information, like the management of data sources and the responsible organisations.	2		low	high	high

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Integrated data sources	API access as preferred mode					
“Pure standards” Instead of vertical standards						
European Consent Management Service	Managing consent beyond the single exchange to regular exchanges					

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Sustainable (green) information technology	DLT like Hedera vs Bitcoin, Ethereum, EBSI. Eg. https://www.globalreporting.org/how-to-use-the-gri-standards/gri-standards-english-language/	2		high	Both if just accounting low	High
The ID Wallet concept	Build on citizenship as identity anchor, but even more liberal that the present approach, based on a SSI logic. First SSI, then anchor to national IDs.	1	1	high	high	Low we are all dead tired of U/P
Attestation/Attribute-based Access management	Example of access to physical location, like churches in DK. Roles are just attributes.	3		low	high	Low as it can be market driven

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Toolbox of directly reusable BB	BB must be sufficiently specific to be used without much project specific configuration. "Plug-and-Play" BB, that encapsulate semantics definitions and technical protocols in a directly interoperable service.					

Governance IOP

Table 7: Goverance IOP

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Governance body that drives use-cases (across different sectors) towards established, cross-sectoral infrastructure	Creating horizontal infrastructures is only successful if all vertical/ sectoral use cases make use of that infrastructure instead of developing/renewing their own sectoral solutions	1		High	High	Low

Solution Element	Description	Rating (1-3)	Extra priority	Probability	Complexity	Level of Barriers
Light-weight (not requiring legislation) approach to agree on use cases or functional extensions of the infrastructure	As opposed to a strict list of cases in legislation like the SDGR Annexes	2		Low	Low	High
Sectoral governance to establish trust and basis for cross-border data access	This is required to ultimately come to legal basis for this access.	3		Low	Low	High

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
IOP Governance Committee	As proposed by the Interoperable Europe Act	1	Maximum	90%	Low	High due to scarce human resources
IOP Advisory Committee	As proposed by the Interoperable Europe Act	1	Maximum	90%	Low	High due to scarce human resources
European interoperability agreements that are also **mandatory** across all administrative sectors at EU level	A procedure to make IOP agreements legally binding when cross-border systems and people have to interact	1	Maximum	70%	Low	High due to DGs resistance to adopt external IOP mandates
An interoperability assessment of legal proposals at European level	Include in the current assessment reports of EU act proposals an evaluation of whether IOP is guaranteed by their provisions	1	Maximum	70%	Low	High due to DGs resistance to adopt external IOP mandates and little human resources to conduct the

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
						IOP assessments

Solution Element	Description	Rating (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
	The proposed means in the Interoperable Europe Act should be followed. Four articles (see Chapter 4) in the proposed Interoperable Europe Act address this topic.					

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Governance interoperability agreements (EIF recommendation 26)/common governance framework(s) between or common to cross-border systems covering **both G2G (OOTS, sectoral systems and successors) and C2G, B2G, C2B, B2B (EUid/Wallet and others)** based on **agreed standards/specifications/ guidelines** (EIF recommendations 21-24) and covering well scalability, availability, quality, change	Could be under umbrella of policy programmes like Digital Decade, ministerial declarations (Berlin…); Cf. Interoperable Europe Act Cf. industry level standards and guidelines. eTOM, ITIL	1	+1	Low?	High given the number of different groups of stakeholders involved, ambitious scope of agreements and challenges especially in cross-sectoral	High (e.g. conflicting views public-private sector)

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
management, disaster recovery (EIF recommendation 25)						
Governance support to basic principles informing "ONE" vision of DSM/eGov for long term with specific focus on citizen-centricity and empowerment, digital self-determination and sovereignty, inclusion and combatting the "digital divide", integrated public services provision.	Basis for principles can be Declaration on Digital Rights and Principles for the Digital Decade, EIF, etc.	2	+1	High (good basis of principle to consolidate)	Low	High to fully develop / apply / operationalize principles in practice
A good understanding of organisational structure within MS and of roles and responsibilities can be key for the success of ambitious initiatives between MS. **Availability of governance information.**	Cf. administrative levels etc.	3		High if information is made easily available	High (multiple levels of administration, sectors…)	High if motivation / understanding of benefits is lacking
Collaborative governance models (templates, multilateral agreements?) based on the experience of large cross-border governance approaches (eIDAS, SDG, sector-specific) that can support multi-stakeholder collaborative business processes (including where relevant private sector), enabling cross-sectoral use cases, and considering also how corresponding financial needs can be adequately covered.	We may need to aim for a substantial evolution of EIF and EIRA based on a wide discussion and agreement for emerging priorities, shared objectives, principles, timelines and the role of governance to facilitate further alignment	4	+1	Low (as highly complex to reach consensus towards substantial evolution of EIF/EIRA)	High	High as different mindset needed for cross-border and cross-sectoral governance modelling and for breaking silos towards user-centric

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
	around shared digital services/frame works to **break away silos and obsolete 'administration-centric' design.**					administration
Skills development for interoperability expert and pooling of experts	Lack of skills / senior experts (eID, record matching, powers and mandates, eDelivery…) needs to be also addressed: initiatives like **"Interoperability Academy"** should be fostered and followed up as well as ways to pool and share such expertise among MS.	5	+1	High if will exists to train new experts	High (complexity of pooling experts)	High (resistance to share experts' time to train others)

Solution Element	Description	Rating (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Sematic agreements incl. lifecycle of the agreement	Versioning	2		Low	high	high

Solution Element	Description	Rating (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Union-level management of code lists		1		high	high	high
Unions-level semantic standardization body		1		high	high	high

Solution Element	Description	Rating (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Horizontal integration of services governance	Beyond Taxud, BRIS, EUCARIS					

Solution Element	Description	Ranking (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Governance that transcends the current legislative and administrative borders	Acceptance of certificates across jurisdictions. Eg. Liability for MDR or FDA	1		Low	high	high
Self-sovereignty of technical solutions	We will have both open and closed code. But maybe we have to divulge the requirement or the Questions asked.	3		high	low	low
Operational governance of biometric information	Ethnicity	2		High	Low	high

Solution Element	Description	Rating (1-3)	Extra priority weight	Probability (high/low)	Complexity (high/low)	Level of Barriers and Resistances (high/low)
Mainly Member-state driven Governance to mandate transveral interoperability solutions across the Union and to provide **biding advice** in interoperability checks of European legal proposals	The importance is the governance must be able to mandate (not merely recommend) solutions that are applicable across sectors and member states. The **Interoperable Europe Board** could develop into such a governance body, by adding the required tasks and mandates.					
Union-level interoperability **agency** to maintain interoperability solutions and manage interoperability infrastructures and services	The current fragmentation and programme financing (5 years) results in fragmentation and continuity issued (inc. knowledge and competences): ISA/CEF, CEF BB, DEP, IOP, Digital Policy Programme, TESTA, GEANT, sectoral solutions (PEPPOL, EESSI, BRIS) and cross-sectoral solutions (OOTS, EUDI Wallet)					

Annex V: Mind Maps following EIF layers

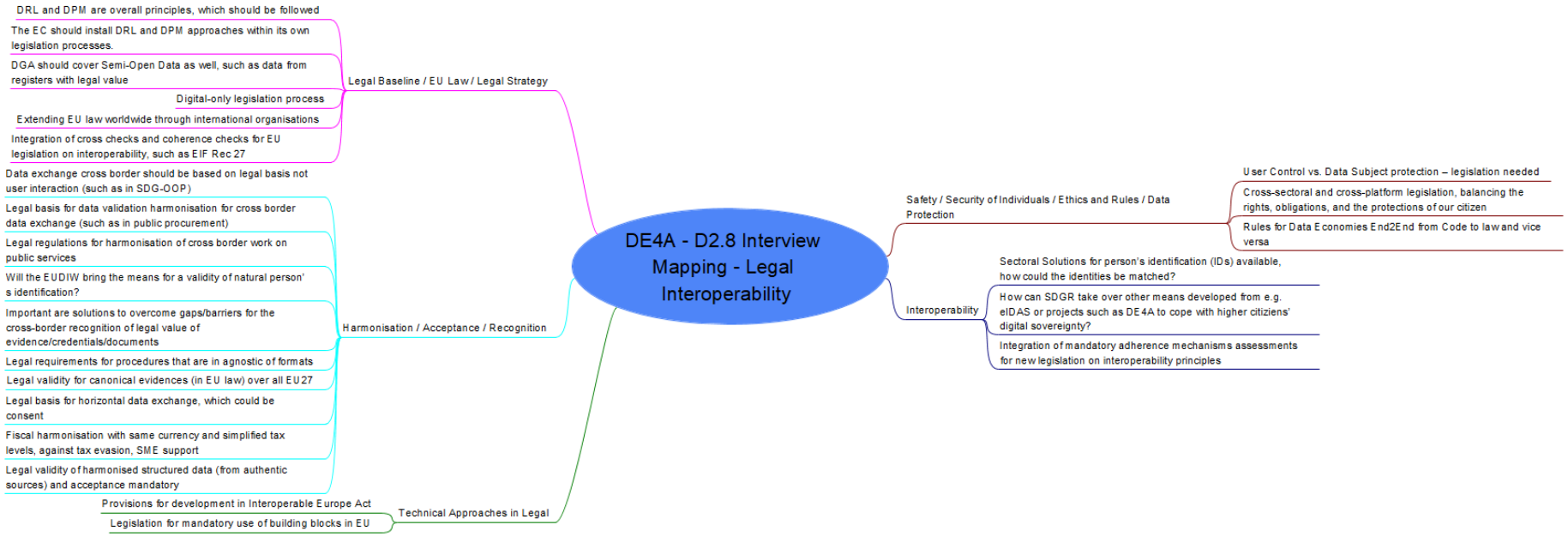

Figure 7: Legal IOP Map (EIF Layer Structure)

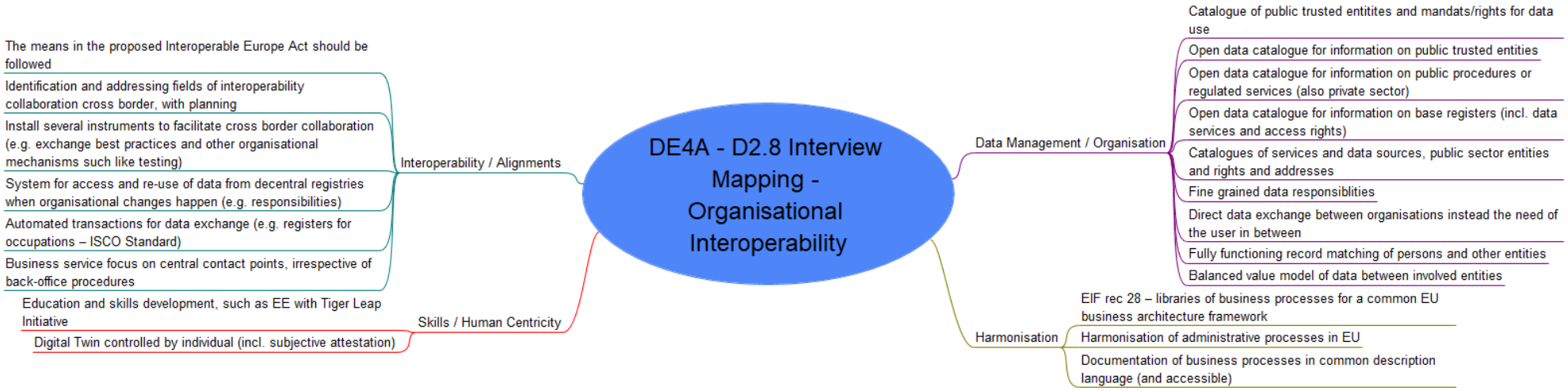

Figure 8: Organisational IOP Map (EIF Layer Structure)

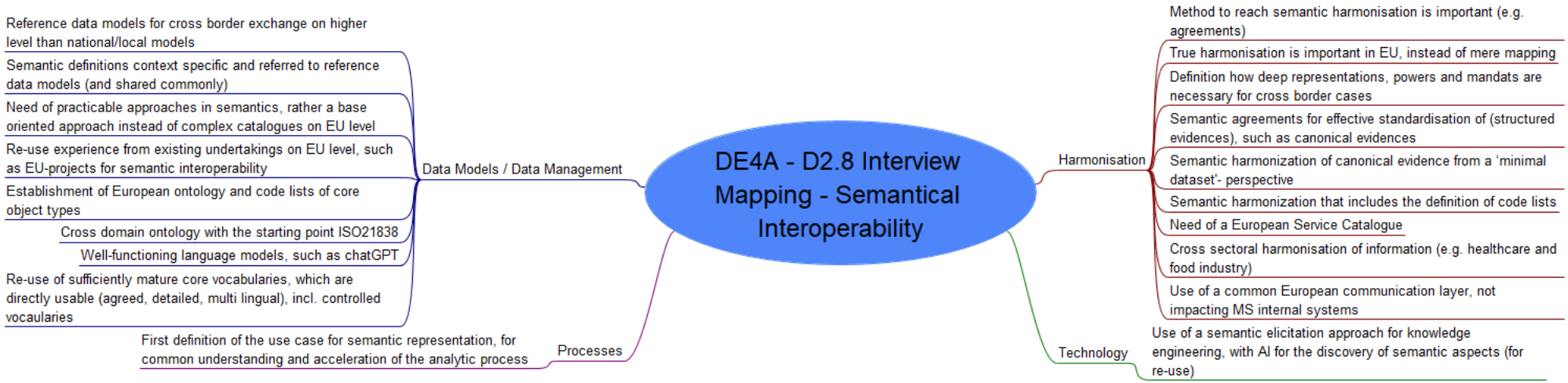

Figure 9: Semantical IOP Map (EIF Layer Structure)

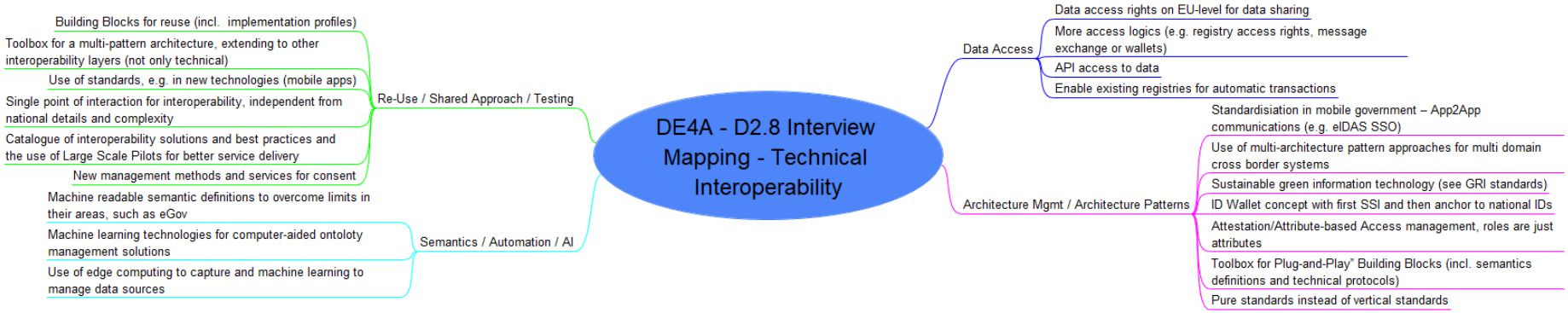

Figure 10: Technical IOP Map (EIF Layer Structure)

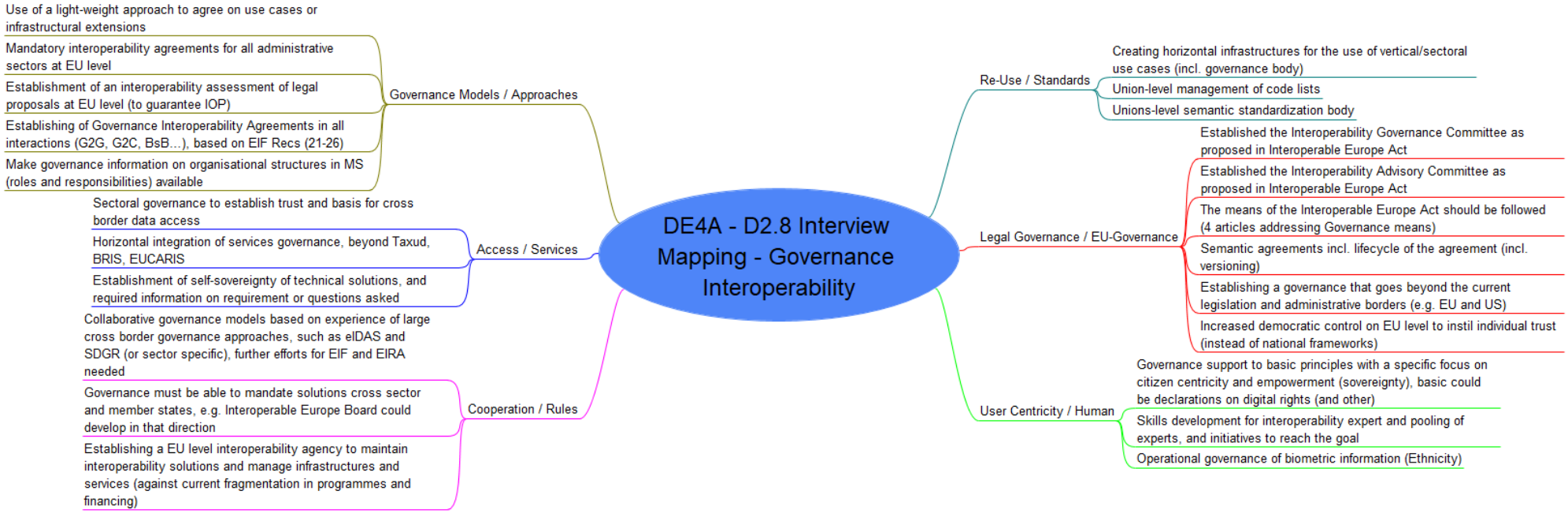

Figure 11: Governance IOP Map (EIF Layer Structure)

[page intentionally blank]