Co-funded by the European Union

DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

D8.1 Governance registries and frameworks

Version 1

Work package	WP 8
Task	Registers of governing authorities, verifiable data registries, trust registries, attribute / schema registries, ecosystem members, and guidelines for ecosystem member enrolment.
Submission date	31/01/2024
Deliverable lead	VM – Finnish Ministry of Finance
Version	1
Authors	Teemu Kääriäinen (VM) Antti Kettunen (VM)
Reviewers	Andreea Dinu (ICI Bucharest) Alberto López (INCM) Lluís Alfons Ariño Martín (SGAD) Gerd Bauer (DVSV) Stefan Liström (SUNET)

Abstract	The purpose of this study is to create a foundation for DC4EU consortium Ecosystem Governance Framework (EGF), which addresses governance-related topics, such as privacy protection, security standards, interoperability, user-centric design, trust frameworks, legal and regulatory compliance, and governance structures. The study uses an enhanced version of the Trust Over IP (ToIP) metamodel to provide a set of tools that can be used to identify gaps, overlap, and inconsistencies in existing governance frameworks, and to effectively communicate the most relevant EGF control documents to project stakeholders. Finally, the study will be further extended during the project lifecycle so that it can be adopted by additional domains (education and professional qualifications, and social security) and Member States, and to make the tooling from usable for project stakeholders.
Keywords	eIDAS, EUDI wallets, governance, ecosystems, interoperability, trust frameworks, ecosystem governance frameworks, legal and regulatory compliance.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	30/10/2023	1st version of the deliverable for comments	Teemu Kääriäinen (VM) Antti Kettunen (VM)
v0.8	06/11/2023	2nd version updated based on comments	Andreea Dinu (ICI Bucharest) Alberto López (INCM)
V0.9	23/01/2024	3rd version updated based on comments	Lluís Alfons Ariño Martín (SGAD) Gerd Bauer (DVSV) Stefan Liström (SUNET)
V1.0	31/01/2024	Version of deliverable approved internally by COO & Strategic Committee	SGAD, Strategic Committee

DISCLAIMER

COPYRIGHT NOTICE

Project co-funded by the European Commission in the Digital Europe Programme		
Nature of the deliverable:	**R**	
Dissemination Level		
PU	Public, fully open, e.g. web	**X**
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to DC4EU project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

EXECUTIVE SUMMARY

DC4EU consortium's goal is to pilot education and professional qualifications, and social security use cases in an EUDI wallet ecosystem based on the revised eIDAS regulation. As such, the consortium will need to establish a complex, decentralised, cross-border data exchange ecosystem, which needs to ensure that a common set of guidelines are followed across piloting partners. In order to effectively manage such an ecosystem, there is a need for a comprehensive Digital Identity Ecosystem Governance Framework (EGF).

Ecosystem Governance is a complex topic, which needs to cover aspects related to e.g. privacy protection, security standards, interoperability, user-centric design, trust frameworks, legal and regulatory compliance, and governance structures. Further complications are created by varying Member State regulations, varying levels of maturity in education and professional qualifications, and social security sector digitalisation across Member States, and the existence of existing data exchange initiatives and governance frameworks.

As such, it is not possible to use any existing EGF as a basis, but adaptation and flexibility is needed from the framework to address the governance-related challenges of such a complex, decentralised ecosystem.

Trust Over IP (ToIP) metamodel provides one way to model a governance framework that can be used to build an EGF for EUDI wallet-based ecosystems. Closer study of the metamodel revealed that in its current form the model was not suitable to build an EGF for DC4EU consortium use, but instead it needed to be augmented with additional capabilities.

This study has showed that with the enhanced ToIP metamodel it is possible to come up with an EGF that can be effective in identifying existing governance frameworks to identify overlaps, gaps, and inconsistencies across them. The enhanced metamodel can be also used as an effective communications tool of the EGF control documents that deal with e.g. privacy, data protection, governance structure, and cybersecurity.

The study was initiated by first creating a questionnaire that was sent out to DC4EU consortium partners to get a general understanding of the current state of education and professional qualifications, and social security sector governance in the Member States, and within the existing data exchange initiatives. Additionally, the governance structure of the EBSI network was studied. The study focused on national registries and legislation, shared data models, data protection and retention, governance structures, and technical standards that are relevant for the ecosystem governance. In parallel to the study of the current state, the ToIP metamodel was studied and extended to better cover the existing governance frameworks applicable in DC4EU ecosystem piloting. Finally, the results from the current state analysis were integrated with the enhanced ToIP metamodel to come up with education and professional qualifications, and social security sector specific mappings of governance structures.

This was the first iteration of the DC4EU ecosystem governance study, but the EGF will continue to be developed throughout the project lifecycle. Additional updates to the EGF include e.g. extending the study to social security domain, including additional Member States and data exchange initiatives to the study, and improving the ability to use the developed tools to communicate about the most relevant EGF control documents.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

TABLE OF CONTENT

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

LIST OF FIGURES

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

LIST OF TABLES

N/A

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

TERMS AND ABBREVIATIONS

API Application Programming Interface

ARF Architecture Reference Framework

Bologna Process A set of agreements between European countries to ensure comparability in the standards and quality of higher-education qualifications.

Control Document For example a policy, regulation, or guideline that is used to define some aspect of the Ecosystem Governance Framework (EGF), such as data protection, user-centric design, or legal and regulatory compliance.

Digital Identity Ecosystem Governance Framework A structured set of rules, standards, and principles that help govern the development, operation, and management of digital identity systems.

Diploma Supplement A document which provides information that makes it easier for employers and education institutions to understand an educational qualification.

EAA Electronic Attestation of Attributes

EBSI European Blockchain Services Infrastructure

ECTS European Credit Transfer and Accumulation System

EDC European Digital Credential for Learning

EDIC European Digital Infrastructure Consortium

EGF Ecosystem Governance Framework

eIDAS European Union regulation for electronic identification and digital trust services.

ELMO Data format for the exchange of (education) result information.

EMC EMREX Contact Point

EMP EMREX Client

EMREX European education data exchange initiative.

EUDI European Union Digital Identity

GDPR European Union General Data Protection Regulation

metamodel An overall model which composes of elements, which themselves are models.

MS Member State

SDG/OOTS Single Digital Gateway / Once-Only Technical System

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

ToIP	Trust over IP

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

1. INTRODUCTION

DC4EU consortium is engaging in the piloting of European Digital Identity (EUDI) wallets in the education and professional qualifications, and social security sectors. As such, its aim is to establish a decentralised cross-border ecosystem of actors that need to follow a common set of guidelines when taking part in the piloting activities. For this purpose, the consortium needs an effective *digital identity and data ecosystem governance framework* (EGF).

Digital identity and data ecosystem governance frameworks are structured sets of rules, standards, and principles that help govern the development, operation, and management of digital identity systems. These frameworks are essential for ensuring the secure, privacy-respecting, and interoperable use of digital identities in various contexts, such as education and professional qualifications, and social security in the case of DC4EU. They define how digital identity systems should be designed, implemented, and regulated to protect the rights and interests of individuals, relying parties, and other stakeholders.

DC4EU Work Package 8 has been tasked with defining a general model for digital identity and data ecosystem governance for DC4EU consortium piloting, and to build the foundation for the adoption of the ecosystem governance model in education and professional qualifications, and social security domains. Eventually, the goal of the consortium is to create a coherent, secure, and user-centric environment for EUDI wallet piloting that benefits end-users, piloting partners, and society as a whole.

1.1 KEY COMPONENTS OF ECOSYSTEM GOVERNANCE

Digital identity and data EGFs should primarily focus on the following components of ecosystem governance:

Privacy protection

Ensuring that individuals have effective full sole control over their identity and personal data and consent to its use in the EUDI wallet ecosystem. This typically involves compliance with local and EU-level data protection regulations, such as GDPR [10].

Security standards

Defining security measures to protect the systems that are part of the EUDI wallet ecosystem from unauthorised access, data breaches, and fraud. This includes using capabilities, such as strong authentication methods and encryption.

Interoperability

Establishing standards and protocols that enable different parts of the EUDI wallet ecosystem to work together seamlessly. Interoperability is crucial for cross-border or cross-sector use cases that are within the scope of the DC4EU consortium piloting.

User-Centric Design

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

Focusing on the needs and preferences of users, making digital identity wallets and accompanying solutions user-friendly and accessible to all, including individuals with disabilities.

Trust Frameworks

Developing a system of trust and assurance among parties in the EUDI wallet ecosystem through the use of accreditation and certification processes. DC4EU aims to adopt capabilities that have been established as part of the European Blockchain Services Infrastructure (EBSI) trust framework.

Legal and Regulatory Compliance

Ensuring that the systems that are part of the EUDI wallet ecosystem adhere to relevant national and EU-level laws and regulations.

Governance Structure

Defining the roles and responsibilities of various stakeholders, such as *electronic attestation of attributes* (EAA) providers, wallet providers, relying parties, authentic sources, and accreditation bodies.

1.2 THE ECOSYSTEM GOVERNANCE CHALLENGE

DC4EU consortium will pilot a decentralised, cross-border data exchange ecosystem built on top of the revised eIDAS trust service regulation and European Digital Identity (EUDI) wallets. The main use cases include cross-border data exchange of education and professional qualifications, and social security-related verifiable data (including e.g. attestations or entitlement documents for social security coordination).

DC4EU consortium EGF should facilitate building a trustworthy, secure, and privacy-preserving data exchange ecosystem in order to manage the complex multi-party data exchange activities happening between the consortium partners. Some practical examples of the challenges that the EGF should solve include e.g.

- Reducing the need to maintain a multitude of bi-lateral agreements between parties, which eases the onboarding of new ecosystem members.
- Establishing the necessary security and authentication standards to ensure that individuals are who they claim to be, reducing the risk of fraudulent activities.
- Incorporating the necessary safeguards for user privacy and personal data protection. By setting guidelines for data collection, usage, and sharing, the EGF should help ensure that individuals' sensitive information is handled responsibly and in compliance with relevant data protection laws.
- Prescribing security measures, like encryption, multi-factor authentication, and periodic security audits, to mitigate vulnerabilities and breaches.
- Defining the necessary trust frameworks and certification processes to ensure that participants in the digital identity ecosystem are reliable and trustworthy.

Conducting data exchange in a cross-border setup poses challenges related to establishing an EGF. As such, the EGF should address issues related to following aspects of cross-border piloting:

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

- There may be significant differences in Member State (MS) regulations related to the use of digital identities. EGFs should be flexible enough to be able to address the varying local regulations between MSs.
- MSs may be at varying levels of maturity in relation to the digitalisation of education and professional qualifications, and social security data exchange. Some MSs may have very mature and well-defined data exchange ecosystems, whereas some MSs may be taking their first steps in digitalising their education and professional qualifications, and social security domains.
- There exists a multitude of pre-existing, voluntary, non-regulation based cross-border data exchange initiatives with which interoperability should be achieved.
- There exists overlap, gaps, and conflicts in the governance rules and policies of local regulations, EU-level regulations, and existing data-exchange initiatives.

These aspects need to be appropriately addressed in the DC4EU consortium EGF in order to enhance the ability of the ecosystem partners to adopt a common decentralised governance approach.

1.3 SOLVING ECOSYSTEM GOVERNANCE IN DC4EU CONSORTIUM PILOTING

The purpose of this document is to study the actions needed in order to establish the foundational definitions for DC4EU Ecosystem Governance Framework (EGF). The EGF consists of a set of consortium-specific ecosystem-level governance *control documents* that define rules and recommendations for various aspects of interoperable cross-border verifiable educational, professional qualifications, and social security data use and processing.

The document starts by studying three types of existing domain-specific governance frameworks:

- National governance frameworks used by Member States in the education and professional qualifications, and social security sectors focusing on national registries and legislation, data models, and data protection and retention.
- Existing domain-specific cross-border data exchange-related governance frameworks.
- Governance frameworks used in the EBSI trust framework.

Revised eIDAS regulation and EUDI wallets are influenced by the concepts of Self-Sovereign Identities (SSI). In order to effectively deploy SSI solutions on various domains, there is a need for an open governance framework that can be adapted to various use cases to ensure their trustworthiness. Governance frameworks are often developed as domain-specific solutions, whereas EUDI wallet LSP piloting requires a framework that is generic enough to cater for the different needs arising from different domains and Member States. As such, DC4EU WP8 has chosen one of the central governance frameworks developed in the SSI domain, the Trust over IP (ToIP) framework, as the foundation to study its applicability as the basis to define the DC4EU EGF. After introducing the basic concepts and layer model of ToIP, the document continues to map the existing governance frameworks to an EGF model which is based on an adapted version of the ToIP framework.

The Trust over IP (ToIP) Foundation has defined the ToIP Governance Architecture Specification [20] to specify the standard requirements that apply to all ToIP compatible governance frameworks (GFs) regardless of their layer in the ToIP stack (utility governance layer, agent/wallet governance layer, trust task governance layer, which includes credential

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

governance, and ecosystem governance layer), and the ToIP Governance Metamodel Specification [21] and its companion guide [22], to provide an overall template for ToIP-compatible governance frameworks from which layer-specific templates are derived. It identifies a set of controlled documents which form the trust framework itself. As such, the DC4EU Trust Framework can benefit from the general approach set forth by the ToIP Foundation.

Finally, a comprehensive hierarchical model of DC4EU ecosystem governance is presented along with a set of recommendations on how to implement the EGF in concrete terms. DC4EU EGF should be considered as a document that will evolve continuously throughout the lifecycle of the project. A set of follow-up actions is identified at the end of the document to further improve the scope and depth of the EGF. Examples of these actions include e.g.

- Expanding the study to social security sector and to additional cross-border data exchange initiatives.
- Expanding the study to additional Member States with varying level of maturity in education and professional qualifications, or social security sector digitalisation.
- Establishing a maintainable and discoverable register of control documents.

1.4 DC4EU ECOSYSTEM GOVERNANCE FRAMEWORK CONTROL DOCUMENTS

DC4EU EGF is part of a hierarchical governance structure. The control documents will consist of a set of foundational governance rules and policies along with their sector-specific counterparts. As such, DC4EU EGF will define the appropriate procedures for governance precedence, including recommendations how conflicts, overlaps, and gaps are addressed and managed.

In order to advance interoperability across ecosystem partners, the DC4EU EGF will provide a register of control documents to cover at least the following aspects of ecosystem governance:

- Privacy and data protection, including personal data processing, release and retention, and data minimisation
- Information security
- Semantic and technical interoperability
- Trusted lists of governing authorities
- Use case specific trust registries
- Attribute and schema registries
- Revocation registries

The proposed hierarchical governance structure along with the recommendations for establishing the DC4EU consortium EGF are covered in detail in section 5.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

2. CURRENT STATE OF EDUCATION AND PROFESSIONAL QUALIFICATIONS SECTOR GOVERNANCE

In the context of DC4EU consortium piloting, the education and professional qualifications use cases currently suffer from the fragmentation of governing rules and policies across Member States (MS). Additionally, there is a number of pre-existing cross-border data sharing initiatives each with their own governance rules and guidelines. In order to build an effective ecosystem for education and professional qualifications data sharing, there must be a process how to incorporate the existing data sharing governance rules and procedures into a common DC4EU Ecosystem Governance Framework (EGF).

This section first studies the current state of education and professional qualifications data governance in couple of exemplary Member States (Finland, Norway, and Poland). It is followed by a study of an existing cross-border data sharing initiatives (EMREX and EWP) and their governance structures. Having an overview of the existing MS- and data-sharing-initiative-level governance structures allows us to incorporate these into a coherent DC4EU EGF. This makes it possible e.g. for other MSs or data sharing initiatives to easily adopt the DC4EU EGF.

The current state analysis about the Member States and cross-border data sharing initiatives is based on a questionnaire that was sent to DC4EU consortium partners during June-September 2023. The answers to the questionnaire were collected to the DC4EU consortium workspace and were assessed as part of the WP8 delivery.

2.1 GENERAL OVERVIEW OF EDUCATION SECTOR AND PROFESSIONAL QUALIFICATIONS GOVERNANCE

Based on the study, most Member States are hosting or planning to host a central national register for national education data. There are differences between Member States whether the central register hosts the official degree certificates in a signed or sealed format, or only the machine-readable data. Throughout MSs, it is the responsibility of the educational institutions to populate the data in the central registries. National legislation is in place in the studied Member States to define the governance of the central registers, which have the necessary authority to attest education- and professional qualifications-related information. Additionally, the studied Member States have ensured alignment with the relevant data protection regulations (GDPR [10] especially).

The studied Member States have implemented the EU Directive 2005/36/EC [1] in their national legislations to accept professional qualifications issued in other EU Member States. There are not, however, any centralised registers for professional qualifications and as such, the professional qualifications are managed in various sector-specific registries.

The three studied Member States have higher educational institutions who take part in the EMREX [8] data sharing initiative. Throughout the Member States, it has been defined as the responsibility of individual educational institutions to determine whether they should be part of the initiative.

2.2 GOVERNANCE STATUS IN MEMBER STATES

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

The study of existing Member State governance frameworks focused on national registries and legislation, data models used, and date protection and retention guidelines. This section provides an overview of the situation in three Member States: Finland, Norway, and Poland.

2.2.1 Finland

National registries and legislation

Finland hosts three national education-related registries (VIRTA [2], Koski [3], and the matriculation examination register) that contain information about education on a national level. The registries cover all educational levels and contain the information in machine-readable format. National registries do not contain official degree certificates, and the data does not contain qualified signatures of seals. The integrity of the data is based on the Act on the National Registers of Education Records, Qualifications and Degrees (884/2017) [4].

VIRTA is managed by a steering group consisting of representatives from the Ministry of Education and Culture, and representatives from higher education institutions. The national Koski register is governed Finnish Agency for Education.

Awarding professional qualifications and managing data on professional qualifications is divided between several public authorities. These authorities manage their own registers and there is no centralised register for professional qualifications. Directive 2005/36/EC [1] on the recognition of professional qualifications has been applied to national legislation 1384/2015 Act on the Recognition of Professional Qualifications [5].

Data Models

The governing national bodies of national registers (Finnish Agency for Education, Ministry of Education, and CSC – IT Center for Science) define and issue decrees on the data model and the data that is to be transferred to the national registries. The data model for the Koski register is defined by the Finnish Agency for Education in collaboration with educational institutions.

As a Member State participating in the Bologna Process [6], all higher education institutions in Finland issue the diploma supplement automatically for higher education diplomas. Vocational institutions are obliged to issue a Europass diploma supplement [7] on vocational diplomas only when the student requests it.

Higher education institutions can individually decide to join EMREX [8]. In Finland, the EMREX network is powered by CSC – IT Center for Science. Some individual educational institutions are also issuing European Digital Credentials for learning (EDCs) in Europass [9]. There are no common practices between educational institutions and each institution can independently decide to join Europass and issue EDCs.

Data Protection and Retention

In the case of VIRTA and Koski, the legislation states that educational institutions and the national governing bodies act as co-registrars. The responsibilities of each co-registrar are defined in act 884/2017 [4]. Educational institutions are responsible for the accuracy and rectification of data as defined in the General Data Protection Regulation [10]. National governing bodies are responsible for the other GDPR obligations.

Data transfers are mostly centralised to Koski service by act 884/2017 [4]. Finnish National Agency for Education is responsible for data sharing agreements and creating APIs to third parties.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

2.2.2 Norway

National Registries and Legislation

Norwegian formal education is, with few exceptions, subject to the Ministry of Education and Research. There are separate laws for the different levels of education, all these include legislation on how to handle storage and citizens' access to their education and professional qualifications in a life-long perspective.

A Norwegian Education and Accreditation registry is under development and planned to be published in 2024. This solution will include proof of formal recognition of institutions and their education, along with the ability to verify the publisher of digital results and diplomas from education.

Sikt - Norwegian Agency for Shared Services in Education and Research – develops and runs these services for storage, access, and sharing of results from education.

Data Models

All data exchange for credentials currently follows the EMREX protocol [8]. Diploma Supplement follows the Diploma data model from higher education [7]. This has been included as standard in the Student Information System(s) and is part of the production of the Diploma itself.

The number of ECTS credits is implemented in the data exchange via EMREX/ELMO. All results from higher education (courses and qualifications) include ECTS credits, together with the level of study.

There are discussions on strategy level on how to build national common services for micro-credentials especially to ensure this data in a life-long perspective.

Data Protection and Retention

All results from higher education are available for Norwegian citizens, for sharing with any third parties, both public and private sector. For upper secondary school, the diplomas are also available as structured data.

2.2.3 Poland

National Registries and Legislation

In Poland, there is one national registry that contains information on higher education. The national registry does not contain official degree certificates, and the scope of collected data is based on the Act of 20th July 2018 - Law on Higher Education and Science [11]. The register contains basic information about studies and degrees without study transcripts. It covers first and second-degree studies as well as doctoral studies.

The rules for recognition of professional qualifications acquired in the Member States are governed by Directive 2005/36/EC [1], implemented into the Polish legal system by the Act of 22 December 2015 on the rules governing recognition of professional qualifications acquired in the Member States of the European Union (Journal of Laws of 2016, item 65) [12], and by amending some acts governing issues related to professions.

Data Models

A paper diploma is mandatory and issued by all universities, however some universities issue an additional electronic diploma as a PDF file, that is signed by a qualified electronic seal and

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

by a rector's qualified electronic signature. A digital version of the diploma is not recognised by the public administration in Poland. This kind of document is not currently legally regulated. The minimum scope of attributes, that should be included in the diploma and the diploma supplement, is defined by law. On the diploma and supplement it is allowed to include more information than the legal minimum.

Poland conforms to the guidelines from the Bologna Process [6] in European higher education. The Polish structure of studies has been successfully implemented together with the European Credit Transfer and Accumulation System (ECTS).

Additionally, several Polish higher education institutions have joined EMREX [8].

Data Protection and Retention

Act of 20th July 2018 - Law on Higher Education and Science [11] is in compliance with the provisions of GDPR [10]. The Polish Ministry of Education and Science has been working on amendments to the polish law related to the diploma. There is an idea to create a centralised registry of diplomas that will be responsible for generating digital credentials. Each university will be responsible for registering diplomas in the centralised system.

2.3 GOVERNANCE OF EXISTING CROSS-BORDER DATA SHARING INITIATIVES

The study of existing cross-border data sharing initiative governance frameworks focuses on the governance models, data models, and technical standards that are defined by the initiatives. The study currently covers the EMREX data sharing intiative.

2.3.1 EMREX

EMREX [8] as a data exchange solution aims to offer individuals control over their own student data and how it is used in cross-border setup for various use cases. EMREX is a network of data repositories where the owner of the data (the individual) has access to their qualifications and proofs of competence. The network is open for any organisation to consume data, so that the data owners themselves are in control of the sharing of their own information.

EMREX uses the ELMO Data format for student data exchange, which is based on a CEN 15981:2011 standard model. EMREX also defines a set of technical standards that need to be met in order to take part in the network. Additional technical definitions include:

- EMC – EMREX Contact Point: Official sources with data about proof of results and other proofs of competence. To be an EMC in the network, you must be approved by the EMREX Executive Committee. The official list of EMC's is part of the EWP registry.
- EMP – EMREX Client: Services that consume data from the EMREX network. The network is open for any client to connect, but it is the owner of the results (the individuals) that delivers the data to these clients.

EMREX governance consists of following bodies:

- EMREX User Group: The group of organisations that participates in building the network.
- EMREX Executive Committee: The group of people handling the day-to-day activities in the network.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

- Data Providers: Official data sources with qualifications/proof of competence.
- Data Consumers: The consumer of data (any private of public organisation).
- Data Owners: The users that get access to their own data, for sharing these with a consumer.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

3. EBSI

The European Blockchain Services Infrastructure (EBSI) is a European Union (EU) initiative aimed at developing a secure and trusted blockchain infrastructure to support various public services and cross-border digital interactions within the European Single Market. EBSI is part of the broader European Blockchain Strategy, which seeks to harness the potential of blockchain technology for enhancing transparency, security, and efficiency in various sectors.

3.1 EBSI GOVERNANCE MODEL

European Blockchain Services Infrastructure (EBSI) is governed by EBSIC-EDIC whose role is to establish and operate an infrastructure for delivering EU-wide cross-border services, in particular public services. As defined in the EBSIC-EDIC Draft Statues, a key objective of EBSI is to “enable the cross-border exchange of trusted and secure verifiable credentials and to contribute to the European Digital Identity framework” and also to “reinforce trust and cyber resilience in delivering those services”. EBSIC-EDIC hosts multiple governing bodies that are shown in below diagram:

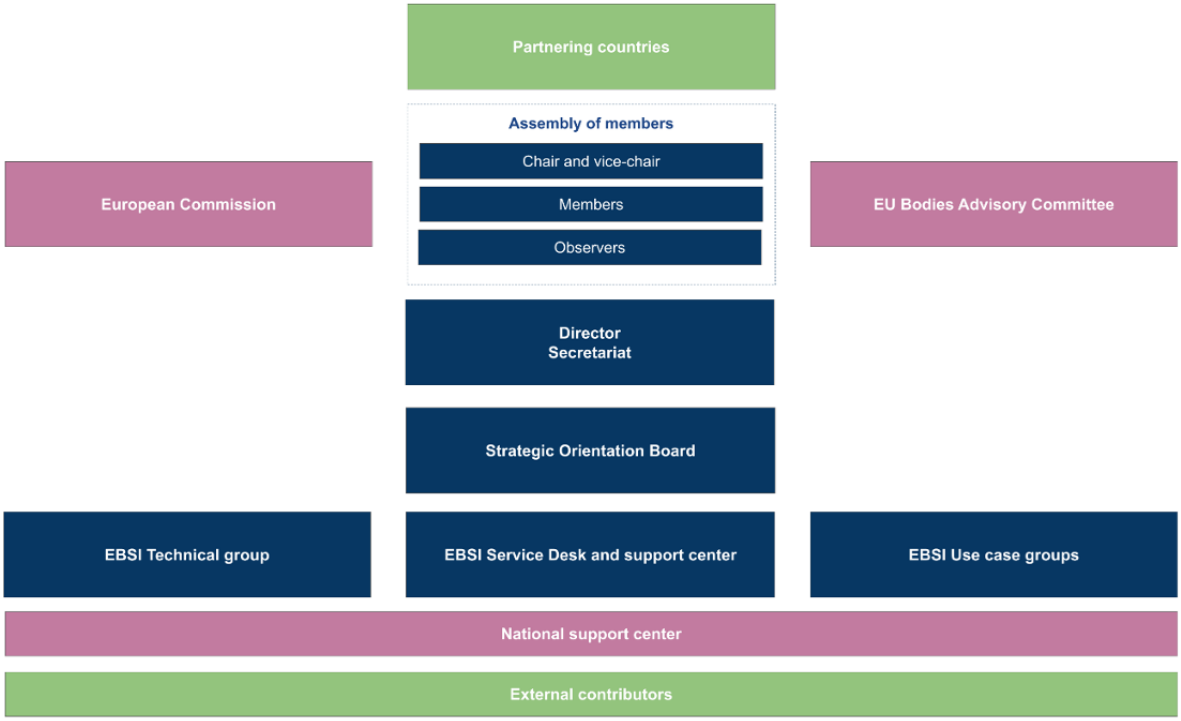

FIGURE 1 EBSIC-EDIC GOVERNANCE BODIES

Assembly of members is the supreme governing body of EBSIC-EDIC.

The Assembly of members appoints the Director of EBSIC-EDIC in accordance with a procedure adopted by the Assembly of members. The Director is the legal representative of EBSIC-EDIC. The Director carries out the day-to-day management of EBSIC-EDIC. The Director is also responsible for the implementation of the decisions made by the Assembly of members.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

The Strategic Orientation Board supports the Assembly of members and Director in the implementation of their tasks. The Strategic Orientation Board consists of the Director, representatives of the Assembly of members, representatives of the EBSI Technical Group, and representatives of the EBSI Use Case Groups appointed by the Assembly of members

EBSI Service Desk includes the support services provided for developing and deploying EBSI, as well as the support services to EBSI Node Operators and EBSI Application Service Providers.

EBSI Technical Group is the working group composed of technical experts, as appointed by the Assembly of members, who advises on the technical and operational aspects of the implementation of EBSI and its evolution.

EBSI Use Case Groups are working groups, dedicating their work to the technical specifications and first implementations of specific EBSI Use Cases.

EBSI may also host members either in EBSI Application Service Provider or in EBSI Node Operator roles:

- EBSI Application Service Providers means a natural or a legal person who provides one or more services to End Users using an EBSI Network, for instance by operating a digital wallet provided as a service, providing, or making available a digital wallet that is implemented as a mobile app, issuing digital credentials, or requesting digital presentations, and has submitted to and signed the EBSI Application Service Provider General Conditions.
- EBSI Node Operator means a public or private entity which has been approved by an EBP Member of its jurisdiction to host and operate an EBSI Node and has submitted to and signed the EBSI Node Operator General Conditions detailing the legal, technical and governance requirements for the EBSI Node Operators.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

4. TRUST OVER IP GOVERNANCE METAMODEL

DC4EU WP8 has chosen the Trust Over IP Governance Metamodel as the basis for its EGF. This section provides an overview of the Trust Over IP organisation and its metamodel. Finally, the section describes how the ToIP metamodel is adapted so that it is more suitable to be used as a basis for the ecosystem governance of the DC4EU education and professional qualifications, and social security use cases.

4.1 TRUST OVER IP

Trust over IP (ToIP) Foundation [13] is a non-profit organisation, operating under the auspices of Linux Foundation. Trust over IP is an open development organisation, comprising of public and private member organizations and individuals. ToIP Foundation develops tools and specifications to help communities of any size use digital networks to build and strengthen trust between participants. ToIP Foundation has over 300 organisational and 140 individual members from around the world, who work together in Working Groups and Task Forces to create architectures, component specifications, and interoperability definitions for the technical and governance layers.

Trust over IP aims to define a complete architecture for internet-scale digital trust that combines cryptographic assurance at the machine layer with human accountability at the business, legal, and social layers. It is an initiative focused on establishing a global framework for trusted and secure digital interactions. It emphasises decentralised identity management, verifiable credentials, and agent-to-agent communication to enhance trust, privacy, and interoperability in the digital ecosystem.

ToIP envisions a world where individuals have control over their digital identities and can securely share verifiable credentials across various domains. It promotes the use of decentralised identifiers (DIDs) and verifiable credentials, creating a foundation for secure and privacy-preserving interactions in sectors like education and social security.

The name “Trust over IP” comes from the vision of a “trust layer” for the Internet that could be achieved by following the same architecture as the Internet itself: each peer running an instance of a standard “stack” of protocols just as each device on the Internet runs an instance of the TCP/IP stack.

4.2 TOIP METAMODEL OVERVIEW

One of the most recognised deliverables from ToIP is the dual-stack metamodel that describes the conceptual four layers generally present in decentralised digital trust ecosystems. DC4EU WP8 has chosen the ToIP metamodel as the basis to define the DC4EU consortium EGF.

The Trust over IP metamodel shows two vertical stacks, one denoting technology and the other governance topics. Both stacks are divided to four layers that describe the different conceptual layers. Each layer solves a specific set of problems required to support the higher layers.

Layer 1 is for the public utilities that are needed to look up and verify the issuers of digital credentials (such as EAAs). In public/private key infrastructure, these cryptographic “starting

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union’s Digital Europe Programme under Grant Agreement no. 101102611

points" are called *roots of trust* or *trust anchors*. This layer may also include other common components that all ecosystems need when performing trust interactions.

Layer 2 describes the systems, such as digital identity wallets, needed by individuals, organisations, and digital "things" (or the digital twins of non-digital things) in order to accept, store, and exchange digital credentials or attestations over commonly agreed protocols. The layer title 'peer-to-peer communication' is a broad term and includes multiple ways for interactions between two or more peers. In the simplest sense, this layer describes the technical interaction between the technical endpoint systems.

Layer 3 is for the trust task protocols, such as the verifiable credential exchange trust triangle (consisting of *issuers*, *holders*, and *verifiers*). Trust tasks are a general term for different types of trust interactions between parties, such as the credential exchange, education institution validation, personal authentication, presentation of professional qualifications, etc.

Layer 4 is for the ecosystems adopting the decentralized digital trust infrastructure. Ecosystems define the roles, data models, and processes needed to utilise the three lower layers. In the context of DC4EU, some of these are defined in the revised eIDAS regulation and its controlling documents (e.g. ARF [14]). Also, this layer will include most of the use case specific requirements that are applied on top of the base eIDAS requirements.

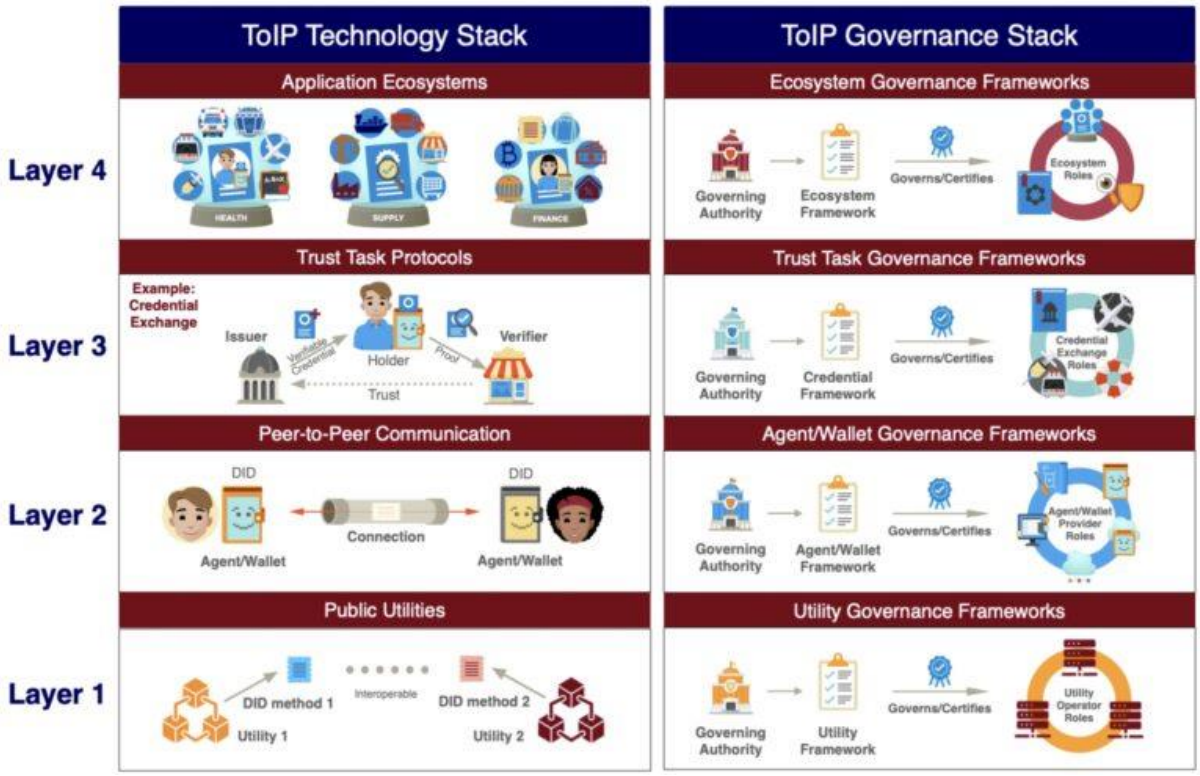

FIGURE 2 THE TRUST OVER IP METAMODEL

The ToIP metamodel is useful in clarifying how different implementation and governance layers are stacked to form a coherent big picture of the ecosystem.

For example, in DC4EU, the ecosystem consists of multiple layers that all have an impact for the different elements and parties in the ecosystem. General EU regulations, eIDAS and ARF, use cases (education and professional qualifications, and social security), and Member State policies will all affect the implementation done by public and private entities in the ecosystem.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

The governance layers and their impact to the implementation is mapped using the Trust over IP metamodel. This enhances understanding of the interoperability requirements for each use case ecosystem and implementing parties having different roles.

4.3 USING TOIP FOR MAPPING LAYERED GOVERNANCE STRUCTURES

Any ecosystem with decentralised governance structure can be thought as consisting of layers stacked on top of each other. Each layer builds its own governance on top of the lower layers, detailing and enhancing the requirements set to its applicable layers.

The bottom layers, having the widest coverage are usually regulations, directives, or policies that set higher-level principles and general requirements, affecting all parties and systems in the ecosystem. Accordingly, the top-most layers define the most detailed, use case-related requirements that affect only the selected scope, specific roles or data objects.

FIGURE 3 DC4EU STACKED GOVERNANCE MODEL

This is the case also in the EUDI wallet ecosystem, where EU-wide regulations, Member State policies and laws, and use case governance all define their own layers of governance that function together as a whole.

Mapping the EUDI wallet ecosystem with this layered governance dimensions to Trust over IP requires some restructuring of the ToIP metamodel. The current ToIP metamodel defines the layers in a way that doesn't allow for comprehensive view of the whole governance ecosystem. For this purpose, DC4EU WP8 has chosen to create a modified version of the Trust over IP metamodel to represent the EUDI wallet ecosystem and its various layers more accurately.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

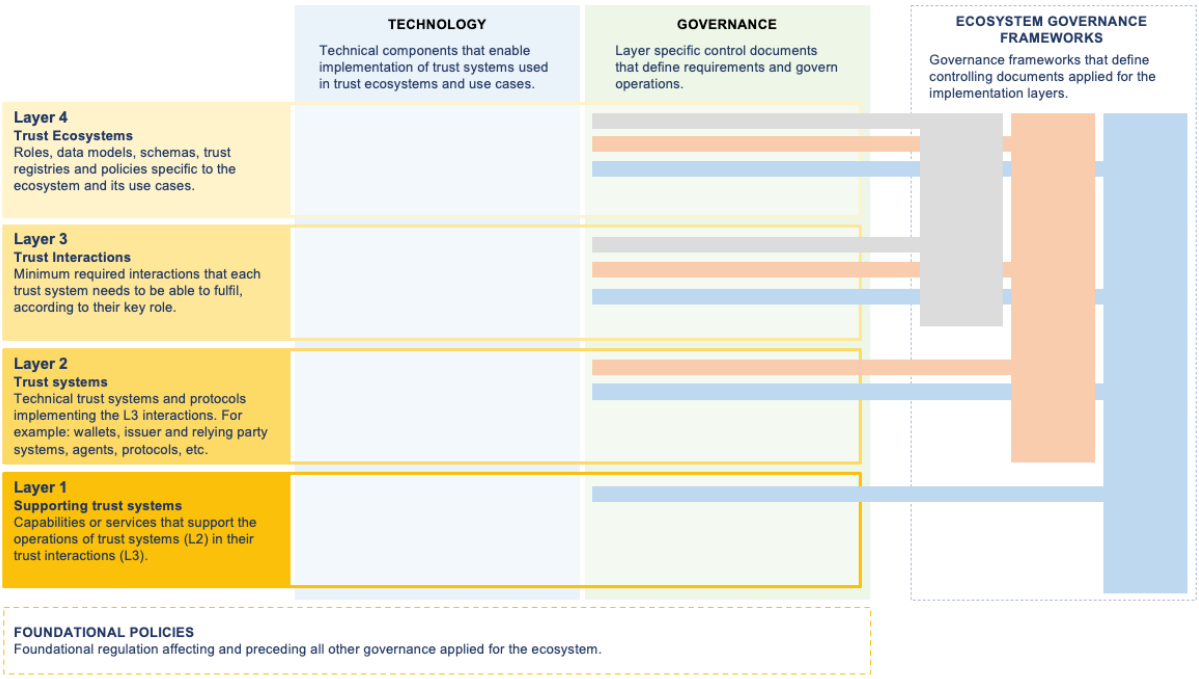

FIGURE 4 MODIFIED DC4EU GOVERNANCE METAMODEL BASED ON TOIP

The new proposed model enhances the original model in three ways:

1. Redefines the Trust over IP metamodel layers more specifically in how they are implemented in the EUDI wallet ecosystem, while retaining the core meaning of the layers.

2. Introduces a new layer: Foundational policies. This layer describes regulations and policies that are applied to all layers, roles, and use cases implementing EUDI wallet use cases.

3. Introduces a new section: Ecosystem Governance Frameworks. It is a visual tool for describing the governance frameworks that define the layer-specific controlling documents. This helps understanding the scope of each governance framework (or entity) and what kind of control documents are used to govern the layers.

DC4EU WP8 will use this model to define the high-level technology and business architecture, and map the various governance frameworks to each layer. Mapping the frameworks creates a holistic view on the various governance structures in place for the EUDI wallet ecosystems.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

5. PROPOSAL ON DC4EU GOVERNANCE FRAMEWORK STRUCTURE

This section provides an overview of a proposal about DC4EU consortium piloting ecosystem governance. It describes a layered governance model along with an approach how to map EUDI wallet ecosystem governance structures to the enhanced ToIP metamodel. Finally, it provides an overview of the education- and professional qualifications-specific EGF that will be applied to DC4EU consortium piloting. Similar model will be created also for social security in subsequent versions of this document.

5.1 GOVERNANCE STRUCTURE

The EUDI wallet ecosystem governance can be described using a three-layer governance structure that consists of *foundational governance*, *technical governance*, and *use case governance*. Each of these layers are focused on different aspects of the trust ecosystem, building on top of the structures created by the other layers.

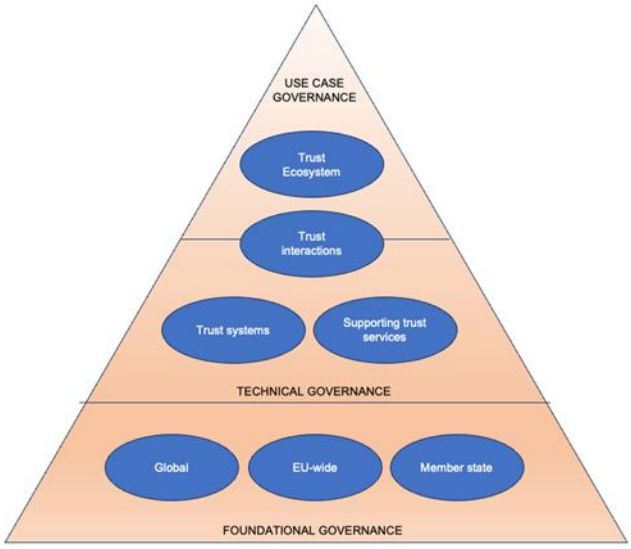

FIGURE 5 EUDI WALLET ECOSYSTEM GOVERNANCE STRUCTURE

Foundational governance represents the constitutional documents that have an effect on all technical systems and use cases above it. They provide the foundation, which enables effective definition of key capabilities in the higher layers.

Technical governance focuses on the common governance that is applicable to all ecosystems and use cases using the technical capabilities. The main goal of the technical governance is to assert common rules, standards, and specifications that enable the ecosystems to be interoperable without needing to create any non-ecosystem-related common technical governance. The technical governance layers should provide only common components that are applicable to all ecosystems.

Use case governance focuses only on the special requirements that the ecosystem use cases have for the implementation. While ecosystems should understand the requirements of the

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

implementation and trust model (e.g. wallets), they should be built agnostic to the implementing infrastructure. It is especially important for interoperability, that the ecosystem governance does not create mechanisms that create exceptions or overlap with the technical governance. Instead, technical governance should be adapted to support various ecosystem requirements.

5.2 MAPPING THE EUDI WALLET ECOSYSTEM GOVERNANCE STRUCTURES TO THE ENHANCED TOIP METAMODEL

To capture the various governance frameworks and controlling documents in use for EUDI wallet ecosystems, and for understanding their scope and potential overlaps, a new *governance structure mapping tool* was created. The spreadsheet displays the Trust over IP model layering with subtopics relevant for EUDI (e.g. from ARF [14] and other sources) on the vertical columns. The relevant governance frameworks and controlling documents are listed in the horizontal rows. For each row, the affected subtopics within the layers are crossed, creating a clear diagram showing potential overlaps or gaps.

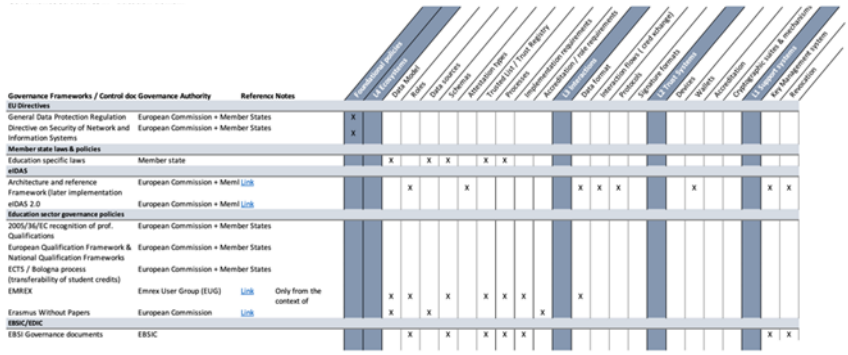

FIGURE 6 EXAMPLE OF THE GOVERNANCE STRUCTURE MAPPING TOOL SPREADSHEET

The tool is useful for many purposes. It can be used to present a big picture on the governance; help new ecosystems to onboard and map their ecosystem governance, or by Member States to map their national policies to the EU-wide scheme.

5.3 EDUCATION AND PROFESSIONAL QUALIFICATIONS GOVERNANCE LAYERS

Using the modified Trust over IP metamodel presented in section 4.3 and the governance mapping tool presented in section 5.2, we are able to detail the high-level governance structure into the relevant foundational policies and governance frameworks, and assign controlling documents to applicable layers. The visualisation makes it possible to easily view the governance frameworks and foundational policies that are applicable for the EUDI Education and Professional Qualifications ecosystem.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

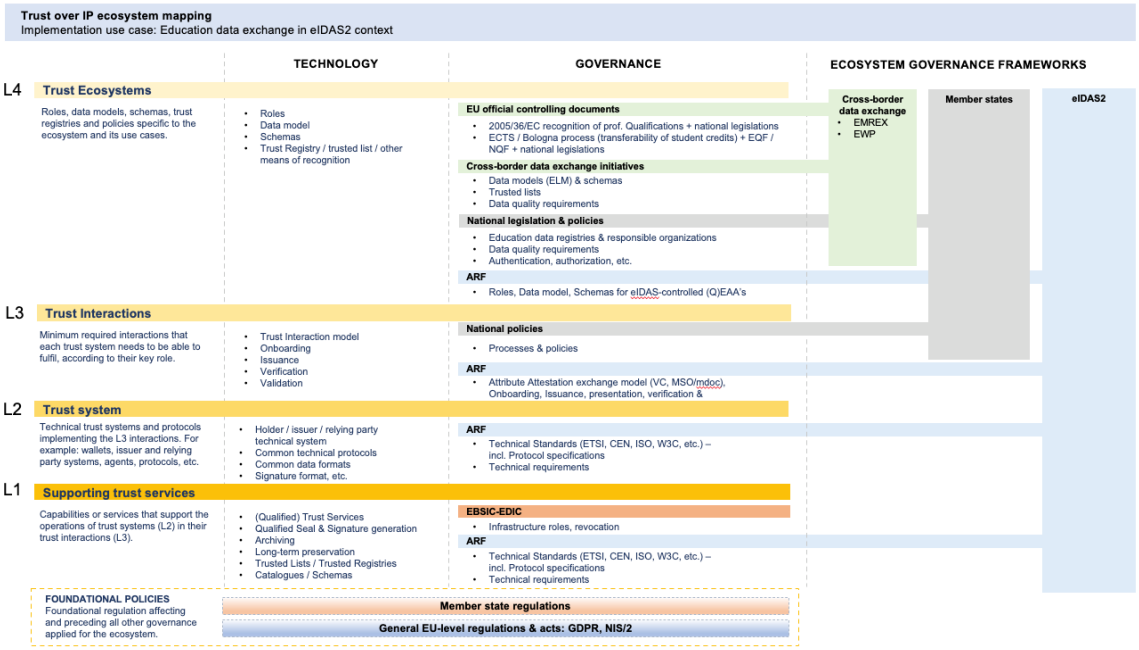

FIGURE 7 EDUCATION AND PROFESSIONAL QUALIFICATIONS GOVERNANCE STRUCTURE VISUALISATION.

5.3.1 Foundational Policies

The foundational policies that affect all EUDI wallet ecosystems are the EU-level regulations and acts, especially General Data Protection Regulation (GDPR) [10], and the Directive on Security of Network and Information Systems (the NIS Directive, or NIS/2) [15]. Other similar acts may also be prevalent in the near future, that have strong relevance, such as the Data Act [16], including DSA [17], DMA [18], and DGA [19]. Foundational policies also include each Member States own general policies.

5.3.2 Supporting Trust Services

Supporting trust services include governance from the revised eIDAS regulation, as well as the EBSI-infrastructure governance described in section 3.1. As the supporting trust services may include multiple Qualified Trust Service Provider (QTSP)-provided services (e.g. Qualified Seals and Signatures, archiving, Trusted Lists, etc), the governance will include also a long list of technical requirements, implementation guides, and other similar governing documents.

5.3.3 Trust Systems

Trust systems in the EUDI wallet ecosystem are mainly controlled by ARF [14] (and later on by the Implementing and Delegating acts of the revised eIDAS regulation), as the active endpoint systems are defined in those documents. Interfaces to other potential trust systems (e.g. dataspace systems, IoT-devices, etc.) may be relevant in the future, but initially the trust systems are defined in ARF.

5.3.4 Trust Interactions

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

Trust interactions have overlap from the base descriptions provided in ARF [14], as well as some policies from Member States or ecosystem initiatives.

5.3.5 Trust Ecosystems

The trust ecosystem governance has the most overlap, since all ecosystems, including the base EUDI wallet ecosystem (as defined in ARF [14]) capabilities also define roles, and data models. These are generally supplemented by the member-state specific processes, data models, and requirements from domain ecosystems, as well as additional policies that affect only specific ecosystem implementations in EU or within Member States.

In education and professional qualifications domain, the complexity of the ecosystems is apparent in this layer, as it is populated by multiple governance frameworks, each including their own flavor, with potential for overlaps and conflicts.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

CONCLUSIONS

The study has shown that it is possible to use an enhanced version of the ToIP metamodel to come up with an ecosystem governance framework which can be used as a tool help Member States, implementers, evaluators, and domain ecosystems to evaluate their governance structures against other frameworks in the EUDI wallet ecosystem. The implemented tools will be further enhanced in the DC4EU piloting project to make them more useful in identifying the interfaces, overlaps and gaps, when designing ecosystems within EUDI.

This document describes the first iteration of an EGF definition for DC4EU consortium piloting and will be further developed during the project lifecycle. Identified actions to further improve the coverage of the EGF are at least:

- Extend the study from education and professional qualifications to social security.
- Include more Member States and their governance frameworks to the study.
- Engage DC4EU consortium piloting partners to review and extend the governance structure mappings described in sections 6.2 and 6.3.
- Create a discoverable register of EGF control documents.

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

REFERENCES

[1] Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0036

[2] VIRTA-opintotietopalvelu, https://wiki.eduuni.fi/display/CSCVIRTA/VIRTA-opintotietopalvelu

[3] Koski-tietovaranto, https://www.oph.fi/fi/palvelut/koski-tietovaranto

[4] Finnish Act on the National Registers of Education Records, Qualifications and Degrees, https://www.finlex.fi/en/laki/kaannokset/2017/en20170884

[5] Finnish Act on the Recognition of Professional Qualifications, https://www.finlex.fi/fi/laki/kaannokset/2015/en20151384.pdf

[6] The Bologna Process and the European Higher Education Area, https://education.ec.europa.eu/education-levels/higher-education/inclusive-and-connected-higher-education/bologna-process

[7] The Diploma Supplement, https://europa.eu/europass/en/learn-europe/diploma-supplement

[8] EMREX, https://emrex.eu/

[9] European Digital Credentials for learning, https://europa.eu/europass/en/europass-alati/european-digital-credentials

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[11] Act of 20 July 2018, The Law on Higher Education and Science, https://www.gov.pl/attachment/d6975935-4b24-4be3-96f1-09c51589958a

[12] Recognition of professional qualifications, https://prk.men.gov.pl/en/9en/

[13] Trust Over IP Foundation, https://trustoverip.org/

[14] The European Digital Identity Wallet Architecture and Reference Framework, https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

[15] Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive), https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

[16] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

[17] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[18] 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 (Digital Markets Act), https://eur-lex.europa.eu/eli/reg/2022/1925

[19] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020PC0767

[20] ToIP Governance Architecture Specification, https://trustoverip.org/permalink/ToIP-Governance-Architecture-Specification-V1.0-2021-12-21.pdf

[21] ToIP Governance Metamodel Specification, https://trustoverip.org/permalink/ToIP-Governance-Metamodel-Specification-V1.0-2021-12-21.pdf

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611

[22] ToIP Governance Metamodel Specification Companion Guide, https://trustoverip.org/permalink/ToIP-Governance-Metamodel-Specification-Companion-Guide-V1.0-2021-12-21.pdf

Co-funded by the European Union

The DC4EU project is Co-funded by the European Union's Digital Europe Programme under Grant Agreement no. 101102611