Co-funded by
the European Union

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

6.1 Business Blueprint (BBP)

Revision: v.2.1

Work package	WP 6
Task	6.1. Business Blueprint
Submission date	24/05/2024
Deliverable lead	DVSV
Version	2.1
Authors	DVSV, DRV Bund, STAR
Reviewers	WP 6 Partners DC4EU Work Package Leaders

Abstract	This document proposes the business requirements, scenarios, and interoperability requirements as well as use case governance model design. The Business Blueprint provides a roadmap for the successful implementation of the large-scale pilots in social security coordination.
Keywords	DC4EU, CI, EAA, EESSI, EHIC, eID, eIDAS, EUDIW, EUDIW Toolbox, ID, IR, Issuer, LoA, LSP, PD A1, PID, PRC, QR, SPOC, TSP, VC, Verifier, VP

Document Revision History

Version	Date	Description of change	List of contributors
V1.0	31/01/2024	1st version of the deliverable for comments	WP6 partners
V2.0	29/03/2024	2nd version of the deliverable for comments	DC4EU consortium

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

DISCLAIMER

The information, documentation and figures available in this deliverable are written by the "Digital Credentials For Europe" (DC4EU) project's consortium under the EU's Digital Europe Programme under Grant Agreement no. 101102611 and do not necessarily reflect the views of the European Commission.

The European Commission is not liable for any use that may be made of the information contained herein.

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

The **DC4EU Social Security project** aims to facilitate EU social security systems by introducing universally applicable digital and decentralised frameworks for the issuance and authentication of entitlement documents.

The **project's objective** is to develop a secure and reliable digital architecture for the issuance, revocation, and verification of Electronic Attestations of Attributes (EAA), or "Digital Credentials", utilising the European Digital Identity (EUDI) Architecture, including the European Digital Identity Wallet (EUDIW).

Verifiable Credentials (VCs) are an important pillar of this architecture. They represent information found in physical credentials, as well as innovations that have no physical equivalent, such as authorised possession of credentials. In the context of social security, VCs represent statements made by an authentic source about a subject in a tamper-evident and privacy-respecting manner. VCs can be used to build Verifiable Presentations (VPs), which can also be cryptographically verified.

The **target system** for social security coordination in DC4EU described in this document is an integrated digital system designed to eliminate any media breaks. It aims to address fraud and errors, comply with social security requirements, increase acceptance among all relying parties, and ensure citizens' right to free movement. The core business use case of this system involves the digital verification process, coupled with proof of correct attestation usage during verification. A positive result from this process will authorize access to social security benefits and services. It's important to note that any complementary system relying on traditional paper or plastic card-based entitlement documents—intended for citizens who do not use the digital identity architecture, is out of scope of this target system.

Large-Scale Pilots (LSPs) in social security will test the target system during various implementation phases of the EUDI wallet ecosystem. The primary objective is to assess the system's feasibility, effectiveness, and its potential impact on social security**.** The pilots are conducted in real-world settings to evaluate the system. The testing and pilot configuration will be specified in alignment with different phases of the ARF implementation. This alignment depends on the maturity of national and international implementations. During testing and piloting, simulation, and mock-ups of specific components—such as EUDI wallets, PID providers, and other trust services—will be necessary to achieve the objectives. Additionally, a combination of both simulated and real data will be used in the Large-Scale Pilot (LSP) for social security. The goal is to closely approximate the behaviour of the target system. All these configurations will be documented throughout the project in the Deliverable 6.2 "Deployment, Testing & Piloting Scenarios Results Library".

The adoption of the innovative technologies in the EUDIW ecosystem for social security requires a systematic approach. The basis for this approach is the detailed articulation of organisational and business prerequisites, as outlined in this document.

The present document defines business requirements, scenarios, interoperability requirements, and a use-case governance model design for the social security business cases implemented in the target system. It includes **Business Process Specifications** and **Data Model**, System Architecture, and Specifications of Configuration Processes, utilising Business Process Notation, Business Process Modelling, and Data Modelling instruments.

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 Business Blueprint will encompass several key components like a **status quo report**, **future business processes** for issuing, revoking, and verifying VCs, **data models** for **VCs**, and procedures for the registration and onboarding of various roles within the social security domain. This comprehensive document will serve as a foundational guide for modernising and streamlining social security processes in line with current regulatory frameworks and technological advancements.

The document is intended for the social security community, including policy makers, administrators, and service providers, as well as technical architects who will design and implement the EUDIW solution. The document provides a comprehensive business view of the EUDIW ecosystem in the context of social security, covering the following aspects:

- **Chapter 1** introduces the basic concepts and definitions of the EUDIW and explains the methodology and approach for drafting the business blueprint.
- **Chapter 2** presents the current situation and challenges of the two use cases that the DC4EU will address: PD A1 (Portable Document A1) and EHIC (European Health Insurance Card).
- **Chapter 3** defines the basic principles and requirements that guide the design and development of the EUDIW solution in the context of social security coordination.
- **Chapter 4** describes the conceptual architecture of the target system, including the main components, actors, and interfaces.
- **Chapter 5** illustrates the business scenarios and user journeys that demonstrate how the EUDIW ecosystem will work in practice.
- **Chapter 6** specifies the data models and standards that will ensure the interoperability and security of the EUDIW data.
- **Chapter 7** outlines the procedures and requirements for onboarding stakeholders who will participate in the EUDIW 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

CONTENT

1. INTRODUCTION 1

1.1. General 1
1.2. EUDIW Eco System 2
1.2.1. Technical Components 2
1.2.2. Service Providers 2
1.2.3. Authorising Bodies 3
1.2.4. Active Players 4
1.3. Rulebook 7
1.3.1. Governance and Operational Framework: 7
1.3.2. Technical Specifications: 7
1.3.3. Interoperability and Ecosystem Integration: 8
1.3.4. Quality Assurance and Trust Mechanisms: 8
1.4. Scope and Scenarios 8
1.5. PID as the Base Digital Identity 10
1.6. Business Blueprint for Social Security 11
1.7. Methodology 14

2. STATUS QUO ANALYSIS 15

2.1. Introduction 15
2.2. Participants and Return Rates 15
2.2.1. Participants 15
2.2.2. Return Rates 16
2.2.3. Coverage 18
2.3. Portable Document A1 (PD A1) 19
2.3.1. General 19
2.3.2. Issuance Process of the PD A1 22
2.3.3. Verification Process of the PD A1 24
2.3.4. Onboarding Use Cases for PD A1 27
2.4. European Health Insurance Card (EHIC) 29
2.4.1. General 29
2.4.2. Issuance Process of the EHIC & PRC 32
2.4.3. Verification Process of the EHIC & PRC 37
2.4.4. Onboarding Use Cases for EHIC 39

3. BASIC REQUIREMENTS 43

3.1. Introduction 43
3.2. General Principles 44
3.2.1. Data Minimisation 44
3.2.2. Self-Sovereignty 45
3.2.3. Non-Traceability 46
3.2.4. Data Protection 47
3.3. Personal Identity Data 48
3.4. Trust Framework 51
3.4.1. Relevant Roles 51
3.4.2. Relying Parties 52
3.4.3. Credential Issuers 52
3.4.4. Implementation Aspects 53
3.5. Secure Authentication, Credential Issuance, and Usage 53
3.6. Additional Requirements 55
3.6.1. Offline Usage 55
3.6.2. Revocation 55
3.6.3. Flexibility 56
3.6.4. Technical Neutrality 56
3.6.5. Other basic requirements not in scope 56
3.7. Conclusions for Social Security 57

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. CONCEPTUAL ARCHITECTURE 59

4.1. Introduction 59
4.2. Key Components 61
4.2.1. EUDI Wallet 61
4.2.2. Applications for Verification 61
4.2.3. Public Key Repositories 61
4.2.4. Trusted Registries 62
4.2.5. Issuing of Credentials 63
4.2.6. Requesting Credential Issuance 63
4.2.7. Presenting Credentials 64
4.2.8. Verifying Credentials 64
4.2.9. EUDIW Conceptual Data Model 65
4.2.10. Verifiable Credential (VC) 65
4.2.11. VC Ecosystem 66
4.2.12. Core Data Model 67
4.2.13. VC Building Blocks 68
4.2.14. VP Building Blocks 71
4.3. Validity 74

5. BUSINESS SCENARIOS AND USER JOURNEYS 76

5.1. Introduction 76
5.2. General Business Requirements for Social Security Coordination 77
5.3. Use Case 1: Onboarding of the EUDI Wallet 77
5.3.1. General Description 77
5.3.2. Prerequisites Related to the Use Case 78
5.3.3. Roles, Activities and Tasks 78
5.3.4. BPMN Diagram 79
5.3.5. High Level Requirements 79
5.4. Use Case 2: Issuance of Verifiable Credentials 80
5.4.1. General Description 80
5.4.2. Prerequisites Related to the Use Case 80
5.4.3. Roles, Activities and Tasks 81
5.4.4. BPMN Diagram 83
5.4.5. High Level Requirements 84
5.5. Use Case 3: Revocation of Credentials 85
5.5.1. General Description 85
5.5.2. Prerequisites Related to the Use Case 85
5.5.3. Roles, Activities and Tasks 86
5.5.4. BPMN Diagram 87
5.5.5. High Level Requirements 88
5.6. Use Case 4: Verification of Credentials and Identity 89
5.6.1. General Description 89
5.6.2. Prerequisites Related to the Use Case 89
5.6.3. Roles, Activities and Tasks 90
5.6.4. BPMN Diagram 91
5.6.5. High Level Requirements 92
5.7. Use Case 5: Delegation of Credentials 93
5.7.1. General Description 93
5.7.2. Subject Passes the Verifiable Credential to a Holder 93
5.7.3. High Level Requirements 94

6. PHYSICAL DATA MODEL 95

6.1. Introduction 95
6.2. Logical Data Model 96
6.3. Data Model for the PD A1 99
6.4. Data Model for the EHIC 100

7. ONBOARDING OF ACTORS 101

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

7.1. Introduction 101
7.2. EESSI Institution Repository – a Trust Framework for Social Security 101
7.3. EIDAS 2.0 Trust Framework 102
7.4. Onboarding Implementation 103
7.4.1. Onboarding Issuers 103
7.4.2. Onboarding Citizens 106
7.4.3. Onboarding Verifiers 106

8. LIST OF FIGURES 107

9. LIST OF TABLES 108

10. ABBREVIATIONS AND TERMS 109

11. REFERENCES 118

12. APPENDIX A – EXAMPLES OF THE DATA MODEL 121

13. APPENDIX B - REFERENCE ARCHITECTURE FOR THE INTEGRATION OF AN AUTHENTIC SOURCE 125

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

1.1. GENERAL

The **increased mobility** of citizens within the European Union (EU) poses significant **organisational and technical challenges** in protecting the **social security rights** of those exercising their right to free movement. As individuals relocate within the EU — whether changing their residence or workplace — they are assured the **same rights and obligations** as the nationals of the host country. The EU has implemented **uniform regulations** to safeguard the social security entitlements of individuals moving throughout its member states (MSs), including the **27 EU countries**, as well as **Iceland, Liechtenstein, Norway, Switzerland, and the United Kingdom**. These measures are essential for upholding a just and unified system that supports the EU's core principle of **free movement for European citizens**.

To verify and protect the rights of EU citizens during changes in residence or workplace, various **social security documents and forms** are issued to citizens at the national level. These documents are mainly provided in paper format and serve as proof of entitlement to social security benefits across MSs, the current system faces several practical challenges:

- The revocation and update processes are notably inefficient or may not even exist.
- Paper-based documents are susceptible to fraud and error.
- The current issuance process (plastic card EHIC & paper PD A1) is both excessively expensive and environmentally unsustainable.
- The issuance and verification procedures lack flexibility, both temporally and geographically.
- The verification process is complex, time-consuming, and prone to errors.

These challenges underscore the urgent need for a more **streamlined and secure system** that supports the mobility of EU citizens while preserving their social security rights. A significant advancement in social security is the transition to **digital and decentralised methods** for managing entitlement documents — including issuance, verification, and revocation. This contemporary approach:

- Ensures smooth and protected access to entitlement verifications.
- Grants local authorities the independence to manage their operations, in accordance with a unified European framework.
- Enhances transparency and efficiency in the creation and verification of social security documents.
- Implements a common framework for digital identity management in the single digital market.

The overarching goal for DC4EU Social Security is to design and implement a **sustainable, reliable, and secure technical and business architecture** for the issuance, updating, revocation, and verification of **electronic attestations of attributes (EAA)**, also referred to as "Digital Credentials," within the social security coordination context.

This solution will utilise the **EUDIW Toolbox**, which encompasses the **European Digital Identity Wallet (EUDIW)**. **Large-Scale Pilots** will be carried out in a **pre-production environment**. Furthermore, DC4EU WP 6 will contribute significantly to the development of the EUDI Reference Wallet's capabilities, thus facilitating the implementation of a EUDIW in MSs, with a special emphasis on the social security domain.

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

1.2. EUDIW ECO SYSTEM

The European Union Digital Identity Wallet (EUDIW), a key component of the European Digital Identity Framework, is designed to provide a secure and user-friendly method for European citizens and businesses to utilise identity data necessary for accessing digital services.

Objectives: The EUDIW aims to foster a high level of trust in digital transactions across Europe. It can be used for a variety of digital services, to prove identity and to attest personal attributes in a cross-border context.

Actors of the Ecosystem: The ecosystem comprises supporting organisations responsible for issuing and verifying attributes, as well as facilitating the exchange of credentials. These entities serve as the backbone of the wallet's operation, ensuring its smooth and secure functioning.

Functional and Non-Functional Requirements: The wallet has specific functional and non-functional requirements to ensure its safety, interoperability, and user-friendliness.

Potential Building Blocks: The EUDIW is constructed with a set of potential building blocks that form the technical backbone of all future EUDIWs.

EUDIW Toolbox: A common EU Toolbox for implementing the EUDIW will be developed by the European Commission (EC). The toolbox serves as the foundation for engineering a prototype EUDIW that can be tested in several Large-Scale Pilots.

Below is a list of all the key players in the EUDIW ecosystem, each playing a crucial role in the functioning and security of the EUDIW. They work together to provide a secure and efficient system for digital identification and attestation of attributes. Please note that the roles and responsibilities of these players may vary based on national laws and regulations, as well as EU regulations for certain business domains (e.g., social security coordination):

1.2.1. Technical Components

Device Manufacturers: Device Manufacturers are actively developing products that incorporate integrated wallet solutions, aiming to enhance the user experience.

1.2.2. Service Providers

Person Identification Data (PID) Providers: These are trusted entities responsible for verifying the identity of EUDIW holders and supplying secure PIDs to the EUDIW.

Qualified Electronic Attestation of Attributes (QEAAs) Providers: These providers are responsible for maintaining an interface that offers the requesting and delivery of secure QEAAs to users within their EUDIW. QEAAs are a secure method for issuing and verifying attributes of digital identities. These providers adhere to strict eIDAS requirements. QEAAs have the same legal effect as their paper counterparts, and cross-border recognition is guaranteed.

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

Electronic attestation of attributes providers by or on behalf of a public sector body responsible for an authentic source (EAAPSB): These providers are responsible for maintaining an interface that offers the requesting and delivery of secure EAAs to users within their EUDIW. These providers adhere to strict eIDAS requirements. EAAs issued by EAAPSBs meet the equivalent level of reliability and trustworthiness as QEAA providers, so they equate the same legal effect as their paper counterparts, and cross-border recognition is guaranteed.

Electronic Attestation of Attributes (EAAs) Providers: These providers are responsible for the secure exchange of electronic attributes within the EUDIW ecosystem. Public bodies such as the competent institutions (CIs) in social security have a special quality as EAA providers.

Qualified Trust Service Providers (QTSPs): QTSPs are entities that offer trust services in line with the eIDAS regulation. Their mission is to establish trust in digital transactions by providing reliable services. QTSPs adhere to strict eIDAS requirements and national supervisory bodies monitor their compliance.

Qualified and Non-Qualified Electronic Attestation of Attributes Schema Providers: These providers publish schemas and vocabularies describing the structure and semantics of Qualified and Non-Qualified Electronic Attestation of Attributes ((Q)EAAs). They may enable other entities such as Relying Parties to discover and validate (Q)EAAs.

Providers of registries of trust sources: Providers of registries of trusted sources are responsible for maintaining a list of trusted sources that can be used to verify the authenticity of the data provided by the PID providers.

1.2.3. Authorising Bodies

Authentic Sources: Authentic Sources refer to repositories or systems, recognised or mandated by law that contain information regarding natural or legal persons' attributes. EAAs issued by such an entity would automatically equate QEAAs with respect to authority.

EUDIW Providers: These are the entities that provide users with access to the wallet and its services. They ensure that all EUDIW components comply with the relevant legal and regulatory requirements in each MS.

Supervisory Bodies: These are entities notified to the EC by the MSs to supervise QTSPs and take action, if necessary, in relation to non-qualified Trust Service Providers.

National Accreditation Bodies: These bodies accredit Conformity Assessment Bodies (CABs) and ensure they meet the standards set by the European co-operation for accreditation.

Conformity Assessment Bodies (CABs): These are entities that assess and verify the conformity of products, services, and systems against the requirements of standards or

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

technical specifications. The EUDIW must be certified by accredited public or private bodies designated by MSs.

1.2.4. Active Players

EUDIW Users: Users, whether they are individuals or legal entities, actively engage with the EUDIW. They have the capability to securely store and share confidential electronic documents, enhancing their digital interactions.

Relying Parties: Relying parties are entities or individuals that rely on trust services provided by QTSPs under the eIDAS regulation. These parties use trust services to ensure the authenticity, integrity, and security of electronic transactions.

The EUDIW ecosystem assigns different roles to public sector entities. The Business Blueprint for Social Security will allocate specific roles for the social security domain. The current document will also outline the necessary business requirements and orchestrate the business processes that are essential for the effective functioning of social security coordination.

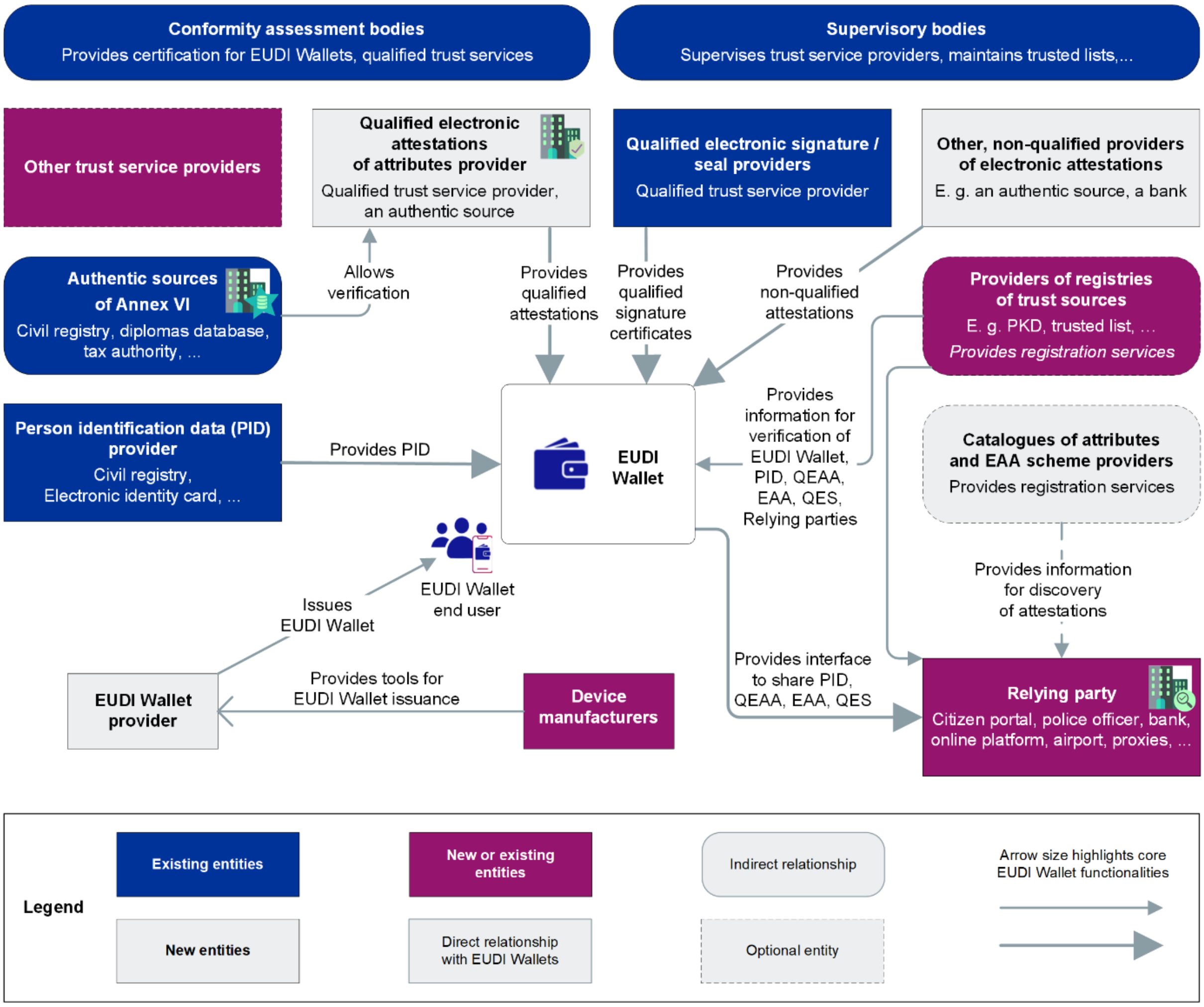

Conformity assessment bodies
Provides certification for EUDI Wallets, qualified trust services
Supervisory bodies
Supervises trust service providers, maintains trusted lists,...
Other trust service providers
Qualified electronic attestations of attributes provider
Qualified trust service provider, an authentic source
Qualified electronic signature / seal providers
Qualified trust service provider
Other, non-qualified providers of electronic attestations
E. g. an authentic source, a bank
Authentic sources of Annex VI
Civil registry, diplomas database, tax authority, ...
Allows verification
Provides qualified attestations
Provides qualified signature certificates
Provides non-qualified attestations
Providers of registries of trust sources
E. g. PKD, trusted list, ...
Provides registration services
Person identification data (PID) provider
Civil registry, Electronic identity card, ...
Provides PID
EUDI Wallet
Provides information for verification of EUDI Wallet, PID, QEAA, EAA, QES, Relying parties
Catalogues of attributes and EAA scheme providers
Provides registration services
EUDI Wallet end user
Issues EUDI Wallet
Provides information for discovery of attestations
Provides interface to share PID, QEAA, EAA, QES
EUDI Wallet provider
Provides tools for EUDI Wallet issuance
Device manufacturers
Relying party
Citizen portal, police officer, bank, online platform, airport, proxies, ...
Legend
Existing entities
New or existing entities
Indirect relationship
Arrow size highlights core EUDI Wallet functionalities
New entities
Direct relationship with EUDI Wallets
Optional entity

FIGURE 1: ROLES AND ENTITIES IN THE EUDIW 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

Guidelines will be established how a public and private service should issue (Q)EAAs for natural and legal persons by digital means in the EUDIW ecosystem. Furthermore, the European Identity Framework will also define how trust and security can be reached in a full digital manner. The starting point for specifying the implementation details is the eIDAS regulation [1]:

“The “European Declaration on Digital Rights and Principles for the Digital Decade” proclaimed by the European Parliament, the Council and the Commission6 (the ‘Declaration’), underlines everyone’s right to access digital technologies, products and services that are safe, secure, and privacy-protective by design.” (Preamble 4)

“This includes ensuring that all people living in the Union are offered an accessible, secure and trusted digital identity that enables access to a broad range of online and offline services, protected against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation. The Declaration also states that everyone has the right to the protection of their personal data. That right encompasses the control on how the data is used and with whom it is shared.” (Preamble 4)

“Union citizens and residents in the Union should have the right to a digital identity that is under their sole control and that enables them to exercise their rights in the digital environment and to participate in the digital economy. To achieve that aim, a European digital identity framework should be established allowing Union citizens and residents in the Union to access public and private online and offline services throughout the Union.” (Preamble 5)

“A harmonised digital identity framework should contribute to the creation of a more digitally integrated Union by reducing digital barriers between Member States and by empowering Union citizens and residents in the Union to enjoy the benefits of digitalisation, while increasing transparency and the protection of their rights.” (Preamble 6)

“Everyone should be able to access public and private services securely, relying on an improved ecosystem for trust services and on verified proofs of identity and electronic attestations of attributes, such as academic qualifications, including university degrees, or other educational or professional entitlements.” (Preamble 7)

“European Digital Identity Wallets should facilitate the application of the ‘once only’ principle, thus reducing the administrative burden on and supporting cross border mobility of Union citizens and residents in the Union and businesses across the Union, and fostering the development of interoperable e-government services across the Union.” (Preamble 11)

“The onboarding of Union citizens and residents in the Union to the European Digital Identity Wallet should be facilitated by relying on electronic identification means issued at assurance level high.” (Preamble 28)

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

> *“Public service providers use the person identification data available from electronic identification means pursuant to Regulation (EU) No 910/2014 to match the electronic identity of the users from other Member States with the person identification data provided to those users in the Member State performing the cross-border identity matching process.” (Preamble. 41)*
>
> *“An electronic attestation of attributes should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic attestation of attributes. General requirements should be laid down to ensure that a qualified electronic attestation of attributes has the equivalent legal effect of lawfully issued attestations in paper form.” (Preamble 55)*
>
> *“This Regulation lays down an obligation for qualified trust service providers to verify the identity of a natural or legal person to whom the qualified certificate or the qualified electronic attestation of attribute is issued based on various harmonised methods across the Union.” (Preamble 74)*
>
> *“To ensure that qualified certificates and qualified electronic attestations of attributes are issued to the person to whom they belong and that they attest the correct and unique set of data representing the identity of that person, qualified trust service providers issuing qualified certificates or issuing qualified electronic attestations of attributes should, at the moment of the issuance of those certificates and attestations, ensure with complete certainty the identification of that person.” (Preamble 74)*

The eIDAS framework aims to provide equal conditions for qualified trust services within the EU, ensuring efficient and secure digital interactions for both public and private sectors. Social Security is explicitly mentioned in the eIDAS regulation in terms of demonstrating ownership, verification of credentials and acceptance of credentials [1]:

> *“It should be possible to issue and handle trustworthy electronic attributes and contribute to reducing administrative burden, empowering Union citizens and residents in the Union to use them in their private and public transactions. Union citizens and residents in the Union should be able, for instance, to demonstrate ownership of a valid driving licence issued by an authority in one Member State, which can be verified and relied upon by the relevant authorities in other Member States, to rely on their* ***social security credentials*** *or on future digital travel documents in a cross border context.” (Preamble 54)*
>
> *“The wide availability and usability of European Digital Identity Wallets should enhance their acceptance and trust in them both by private individuals and by private service providers. Therefore, private relying parties providing services, for example in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, telecommunications or education, should accept the use of European Digital Identity Wallets for the provision of services where strong user authentication for online identification is required by Union or national law or by contractual obligation.” (Preamble 56)*

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

1.3. RULEBOOK

The eIDAS 2.0 framework introduces the concept of a "Rulebook" to streamline and govern the application of digital identity and trust services across Europe. This Rulebook is designed to be a detailed guide, supporting the implementation of digital services in a secure, consistent, and interoperable manner across EU member states. Its primary functions include standardization, providing flexibility, ensuring clarity, and harmonizing differences between national systems and the EU framework, especially regarding electronic identification and trust services.

Particularly significant is the potential introduction of a third legal regime within eIDAS 2.0 for electronic attestations of attributes. Here, the Attestation Rulebooks would define crucial aspects such as the attributes schema, data format and proof mechanism for those attestations and the trust mechanism for authentication and authorisation. It would also establish operational guidelines for entities issuing and relying on these attestations, ensuring they operate effectively within the legal framework.

For sector-specific needs in social security coordination, a tailored rulebook by DC4EU would outline the governance structure, operational standards, and technical specifications necessary to support digital credentials. This includes aligning with EU-wide regulations like GDPR, detailing credential management processes, and integrating the European Digital Identity Wallet (EUDIW) to enhance the mobility of citizens across the EU.

This sector-specific approach is designed to enhance the efficiency and security of social security coordination, aligning with the overarching goals of eIDAS 2.0 to create a seamless and inclusive digital single market. It aims to build a trusted and secure digital framework that supports the streamlined administration and verification of social security benefits across member states, thus facilitating easier access to services and improving the mobility of citizens within the EU.

In the following sections, we will establish a rulebook, set to be delineated within the DC4EU framework for the social security domain. This rulebook, grounded on the present Business Blueprint document, will be systematically documented throughout the project's duration in Deliverable 6.2, titled 'Deployment, Testing & Piloting Scenarios Results Library.

1.3.1. Governance and Operational Framework:

Regulatory Alignment: The rulebook must comply with EU-wide regulations, including eIDAS 2.0, the General Data Protection Regulation (GDPR), and specific mandates of the European Digital Identity Wallet (EUDIW). It should ensure legal validity and the protection of personal data in the processing of social security claims and services.

Stakeholder Roles and Responsibilities: Define clear roles for social security stakeholders (issuers), beneficiaries (holders), service providers, and regulatory bodies, detailing their responsibilities in the digital social security ecosystem.

1.3.2. Technical Specifications:

Credential and Data Models: Establish data models for digital credentials in social security, aligning with the W3C Verifiable Credential standards and including specific social security attributes relevant to entitlements and benefits.

Security and Privacy Protocols: Detail the security measures and privacy-preserving technologies, such as encryption and selective disclosure, to be employed in the management and sharing of digital credentials.

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

1.3.3. Interoperability and Ecosystem Integration:

Cross-Sector and Cross-Border Recognition: Create guidelines for the recognition of digital social security credentials across EU member states, facilitating the portability of benefits and entitlements.

EUDIW Integration: Outline the integration of social security digital credentials within the EUDIW, ensuring that beneficiaries have seamless access to and control over their credentials.

1.3.4. Quality Assurance and Trust Mechanisms:

Accreditation and Trust Framework: Establish an accreditation process for social security institutions wishing to issue digital credentials, including criteria for verification processes and the maintenance of trust lists or registries.

Lifecycle Management: Define procedures for the evocation, and expiration of digital credentials, ensuring the ongoing integrity and relevance of credentials in the social security ecosystem.

Dispute Resolution and Audit Trails: Implement mechanisms for resolving disputes related to credential verification or misuse and define requirements for audit trails to ensure traceability and accountability in social security transactions.

1.4. SCOPE AND SCENARIOS

The optimal usage of the EUDIW eco-system involves employing a valid EUDIW, with an onboarded identity (PID), and cryptographically bound credentials stored therein. However, this may not be the only situation in which Citizens and Relying Parties will engage. While the primary focus of the DC4EU Pilot for Social Security interactions will be on the main digital identity scenario using a valid EUDIW, other scenarios do exist for certain credential types in certain countries and may do so for the foreseeable future - if not as a permanent alternative to the digital identity scenario.

Essentially, there are four basic scenarios partitioned along the wallet and identity usage. All four scenarios represent valid forms of entitlement documents and may be presented in situations across Europe to various degrees. The involved level of trust among the various stakeholders involved may also exhibit differences related to the scenario considered.

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

	Scenario	Description	Pilot	Level of ID Certainty	Verification Method
	A	**Valid EUDI Wallet** (with identity)	DC4EU	High (digital linkage)	- Cryptographic Identity - Cryptographic Credential - Issuer Authenticity - Revocation - Machine inspection
	B	**Other Wallet types** (without Identity)	EBSI-VECTOR	Current (manual comparison)	- Cryptographic Credential - Issuer Authenticity - Revocation - Machine inspection
Long-term alternate	C	Electronic (outside wallet eco-system)	N/A	Current (manual comparison)	- Issuer Authenticity - Revocation - Visual inspection
	D	Physical (paper/card)	N/A	Current (manual comparison)	- Issuer Authenticity - Revocation - Visual inspection

TABLE 1:FOUR BASIC SCENARIOS OF WALLET AND IDENTITY USAGE

Scenario B and the potential usage of services for social security coordination is covered by other EC piloting activities alongside DC4EU, which is why it is not treated in more detail in this document.

Improvements of the existing scenarios C and D, lies outside the scope of the DC4EU pilot, but should be considered as potential extensions of any conclusions of the EUDI Wallet pilots. These scenarios are seen as the permanent alternative to the digital identity scenario to be used by citizens unable or unwilling to use the EUDIW.

In all scenarios, a key aspect of DC4EU is the potential to utilise a common authenticity and revocation check framework and associated infrastructure.

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

1.5. PID AS THE BASE DIGITAL IDENTITY

The Person Identification Data (PID) and the electronic Identification (eID) both serve to digitally represent an individual's identity, albeit in slightly different contexts:

1. **eID**: The eID, issued by either public or private entities and recognised by an EU MS, serves as digital proof of identity, and provides a high Level of Assurance (LoA), with some countries still relying substantially on it. It has been in use throughout the EU for several years, enabling citizens to access public (online) services in many EU MSs, and in some cases, private services as well.
2. **PID**: The PID, a newer concept introduced, with a similar data set as the eID for the European Digital Identity Wallet (EUDIW), is provided to the EUDIW in a harmonised common format by trusted entities responsible for verifying the identity of the EUDIW user. It is unique to the specific wallet instance and securely stored and provided as a VC in the Wallet. The data points coming with the PID according to a national eID schema are the same for every PID instance. While it serves a similar purpose as the eID, it is specifically designed for use within the EUDIW ecosystem for authentication and identification.

The PID embraces the concept of a digital identity tailored specifically for use within the EUDIW framework. The PID allows seamless integration of various credentials, such as the European Health Insurance Card (EHIC) and the Portable Document A1 (PD A1), alongside an individual's digital identity. This unified approach ensures that these credentials are universally recognised and accepted across Europe. Moreover, by enabling verification alongside a trustworthy digital identity, the PID enhances their trustworthiness and reliability in both the issuing MS as well as the MS where a verification can take place. While the eID served in some countries as a representation of identity in the past, preliminary for authentication for online services, the PID now fulfils this crucial role within the EUDIW ecosystem, providing a secure and interoperable way to manage identity and attestation of attributes for this identity across the EU in on- and offline situations.

1. **European Interoperability**: Recognised across all EU MSs, the PID ensures that a user's identity can be verified anywhere in the EU, supporting the European Single Market's aim to enable free movement of goods, services, and people across MSs.
2. **EU Regulations Compliance**: The management of PID within the EUDIW ecosystem is designed to comply with EU regulations, including the General Data Protection Regulation (GDPR). This includes principles such as data minimisation, user control over their data, and secure storage and sharing of data.
3. **Cross-Border Services**: With the EUDIW as an eID means, EU citizens can access public and private services in any EU MS, not just their home country. This aligns with the EU's eGovernment action plan to provide cross-border digital public services to citizens.
4. **Trust Framework**: By presenting PID with various credentials, the PID forms the basis of the trust framework in the EUDIW ecosystem, ensuring that these credentials are issued to that verified identity and increasing their trust and reliability across the EU.
5. **EU-wide Identity Verification**: The PID facilitates EU-wide identity verification and correct usage of digital attestations, which is crucial for various EU initiatives and services, such as social security coordination.

In summary, the PID is designed to digitally represent a citizen in a way that supports the goals of the EU, including interoperability, compliance with EU regulations, provision of cross-border services, establishment of a trust framework, and facilitation of EU-wide identity verification by electronic means. As per legal definitions, PID is a set of data, but it is not itself an eID means (on the contrary, PID is contained in an eID means). It is the EUDIW with the identity data points (PID) which makes it an eID means [1]:

> *“electronic identification means’ means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service;” (Art. 3, Paragraph 2)*
>
> *“person identification data’ means a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.” (Art. 3, Paragraph 3)*

The EUDIWs are legally defined as eID means, which mandates that they shall meet the requirements regarding assurance level “high”, particularly concerning identity proofing and verification, and eID means management and authentication [1].

By using the PID together with digital credentials in the EUDIW ecosystem, the verification process for social security documents can become more efficient. When a holder presents a digital credential, the relying party can verify both the authenticity of the credential and the identity of the user in one-step. This not only streamlines the verification process but also enhances the security and trust in the system. It ensures that the legitimate holder, thereby reducing the risk of fraud, is presenting the digital credentials.

1.6. BUSINESS BLUEPRINT FOR SOCIAL SECURITY

In the realm of social security, a crucial advancement is the introduction and execution of a universally applicable and user-friendly digital framework guided by the “Subsidiarity Principle” for the issuance and authentication of entitlement documents. This approach promotes the use of digital technologies to streamline the provision and verification processes, encourages decentralisation by allowing local entities to manage entitlements while adhering to overarching EU principles, and ensures that the solutions are generic and adaptable, capable of being implemented across various social security systems within the EU. The EUDI framework also includes identity management, which is implemented by the EUDIW.

By adopting these innovative concepts and solutions, the EU can enhance the efficiency and security of its social security coordination, benefiting all citizens who exercise their right to free movement.

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 following documents may be of interest (See [2]):

Form	Purpose	Issuing authority and use
A1 **(formerly E 101 E 103)**	Statement of applicable legislation. Useful to prove that you pay social security contributions in another EU country as a posted worker or while working in several countries at the same time.	Issued by the social security institution of the country where you are insured. If you are posted, this is the institution in the sending country. If you work in various countries at the same time, it depends, but you first need to contact the institution in your country of residence.
S1 **(formerly E 106, E 109 and E 121)**	Certificate of entitlement to healthcare if you do not live in the country where you are insured. Useful for posted workers, cross-border workers, pensioners, civil servants, and their dependants.	Issued by your health insurance authority. Submit it to any health insurance authority in the country where you live.
S2 **(formerly E 112)**	Authorisation to obtain planned health treatment in another EU or EFTA country. You should be treated the same as a resident of that country - you may have to pay a percentage of the costs up front.	Issued by your health insurance authority. Submit it to the health insurance authority in the country where you go for treatment.
S3	Certificate of entitlement to healthcare in your former country of employment. Useful for retired cross-border workers who are no longer insured in their former country of employment.	Issued by your health insurance authority. Submit it to the health insurance authority of the country where you used to work as a cross-border worker.
U1 **(formerly E 301)**	Statement of insurance periods to be taken into account when calculating an unemployment benefit.	Issued by the public employment service or the competent social security institution in the last country(ies) where you worked. Submit it to the national employment service in the country where you wish to receive unemployment benefit.
U2 **(formerly E 303)**	Authorisation to continue receiving unemployment benefit while looking for a job in another country.	Issued by the public employment service or the competent social security institution in the country where you became unemployed. Submit it to the national employment service in the country where you are looking for a job.
U3	Warning to the employment services of the country paying your benefits, reporting changes in your situation, which may lead to a revision of your benefit payments.	Issued by the public employment service or the competent social security institution of the country where you are looking for a job on the basis of a U2 form.

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

DA1 (formerly E 123)	Certificate of entitlement to medical treatment under special conditions reserved for accidents at work and occupational diseases in another EU country.	Issued by your health insurance authority. Submit it to the health insurance authority of the country where you are staying.
P1	Summary of pension decisions taken in your case by the various institutions in the EU countries from which you have claimed an old age, survivors, or invalidity pension.	Issued by the pension authority to which you made your pension claim, once the authority has received details of the decisions made by the various authorities who have dealt with your claim.
EHIC	Is a free card that provides insured persons with access to medically necessary government-provided healthcare during a temporary stay in one of the 27 EU countries, Iceland, Liechtenstein, Norway, Switzerland, and the UK under the same conditions and at the same cost (free in some countries) as persons insured in that country. The services covered include, for example, services related to chronic or existing illnesses, as well as in connection with pregnancy and childbirth. Any implementation effort on a European scale using an electronic wallet should use the EHIC, issued by national authorities, as a benchmark for an implementation on a European scale.	

TABLE 2: LIST OF PORTABLE DOCUMENTS

Considering the **clearly structured organisational and legal framework** of social security in Europe, the adoption of innovative technologies and frameworks necessitates a **systematic and incremental approach** to attain comprehensive operational capability. The cornerstone of this strategy is the **detailed articulation of organisational and business prerequisites**, as outlined in the current document. This blueprint will be informed by, and at a minimum, include definitions based on key entitlement documents such as:

- **PD A1** - which certifies the social security legislation applicable to the citizen.
- **EHIC** - which facilitates access to medical care during temporary visits to other EU countries.

This comprehensive document will serve as a foundational guide for modernising and streamlining social security processes in line with current regulatory frameworks and technological advancements.

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

1.7. METHODOLOGY

For creating a comprehensive Business Blueprint, DC4EU Social Security is adopting a **methodology** that is **systematic**, **inclusive**, and **iterative**. The following steps are included:

- **Stakeholder Engagement**: Initiated by identifying and engaging with all key stakeholders within the social security domain, including policymakers, IT professionals, users, and legal experts.
- **Current State Analysis**: Conduct a detailed analysis of existing processes and systems, documenting the current state to establish a baseline for future improvements.
- **Requirement Gathering**: Compile business requirements from stakeholders, addressing all facets of social security processes such as issuing, revocation, and verification of credentials.
- **Regulatory Compliance**: Ensure the blueprint adheres to the eIDAS regulation, GDPR, and other pertinent legal frameworks through close collaboration with legal experts.
- **Process Design**: Develop a clear outline of the future business processes that integrate digital transformation objectives, utilising process modelling techniques for workflow visualisation.
- **Data Modelling**: Create data models for VCs that are compliant with eIDAS and GDPR, prioritising data integrity, privacy, and authenticity.
- **Technology Assessment**: Assess various technologies to support the new processes, focusing on decentralised systems and digital identity solutions.
- **Prototyping**: Construct prototypes or mock-ups of the new processes and systems to validate concepts and solicit early feedback.
- **Feedback Loops**: Establish continuous feedback mechanisms from stakeholders to iteratively refine the Business Blueprint.
- **Documentation**: Assemble all findings, designs, and models into a well-structured Business Blueprint document.
- **Validation and Testing**: Validate the blueprint against real-world scenarios and conduct tests to ensure its feasibility and effectiveness.
- **Implementation Roadmap**: Formulate a phased implementation plan detailing the necessary steps, timelines, and resources to actualise the blueprint.

This methodology emphasises a structured, participatory, and adaptable approach to developing a Business Blueprint that meets the dynamic needs of the social security domain within the EU.

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. STATUS QUO ANALYSIS

2.1. INTRODUCTION

To conduct a thorough examination of the current processes related to European Health Insurance Card (EHIC) and Portable Document A1 (PD A1), two questionnaires have been crafted. These surveys, comprising 121 questions for EHIC and 75 questions for PD A1, have been distributed to both consortium and non-consortium members.

The objective is to gather diverse perspectives and insights, ensuring a comprehensive analysis of the status quo. The questions cover a spectrum of crucial aspects, including:

- General Information about the competent institutions involved
- Statistics related to EHIC, PRC and PD A1 issuance and usage
- Characteristics of EHIC, PRC and PD A1 business data
- General Information about issuance, including
  - Competent institutions involved in the issuing process
  - Validity Period of issued documents
- Process descriptions of issuance, verification and documentation
- Use case descriptions and charts

2.2. PARTICIPANTS AND RETURN RATES

2.2.1. Participants

The questionnaires for the EHIC and PD A1 use cases were distributed to 25 institutions across 16 European countries. Participants are members of the DC4EU consortium or candidates for membership.

A request has been made to ensure that if the receiving institution is not responsible for a specific use case, it should pass the questionnaires along to the appropriate body that is responsible. Additionally, all recipients were requested to share the questionnaires with their national Liaison Body to obtain a comprehensive overview of the respective country's perspective.

Further, the questionnaires were extended to 15 institutions across 14 European countries that are not participating in the DC4EU project.

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. Return Rates

The questionnaires were completed by a total of 41 institutions from 18 countries.

□ Consortium: 15/16 countries (94%)
□ Non-consortium: 3/14 countries (21%)
□ EHIC replies: 28 institutions from 14 countries
□ PD A1 replies: 23 institutions from 18 countries

Below table lists the institutions and questionnaires (EHIC & PD A1) provided.

Country	Institution	Acronym	EHIC	PD A1
AT	Dachverband der Sozialversicherungsträger	DVSV	1	1
AT	Österreichische Gesundheitskasse	ÖGK	1	1
AT	Sozialversicherungsanstalt der Selbständigen	SVS	1	1
AT	Sozialversicherungs-Chipkarten Betriebs- und Errichtungsgesellschaft m.b.H	SVC	1	0
BE	National Social Security Office	NSSO	0	1
CH	Federal Social Insurance Office	FSIO	1	1
CH	SASIS AG	SASIS	1	0
CZ	Česká průmyslová zdravotní pojišťovna	ČPZP	1	0
CZ	Czech Social Security Administration	CSSA, ČSSZ	0	1
CZ	Oborová zdravotní pojišťovna	OZP	1	0
CZ	RBP, zdravotní pojišťovna	RBP	1	0
CZ	Vojenská zdravotní pojišťovna České republiky	VoZP	1	0
CZ	Všeobecná zdravotní pojišťovna České republiky	VZP ČR	1	0
CZ	Zaměstnanecká pojišťovna Škoda	ZPŠ	1	0
CZ	Zdravotní pojišťovna ministerstva vnitra České republiky	ZP MV ČR	1	0
DE	Deutsche Rentenversicherung Bund	DRV Bund	0	1
DE	Deutsche Verbindungsstelle Krankenversicherung - Ausland	DVKA	1	1
DK	Danish Patient Safety Authority - EU Health Insurance	STPS	1	0
DK	International Social Sikring	ISS	0	1

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

Country	Institution	Acronym	EHIC	PD A1
ES	Tesorería General de la Seguridad Social	TGSS	0	1
ES	Instituto Nacional de la Seguridad Social	INSS	1	0
FI	Eläketurvakeskus Finnish centre for pensions	ETK	0	1
FI	Kansaneläkelaitos	KELA, FPA	1	0
FR	Central Agency for Social Security Institutions	ACOSS	0	1
FR	National Health Insurance for Education	MGEN	1	1
FR	National Health Insurance Fund	CNAM	1	0
FR	National Military Social Security Fund	CNMSS	1	0
IE	Department of Social Protection	DSP	0	1
IE	Health Service Executive	HSE	1	0
IT	National Social Insurance Agency	INPS	0	1
LT	State Social Insurance Fund Board Vilnius Office	Sodra Vilnius Office	0	1
LV	National Health Service	NHS	1	0
LV	State Social Insurance Agency	SSIA	0	1
NL	Centraal Administratie Kantoor	CAK	1	1
NL	Dutch Health Insurance Organizations	HIO	1	0
NL	Sociale Verzekeringsbank	SVB	0	1
PL	Narodowy Fundusz Zdrowia	NFZ	1	0
PL	Zakład Ubezpieczeń Społecznych - Centrala	ZUS	0	1
PT	Instituto da Segurança Social	ISS	1	1
SE	The Swedish Social Insurance Agency	Försäkringskassan	1	1
SK	Social Insurance Agency	SIA	0	1
Total			**27**	**23**

TABLE 3: RETURN RATE OF THE QUESTIONNAIRES EHIC & PD A1

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

2.2.3. Coverage

The questionnaires encompass 18 out of the 27 EU member states (MSs). The accompanying figure illustrates this distribution: countries participating in the DC4EU consortium are indicated in a dark blue shade, candidates in light blue, non-members of DC4EU in a light orange colour, and those not participating in the DC4EU questionnaire from the EU are displayed in dark grey.

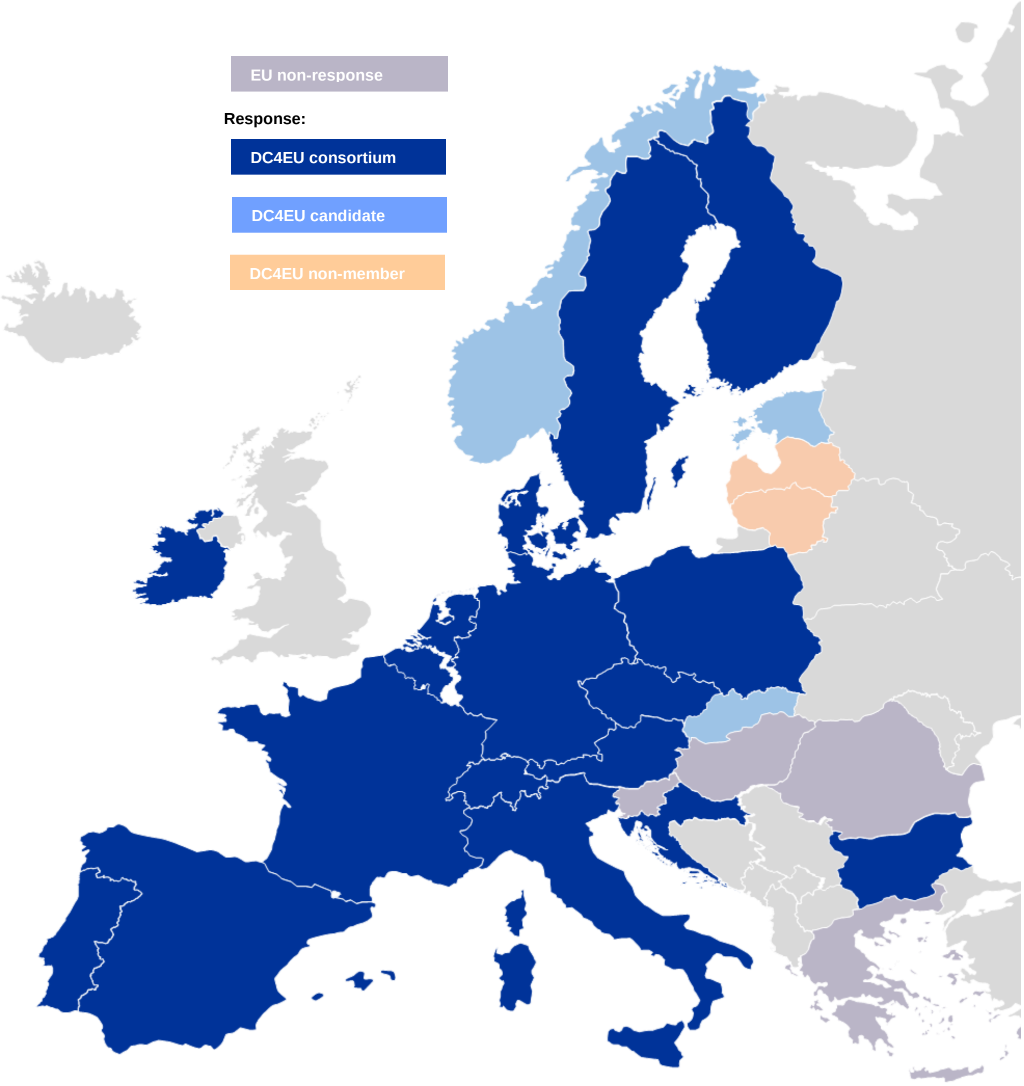


FIGURE 2: COVERAGE BY COUNTRY

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

2.3. Portable Document A1 (PD A1)

2.3.1. General

The PD A1 is a certificate, which documents the applicable law for social security in a cross-border situation of employment(s).

The applicable law for social security is set out in the Regulation (EC) No. 883/2004 [3]. The applicable law for social security stipulates in Art. 11 Paragraph 3 Letter a) of [3] as a principle that a person who pursues an activity as an employed or self-employed person in a MS is subject to the legislation of that MS (i.e. cross border worker). To promote mobility of citizens and to protect their rights, support a stable insurance record and to avoid administrative burden for employees, self-employed persons, employers and social security institutions in cross-border situations the applicable law contains several exceptions of the principle rule. Exceptions of the principle rule apply for:

- Posting (Art. 12 of [3]): A posting situation exists if the pursued employment or self-employment in another MS does not exceed 24 months. If further requirements are met, the social security law of the posting state continues to apply for the employee or self-employed person for the duration of the activity in the other MS.
- Civil Servants (Art. 11 Paragraph 3 Letter b) of [3]): A civil servant is permanently subject to the legislation of the MS to which the administrative unit belongs.
- Mariners (Art. 11 Paragraph 4 of [3]): Mariners are generally subject to the law of the MS under whose flag the ship is sailing. But if the place of residence of the mariner in another MS complies with the registered office of the employer paying the remuneration, the citizen can request a PD A1 which documents the application of the law of this MS.
- Flight or cabin crew (Art. 11 Paragraph 5 of [3]): For flight or cabin crewmembers, the applicable legislation is determined by their ‘home base’.

Finally, Article 16 (1) of [3] permits the competent authorities of two or more MSs to reach agreements dealing with exceptions to the rules governing the applicable legislation.

In posting situations (concerning persons covered by Article 12 of [3]), the PD A1 is issued by the social security authorities of the country (**competent institutions (CIs)**) in which the person normally works, so that the social security regulations in force up to that point continue to apply. In other situations (see other articles mentioned above) another country may also be the issuing country of the PD A1.

According to the statistical assessment provided in the annex to the European Commission's Statistical Report on PD A1 (Note 219-23), on page 19, in Chapter 2.1 titled "Number of PDs A1 issued in 2022," a total of 4.6 million PDs A1 were issued in 2022, at the request of employers or individuals. The majority, around 3 million PDs A1, were issued for individuals covered by Article 12 of [3] (i.e. posted workers).

In 2022, approximately 3.8 million PDs A1 were in circulation issued by the questionnaire respondents in total, demonstrating the coverage of PD A1 issuers participating in DC4EU.

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

2.3.1.1. Legal Framework

The PD A1 is governed by a comprehensive legal framework that ensures its validity and application across European nations. The primary legislative pillars underpinning the PD A1 are:

- **Regulation (EC) No 883/2004 on the coordination of social security systems**: This regulation establishes the overarching principles for determining the applicable social security legislation for mobile workers within the EU. It aims to prevent workers from being subjected to dual social security contributions and ensures that they are covered by their home country's social security system while working temporarily in another MS [3].
- **Regulation (EC) No 987/2009 implementing Regulation (EC) No 883/2004:** This regulation provides more detailed rules on the implementation of the coordination of social security systems, including mobile workers [4].
- **National Social Security Legislation:** The specific provisions governing the application of the PD A1 are further elaborated upon in the national social security legislation of each MS. These national laws provide more granular details on the modalities of applying the PD A1 in various scenarios, such as self-employed workers, posted workers, and those engaged in cross-border activities.

In conjunction with these legislative frameworks, additional relevant documents and guidance play a crucial role in ensuring the proper implementation and utilisation of the PD A1:

- **Single Digital Gateway Regulation:** The Single Digital Gateway Regulation requires MSs to ensure that EU citizens and businesses can access and complete key administrative procedures online, including the PD A1.
- Several **Decisions and Recommendations**: In addition to the above-mentioned regulations there are numerous decisions and recommendations dealing with the topic of workers abroad and the use of PDs A1. Decision No A1 of 12 June 2009 [5], Decision No A2 of 12 June 2009 [6], Decision No A3 of 17 December 2009 [7], and Recommendation No A1 of 18 October 2017 [8] regarding the granting of a PD A1, the Administrative Commission (AC) lays down the structure, content, format and detailed arrangements for the exchange of documents. The AC developed the current structure and design of the paper format of PD A1, however, it was never established in a formal decision. For portable documents, an electronic format (PDF) is allowed according to Recommendation H2. [9]

2.3.1.2. Characteristics of the PD A1

The format of a PD A1 can change from country to country across Europe:

- Most MSs issue PDs A1 in digital formats, as PDF documents (Belgium, Czechia, Denmark, Finland, Ireland, Poland, Slovakia, Sweden).
- Paper formats are still utilised by some MSs (Lithuania, Latvia).
- Notably, some MSs allow multiple formats, accommodating combinations of paper and digital (PDF) forms (Austria, France, Germany, Netherlands, Portugal, Spain, Switzerland).

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 issuance types for validity of PD A1 certificates may vary across MSs, depending on their respective national rules and regulations. The information presented here is based on the responses provided by participating countries in the survey and may not comprehensively represent the entirety of Europe:

- **Limited/Temporary**: The most prevalent type of PD A1, typically issued for up to 24 months for posted workers. This is the default type issued in most European countries.
- **Provisional Temporary**: Issued in particular circumstances, generally, when employment or self-employment is expected to be temporary but with an unconfirmed duration. This type has a limited validity period, typically issued to bridge until temporary PD A1 can be obtained.

Key Findings

- **Format:** The most widely used formats for issuance of documents are paper and digital (PDF) formats.
- **Temporary Validity**: Temporary PDs A1 are the standard issuance type.

2.3.1.3. Central Repository for Notification of PD A1 Issuance

In many countries, PD A1 storage is typically centralised, and access to the central database of all valid PDs A1 is subject to the legal authority of an institution. This necessitates the existence of (separate) repositories for both issued and received PDs A1, each serving as a valuable tool for cross-verification in the back-office. It is essential to highlight that the repository for incoming PDs A1 holds significant value for verification purposes within the country where the respective work activity is conducted.

All 18 respondent countries employ a central database for storing the notification information about the issuance of PD A1 documents. The specific arrangements for incoming and outgoing PD A1 documents vary across countries.

- **Only incoming PD A1** documents (Host MS storing PDs A1 issued in another MS) are centrally stored in Germany (1 country).
- **Only outgoing PD A1** documents (MS storing their own issued PDs A1) are centrally stored in Czechia, Ireland, Poland, Slovakia, Spain, and Sweden (6 countries).
- **Both incoming and outgoing PD A1** documents are centrally stored in Austria, Belgium, Switzerland, Denmark, Finland, France, Italy, Latvia, Lithuania, Netherlands, and Portugal (11 countries). After the go live of “Electronic Exchange of Social Security information” (EESSI) Structured Electronic Documents (SEDs) are stored instead of PDs A1.

Country	Institution Acronym	Incoming PD A1	Outgoing PD A1
AT	DVSV	X	X
BE	NSSO	X	X
CH	FSIO	X	X
CZ	CSSA, CSSZ		X
DE	DRV-Bund	X	

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

Country	Institution Acronym	Incoming PD A1	Outgoing PD A1
DK	ISS	X	X
ES	TGSS		X
FI	ETK	X	X
FR	ACOSS	X	X
IE	DSP		X
IT	INPS	X	X
LT	n/a	X	X
LV	SSIA	X	X
NL	SVB	X	X
PL	ZUS		X
PT	ISS	X	X
SE	FK		X
SK	SIA		X

TABLE 4: CENTRAL REPOSITORY FOR PD A1

2.3.2. Issuance Process of the PD A1

The following chapter outlines the standard issuing process, which has been identified for posting situations. For other matters, the issuance process may differ from the one described here.

The process of the issuance of a PD A1 for posted workers can be initiated by employers or self-employed individuals through the submission of a request to the CI in the country where the individual is regularly employed or resides. This initiation can be done through various channels, such as public authority platforms, email submissions, payroll processes, or in-person interactions. It is worth noting that, in most respondent countries, there is no distinction in the issuance process between the application procedures for employers and self-employed individuals, apart Poland.

The issuance of a PD A1 is contingent upon the competence of the relevant institution, which is designated for specific employment groups. Each European country has its own designated institutions responsible for issuing PDs A1 for various employment categories, including posted workers, self-employed individuals, seasonal workers, cross-border workers, or workers with multiple employment.

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 issuance process for the "as/is" scenario is illustrated in the following diagram.

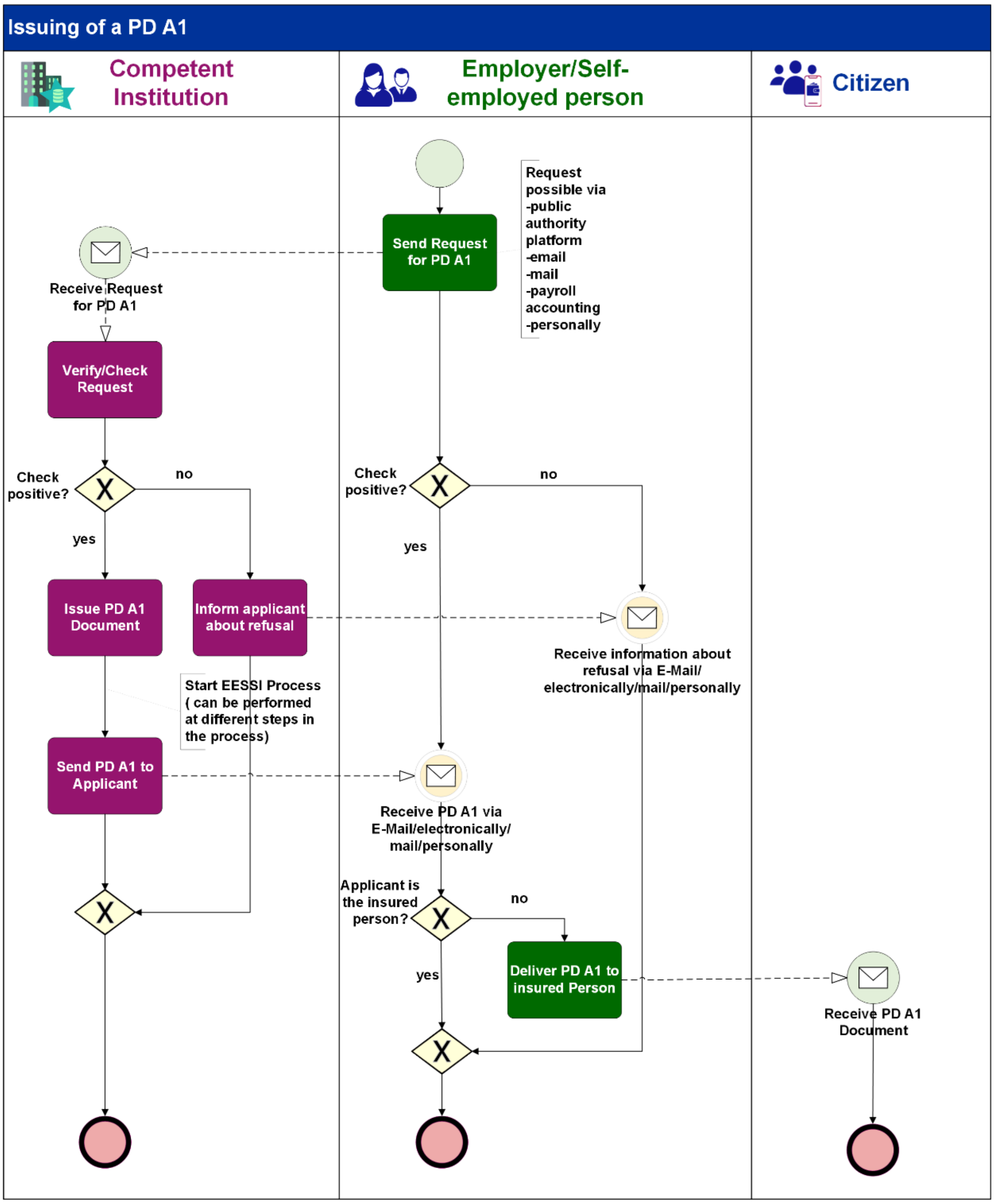

Issuing of a PD A1
Competent Institution
Employer/Self-employed person
Citizen
Send Request for PD A1
Request possible via -public authority platform -email -mail -payroll accounting -personally
Receive Request for PD A1
Verify/Check Request
Check positive?
no
yes
Issue PD A1 Document
Inform applicant about refusal
Start EESSI Process (can be performed at different steps in the process)
Send PD A1 to Applicant
Check positive?
no
yes
Receive information about refusal via E-Mail/ electronically/mail/personally
Receive PD A1 via E-Mail/electronically/ mail/personally
Applicant is the insured person?
no
yes
Deliver PD A1 to insured Person
Receive PD A1 Document

FIGURE 3: ISSUANCE OF PD A1

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

2.3.2.1. Connection with EESSI

The **Electronic Exchange of Social Security Information (EESSI)** is a system used within Europe for the exchange of social security information between MSs. It facilitates the implementation of regulations related to the coordination of social security systems within the EU.

In the context of the PD A1, which certifies the social security coverage of employed or self-employed persons pursuing work in another MS, EESSI plays a role in streamlining and automating the exchange of information related to these situations.

The extent of connection to EESSI processes when issuing PD A1 certificates varies across European States.

- 14 countries reported a direct connection to EESSI processes for PD A1 issuance. This means that once the issuer generates a PD A1 certificate in Austria, Belgium, Czechia, Denmark, Finland, France, Germany, Italy, Latvia, Netherlands, Poland, Slovakia, Spain, Switzerland, the data is automatically sent to EESSI for further processing.
- One country, Ireland, reported a partial connection to EESSI processes. This means that the PD A1 issuance process in Ireland is not fully integrated with EESSI, and there may be some manual steps involved.
- Three countries (Lithuania, Portugal, and Sweden) reported no connection to EESSI processes for PD A1 issuance. This means that the relevant data used for creating the PD A1 certificate must be manually entered in the relevant EESSI message for processing, which can be time-consuming and error prone.

2.3.3. Verification Process of the PD A1

The verification process typically involves the following steps:

- **Identity Verification:** The verifier verifies the identity of the individual by checking their ID card or passport to ensure it matches the information on the PD A1 certificate.
- **Visual Inspection:** The verifier visually inspects the PD A1 certificate to check for authenticity, including the personal data, validity date etc.
- **Documentation of Validation Result:** The verifier documents and transfers relevant information from the PD A1 to the responsible authorities.
- **Back-Office Cross-referencing**: A back-office process is initiated to cross-reference the presented PD A1 with central repositories, e.g. a central database, which contains the electronic messages sent through EESSI to verify presented data and/or to detect potential fraud or errors.

If either the PD A1 or ID verification is unsuccessful, the verifier informs the individual about the negative verification outcome.

Some MSs additionally offer verification services for authenticity checks of the PD A1 certificate.

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

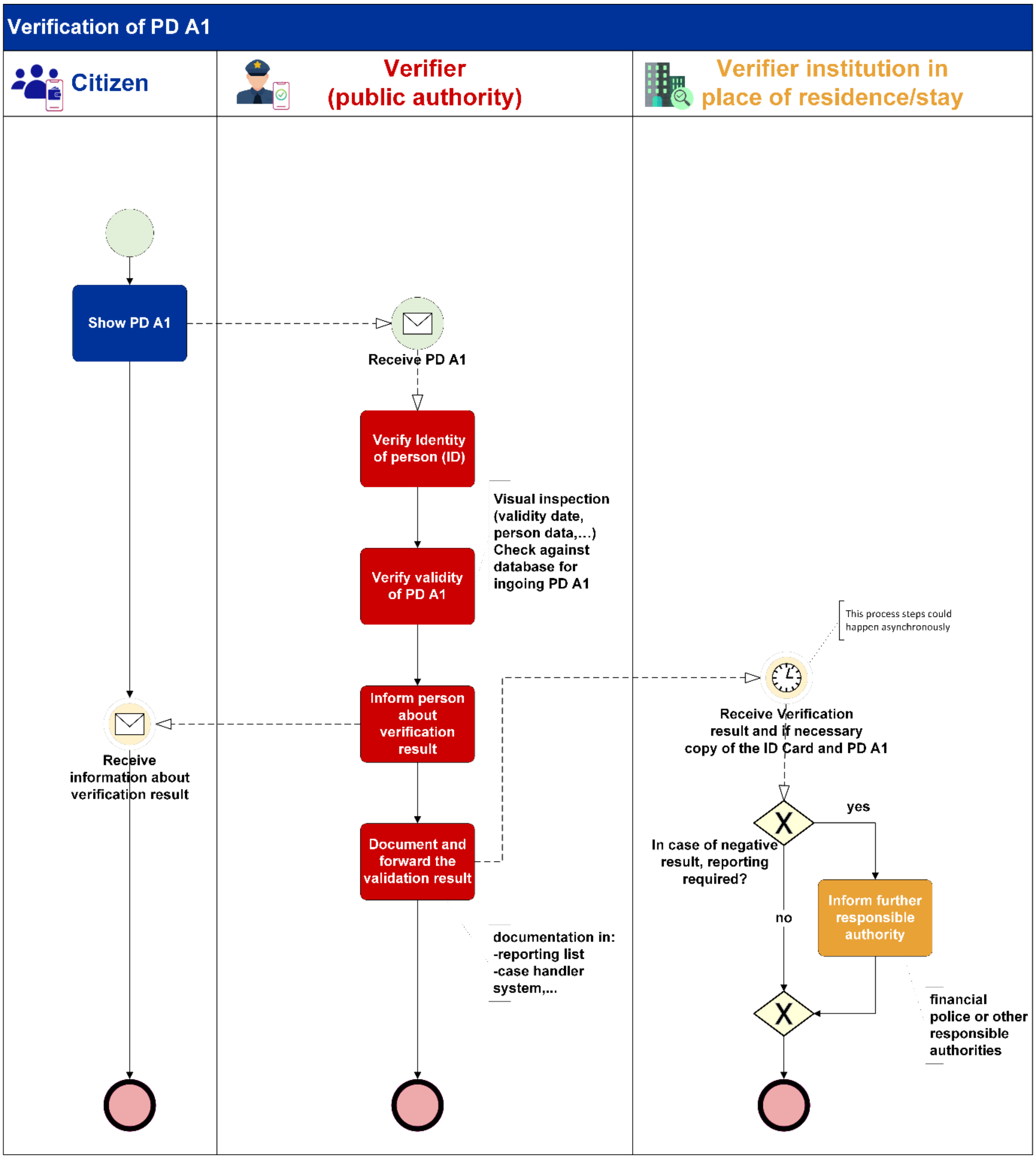

Verification of PD A1
Citizen
Verifier (public authority)
Verifier institution in place of residence/stay
Show PD A1
Receive PD A1
Verify Identity of person (ID)
Visual inspection (validity date, person data,...) Check against database for ingoing PD A1
Verify validity of PD A1
This process steps could happen asynchronously
Inform person about verification result
Receive information about verification result
Receive Verification result and if necessary copy of the ID Card and PD A1
Document and forward the validation result
In case of negative result, reporting required?
yes
no
Inform further responsible authority
documentation in: -reporting list -case handler system,...
financial police or other responsible authorities

FIGURE 4: VERIFICATION OF PD A1

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

2.3.3.1. Documentation Process

The documentation of identity verification by the verifiers is inconsistent across respondent countries, with only a minority of countries specifically documenting this process. However, all respondent countries document the verification of the PD A1 with records stored in various systems and the duration of storage is subject to national regulations.

Documentation of Identity Verification

The majority of respondent countries (15 out of 19) indicated the necessity or possibility of identity verification. However, only four countries (Switzerland, Czechia, Germany, Italy) specifically document this process. Four countries (Austria, Belgium, Portugal, Slovakia) stated that they do not document identity verification. Five countries (out of overall 23 respondent countries) did not provide any response.

Documentation of PD A1 Verification

Most respondent countries (18 out of 19) confirmed documenting the verification of the PD A1 certificate by the verifiers. Six countries did not provide any response. The documentation of PD A1 verification varies by country, with records stored in various systems such as central logging systems, relevant process records, inspection files, internal case handler systems, or registers. The duration for which this information remains stored in the back-office system is subject to national regulations.

2.3.3.2. Central Repository for authorised PD A1 Verifiers

The availability of a central repository for authorised (“trusted”) legal entities to verify PD A1 certificates vary across European countries. Some countries have well-established systems, while others may not have a centralized repository in place.

This variation in central repository practices suggests that the organisation of verifier-related activities differ considerably among European countries. The absence of a central repository may make it challenging to effectively manage verification processes, track their qualifications, and ensure consistent verification practices.

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

2.3.4. Onboarding Use Cases for PD A1

This subchapter outlines the existing onboarding processes for issuers and verifiers of PDs A1 (as-is). Chapter 0, Onboarding, addresses the proposed future processes for onboarding issuers and verifiers (to-be). Issuers are CIs qualified to issue PDs A1. Verifiers are public authorities authorised at a national level to verify PDs A1.

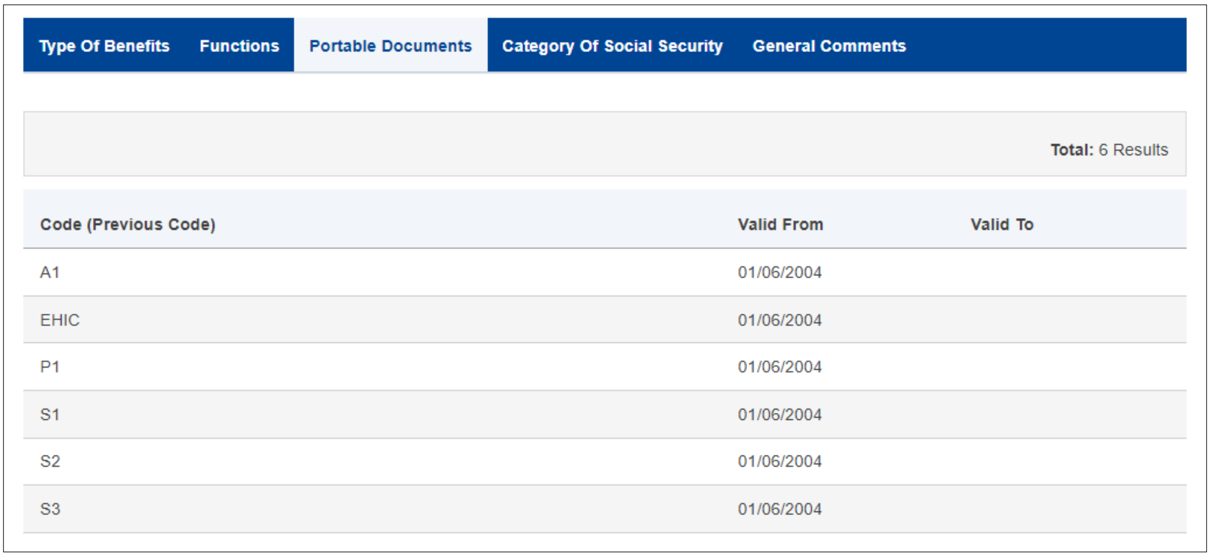
2.3.4.1. Onboarding Issuers

Onboarding New Issuers

In most MSs, the onboarding of new PD A1 issuers is not formally structured due to the limited expectation of new entrants and the mandated issuance of PDs A1 by law. PDs A1 are primarily issued by social security institutions, with limited participation from private issuers. As a result, the number of PD A1 issuers remains relatively low and stable. Issuer authorisation is primarily governed by national legislation, and authorisation is often granted on an indefinite basis. If a completely new institution is added to the EESSI Institution Repository (IR), a substantial change must be notified to the EC one month in advance. Whether an institution issues PDs A1 is listed in the IR under the section "Portable Documents". If an institution is qualified to issue PDs A1 (no matter if it is a newly added institution or an existing institution), no substantial change is necessary. The relevant portable document must be added to this section by the Institutional Repository (IR)-Single Point of Contact (SPOC).

Updating Issuer qualification

Modifications of issuer qualification are implemented in accordance with Decision No E2 of 3 March 2010 [10] and are regulated by AC decisions. These changes are reflected in national registries and the EESSI IR. If an institution is qualified to issue PDs A1 (no matter if it is a newly added institution or an existing institution), a substantial change in terms of the Business Use Case (BUC) competencies may be necessary. The relevant portable document must be added in the IR and competencies for executing certain business processes may be added by the IR-SPOC. Issued PDs A1 remain valid throughout these changes.



Total: 6 Results

Code (Previous Code)	Valid From	Valid To
A1	01/06/2004	
EHIC	01/06/2004	
P1	01/06/2004	
S1	01/06/2004	
S2	01/06/2004	
S3	01/06/2004	

FIGURE 5: THE EESSI INSTITUTION REPOSITORY – PUBLIC ACCESS INTERFACE – ISSUER OF PORTABLE DOCUMENTS. SOURCE: [11]

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

Merging Issuers

The merger of PD A1 issuers is governed by [10], involving the transfer of data to the newly CI. Issued PDs A1 retain their validity throughout the merger process. If two or more institutions in a country are merged, this must be notified to the EC by substantial change one month in advance and entered accordingly in the IR by the IR-SPOC.

Deactivating Issuers

Deactivating PD A1 issuers adheres to [10], with deactivation procedures executed in national registries and the IR. The deactivation of an institution must be notified to the EC one month in advance by substantial change. Furthermore, a successor institution must be notified and entered in the IR by the IR-SPOC.

Maintaining the IR

Updates to the IR are initiated by supervisory authorities or ministries, who notify the IR-SPOC for prompt execution.

2.3.4.2. Onboarding Verifiers

Onboarding New Verifiers

In most MSs, there is no formal onboarding process for new verifiers as the addition of new verifiers is not anticipated. The authorisation of verifiers is primarily regulated by national legislation, and the authorisation period is typically indefinite.

Updating Verifier Information

In most MSs, there is no established process for handling changes in verifier data as significant changes are not expected. However, national registries must be updated to reflect any changes. Additionally, in several MSs verifiers may have access to the central databases, where PD A1 information is stored. In order to handle the updated verifier’s information, the access to the relevant databases may need to be adjusted.

Merger of Verifiers

In most MSs, there is no formal process for handling the merger of verifiers as mergers are not anticipated. However, similar to changes in verifier data, national registries must be updated to reflect any changes. Additionally, a legal decision may be required in some cases.

Deactivation of Verifiers

In most MSs, the deactivation of verifiers follows a similar process to mergers and changes in verifier data. National registries must be updated, and a legal decision may be required. Additionally, in several MSs verifiers may have access to the central databases, where PD A1 information is stored. In order to correctly handle the deactivation of the verifier the access to the relevant databases may need to be revoked.

Maintaining National Repositories

While not all MS maintain national repositories for verifiers, in some cases, when the verifier is an institution listed in the IR, the relevant data there needs to be updated (in case of a new verifier as well as in cases of changes, mergers, deactivation).

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

2.4. EUROPEAN HEALTH INSURANCE CARD (EHIC)

2.4.1. General

The European Health Insurance Card (EHIC) is a complimentary document that entitles EU citizens, their family members, and certain other eligible individuals to access essential healthcare services while temporarily staying in any of the 27 EU MSs, as well as in Iceland, Liechtenstein, Norway, Switzerland, and the United Kingdom. The EHIC ensures that beneficiaries are treated on par with local residents in terms of care level and fees, irrespective of their nationality.

As of now, there are approximately 240 million EHICs in circulation, which equates to nearly half of the total population of the EU. However, the rate of EHIC ownership varies across EU MSs. This variation is due to the absence of harmonised standards governing the application, issuance, and validity periods of the cards. Furthermore, the EHIC can either be a standalone card or be integrated with a national health insurance card.

One of the key features of the EHIC is its role in the reimbursement process, as outlined by EU coordination regulations. When a citizen holding an EHIC avails healthcare services in a MS other than their home country, the costs are typically reimbursed by the competent authority (the home MS) based on the rates applicable in the visited MS. In most cases (about 90%), this reimbursement occurs directly between the involved MSs. Alternatively, the reimbursement may be processed between the competent authority and the insured individual.

As of the end of 2022, institutions either directly or indirectly associated with the DC4EU project (respondents to the questionnaire) issued a total of 116 million EHICs, accounting for nearly half of the overall EHICs in circulation. This highlights the significant role of these institutions in promoting the benefits of the EHIC.

2.4.1.1. Legal Framework

The legal framework for the EHIC is primarily established by the following regulations and directives:

- **Regulation (EC) No 883/2004 on the coordination of social security systems:** This regulation defines who is entitled to receive healthcare benefits in another EU MS and under what conditions. It also outlines the procedures for reimbursement of healthcare costs between MSs [3].
- **Regulation (EC) No 987/2009 implementing Regulation (EC) No 883/2004:** This regulation provides more detailed rules on the implementation of the coordination of social security systems, including specific provisions on healthcare benefits [4].
- **Decision S1 and S2**, from June 2009, concerning EHIC and its technical specifications [12] [13].

In addition to these primary regulatory instruments, the EHIC is also supported by a network of national laws and regulations in each EU MS that implement the EU framework and establish the specific procedures for EHIC application, issuance, and use.

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

Key Provisions of the Legal Framework:

- □ **Entitlement to EHIC:** The EHIC is issued to insured persons of EU MSs, their family members, and certain other categories of individuals, such as students and frontier workers.
- □ **Scope of Coverage:** The EHIC covers the following healthcare services provided during temporary stays in other EU MSs: Benefits in kind provided in the MS of stay in accordance with its legislation and which prove to be medically necessary so that the insured person does not have to return prematurely to the competent MS in order to receive the necessary medical treatment.
- □ **Benefits Availability:** The EHIC ensures that beneficiaries have access to care of the same quality as that provided to their host country's nationals.
- □ **Procedures for EHIC Application and Issuance:** Each EU MS has its own procedures for applying, issuing, and checking the validity period of an EHIC.

The legal framework for the EHIC plays a crucial role in facilitating cross-border healthcare access for EU citizens and ensuring their rights to receive essential medical services throughout the EU. It provides the foundation for a seamless and coordinated approach to healthcare portability within the single market.

The **Single Digital Gateway Regulation** requires MSs to ensure that EU citizens and businesses can access and complete key administrative procedures online, including citizens applying for and acquiring the EHIC.

2.4.1.2. Characteristics of the EHIC

[12] and [14], enacted on 12th June 2009, provide the technical specifications for the EHIC. The EHIC is a standardised plastic card with unique format and dimensions, designed to be easily recognisable and accepted by insured persons, healthcare providers and institutions.

The card’s front design is divided into fields, some of which contain unchangeable elements, while others are personalised. The visible information on the EHIC includes the family name and first names, birth date of the cardholder, the health insurance number as a personal identification number, an identification number of the CI, an identification number of the card, and the card’s expiry date.

The introduction of the EHIC with visible data marks the first stage of a process leading to the use of an electronic medium, such as a microchip or magnetic strip, to prove entitlement to benefits in kind during a temporary stay in a MS other than the competent one or the state of residence. The CIs of the MSs may incorporate the data referred to in this recital on an electronic medium from the initial stage onwards.

In exceptional circumstances where the issuing of an EHIC is prevented, a Provisional Replacement Certificate (PRC), in accordance with a uniform model, shall be issued.

The design and specifications of the EHIC are established in annex I to [14], and the model of the PRC is established in accordance with annex II to this Decision. This Decision applies from the date of entry into force of [4]. However, there are some variations in the issuance formats across EU MSs:

- □ **Digital EHIC**: In France and Belgium the EHIC is issued in digital form (as an image of the plastic card) in certain situations. This is considered as an electronic representation rather than a digital one, which would allow processing of the contained data (attributes).

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

- **Standalone EHIC**: Eight countries (Denmark, France, Ireland, Latvia, Poland, Portugal, Spain, and Sweden) issue standalone EHIC cards, which are distinct from the national health insurance cards (in case those exist).
- **Incorporated EHIC**: Austria, Czechia, Germany, and Switzerland incorporate the EHIC as part of their national health insurance cards, embedding the EHIC's functionality within the national card.
- **Combination Format**: Finland and the Netherlands offer a combination of both standalone and incorporated EHIC formats, allowing citizens to choose between the two options when applying for an EHIC or the format is determined based on the person's status.

The validity period of an EHIC varies from country to country and/or from issuer to issuer and is determined by a combination of factors:

- **National Regulations**: The validity period is primarily defined by the national legislation in each EU MS.
- **Issuing Institution's Policies**: The issuing institutions, typically social security authorities or designated agencies, may have specific policies regarding the validity period.
- **Target Group:** The validity period may vary based on the specific group of individuals eligible for the EHIC, such as pensioners, children, or students.
- **Comparison to National Card:** The EHIC's validity period may differ from the validity period of the national health insurance card issued in the home country.
- **Person Group Changes:** In most EU MSs, a change in person group, such as transitioning from a child to an adult or becoming eligible for a pension, does not affect the validity of the EHIC.

2.4.1.3. Central Repositories for PINs

Regarding the storage of Personal Identification Numbers (PINs), most EU MSs maintain a centralised national database to store and manage PIN information. Thirteen countries (Austria, Switzerland, Czechia, Denmark, Estonia, Finland, France, Ireland, Latvia, Netherlands, Poland, Portugal, and Sweden) confirmed the presence of such a database, while Germany is the only exception.

When the PIN, that is present on the EHIC, differs from the PIN associated with the national health insurance card, several countries have implemented dedicated national databases to store and manage PIN information specific to the EHIC. These countries include Spain, Switzerland, France, and Portugal. Four countries – Denmark, Ireland, Netherlands, and Sweden – indicated that they do not have a dedicated database for the PINs indicated on the EHIC.

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

2.4.1.4. Provisional Replacement Certificate (PRC)

The PRC serves as a temporary replacement for the EHIC when the EHIC is lost or unavailable. The requirements for obtaining a PRC are essentially identical to those for obtaining an EHIC, apart from Austria, where an insurance period is not required. Key differences between the PRC and EHIC include:

- **Temporary Use:** The PRC is intended for short-term use, unlike the EHIC, which can be used for longer periods.
- **Issuing institution**: Issuers are the same for PRC and national card (except for Austria, Portugal, and Spain).
- **Manual Process:** PRC requests are typically handled manually, unlike EHIC applications, which can often be processed electronically.
- **Paper Format:** PRCs are issued either in paper format or PDF rather than as a plastic card like the EHIC. In case of PRC an electronic format (PDF) is allowed according to Recommendation H2. [9]

2.4.2. Issuance Process of the EHIC & PRC

EHIC and PRC Issuance Across EU MSs

The issuance of EHICs and PRCs varies among EU MSs due to country-specific policies and procedures. However, some common practices can be identified.

EHIC Issuance Methods

Integrated into National Card: In countries where the EHIC is integrated into the national card, the EHIC is issued simultaneously with the national card. Both initial and subsequent issuances occur automatically.
Standalone EHIC Cards: The EHIC is issued only upon request in seven countries (Denmark, France, Latvia, Poland, Portugal, Spain, and Sweden) For Finland and Ireland the initial issuance occurs upon application, and subsequent issuances are automatic.

EHIC Issuance based on Initial or Subsequent Issuance

- Initial Issuance:
  - **Automatic Issuance**: Triggered by the birth of a person or registration of a new citizen in the MS. All MS incorporating EHIC as part of their national card experience automatic initial issuance. EHICs are sent via mail after issuance.
  - **Issuance upon Request**: Insured individuals can apply for an EHIC through various channels such as online, phone, email, or in-person. In-person applications result in direct card issuance if feasible; otherwise, the card is sent via mail.
- Re-Issuance:
  - **Automatic Re-Issuance**: MS with EHIC as part of their national card experience automatic re-issuance. Some MS with standalone EHIC also undergo automatic re-issuance. EHICs are sent via mail after re-issuance.
  - **Re-Issuance upon Application**: Most MS with standalone EHIC facilitate re-issuance upon application. Re-issuance is required for loss/theft, changes in insured person data, changes in insurance, and expiration of validity. Application for re-issuance is possible through phone, email, electronic platforms, or in-person. In-person applications result in direct card issuance if feasible; otherwise, the card is sent via mail.

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

Revocation/Deactivation

Deactivation/Revocation occurs exclusively in national registries/databases. Central revocation is not possible; cards in circulation cannot be centrally declared as “invalid.”

PRC Issuance

PRCs are issued similarly to EHICs:

- **Issuance before stay abroad**: In certain MSs, there is no issuance of PRCs in advance. PRCs are exclusively issued upon request, which can be done through various channels such as online, phone, email, or in-person. PRCs are issued specifically for the duration of the stay, with the duration being specified during the application process. PRCs are consistently issued in paper format, or in PDF if they are sent digitally. In urgent cases (when an EHIC request would take too long), PRCs may be issued.
- **Issuance during stay abroad**: PRCs are only issued upon request, facilitated through online, phone, email, in-person, or within EESSI (S_BUC_05). Similarly to pre-stay issuance, PRCs are issued for the specific duration of the stay, with the duration indicated during the application. PRCs are predominantly issued in PDF format, especially when transmitted digitally. Usually, the PRC is requested by the citizen, but in some rare cases, like emergency cases, the PRC can also be requested by the health care provider or an emergency agency on behalf of the citizen.

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

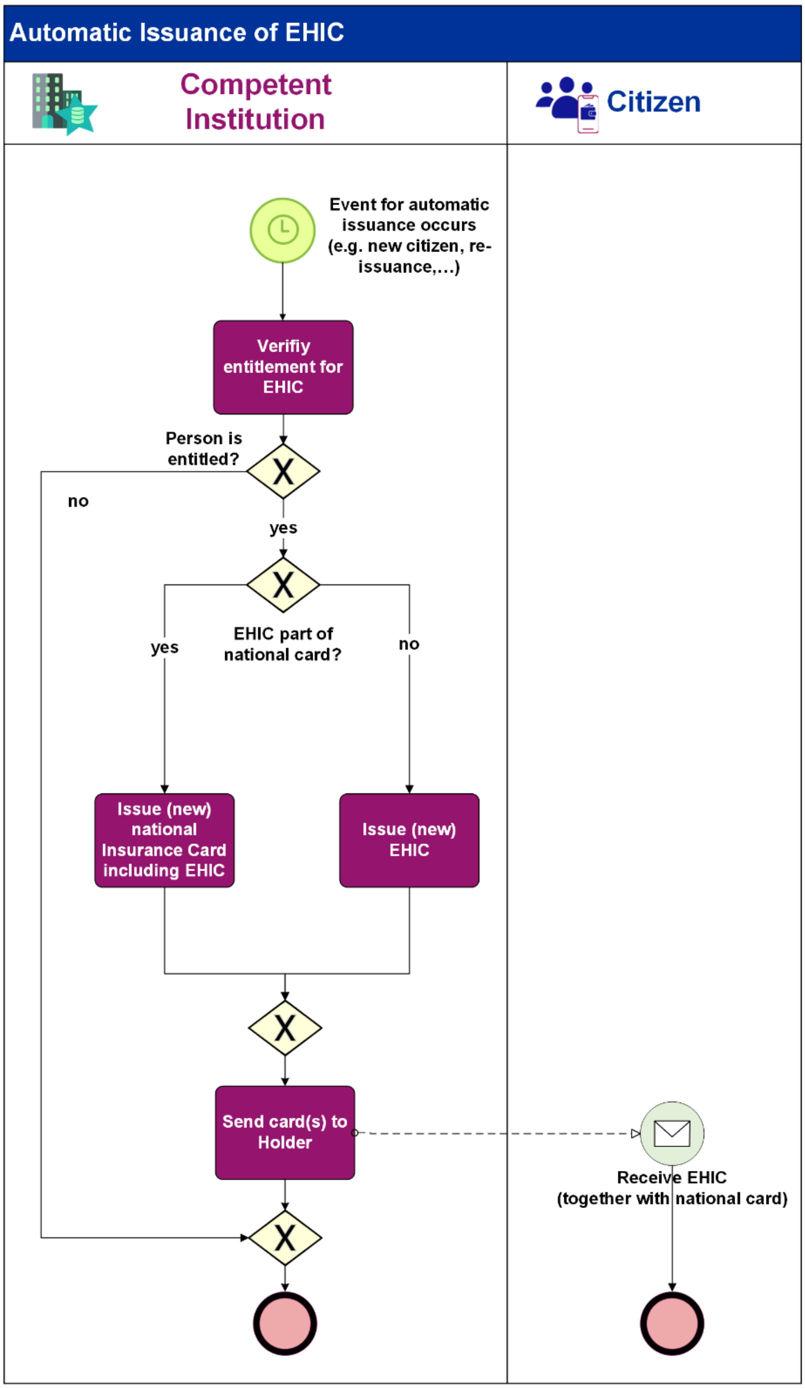

Automatic Issuance of EHIC
Competent Institution
Citizen
Event for automatic issuance occurs (e.g. new citizen, re-issuance,...)
Verifiy entitlement for EHIC
Person is entitled?
no
yes
EHIC part of national card?
yes
no
Issue (new) national Insurance Card including EHIC
Issue (new) EHIC
Send card(s) to Holder
Receive EHIC (together with national card)

FIGURE 6: AUTOMATIC ISSUANCE OF EHIC

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

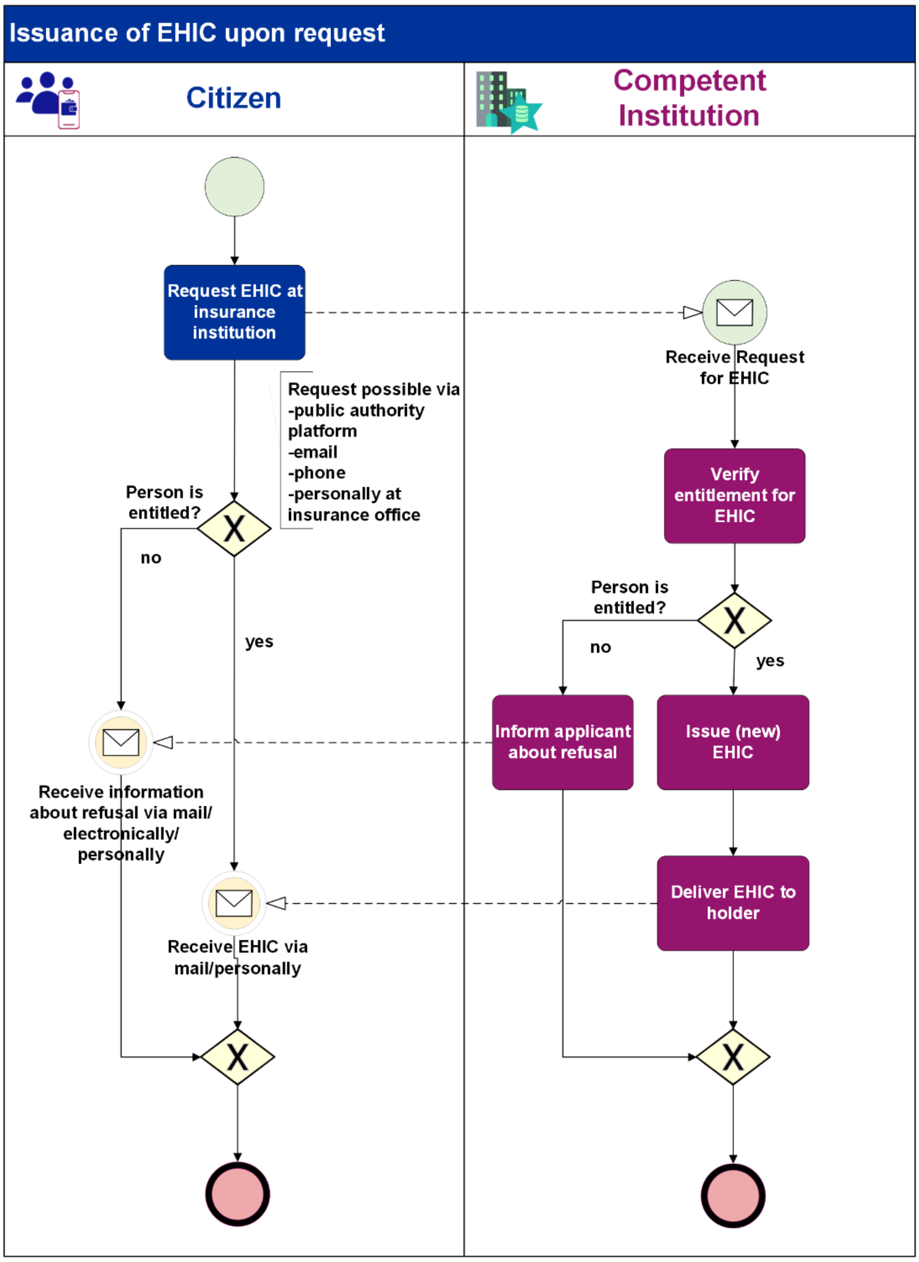

Issuance of EHIC upon request
Citizen
Competent Institution
Request EHIC at insurance institution
Request possible via
-public authority platform
-email
-phone
-personally at insurance office
Person is entitled?
no
yes
Receive information about refusal via mail/ electronically/ personally
Receive EHIC via mail/personally
Receive Request for EHIC
Verify entitlement for EHIC
Person is entitled?
no
yes
Inform applicant about refusal
Issue (new) EHIC
Deliver EHIC to holder

FIGURE 7: ISSUANCE OF EHIC UPON REQUEST

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

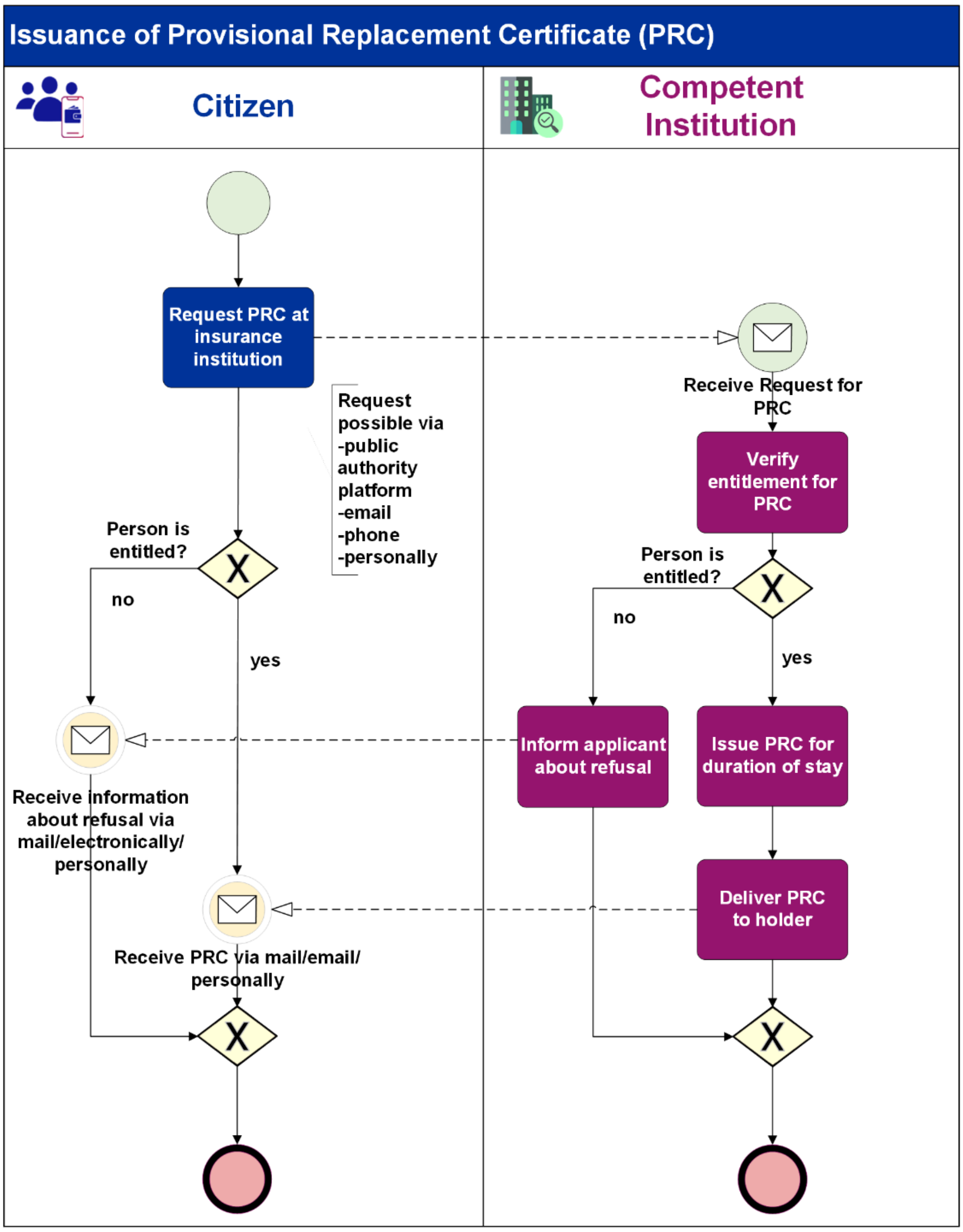

Issuance of Provisional Replacement Certificate (PRC)
Citizen
Competent Institution
Request PRC at insurance institution
Request possible via -public authority platform -email -phone -personally
Person is entitled?
no
yes
Receive information about refusal via mail/electronically/ personally
Receive PRC via mail/email/ personally
Receive Request for PRC
Verify entitlement for PRC
Person is entitled?
no
yes
Inform applicant about refusal
Issue PRC for duration of stay
Deliver PRC to holder

FIGURE 8: ISSUANCE OF PRC

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

2.4.3. Verification Process of the EHIC & PRC

The verification process typically involves the following steps:

- **Identity Verification:** The verifier is supposed to verify the identity of the individual by checking their ID card or passport to ensure it matches the information on the EHIC/PRC certificate.
- **Visual Inspection:** The verifier, which is embodied by the health care provider in the EHIC/PRC case, visually inspects the EHIC/PRC to check for authenticity, including the personal data, validity date etc.
- **Documentation of Validation Result:** The verifier documents and transfers relevant information from the EHIC/PRC verification to the health insurance institution in the place of temporary stay of the insured person. Usually, the healthcare provider copies the EHIC/PRC. They then send a copy of the EHIC/PRC along with the invoice to the health insurance institution in the place of residence or stay of the insured person. In some countries (e.g. France) this proof is used for receiving confirmation from the health insurance institution prior to the treatment.
- **Back-office processes for reimbursement**: Upon receiving the EHIC/PRC copy and invoice, the CI initiates the reimbursement process (via its Liaison Body) with the other CI (via their Liaison Body). This process includes recognising the healthcare services provided, calculating the associated costs, and reimbursing the healthcare provider.

If either the EHIC/PRC or the verification of EHIC/PRC against ID card/passport is unsuccessful, the healthcare provider informs the individual about the negative verification outcome.

EHIC acceptance is contingent on several factors, including validity, unplanned treatment, medical necessity, and temporary stay in the host country. Additionally, certain countries impose additional requirements: Denmark and Switzerland, due to the inapplicability of Regulation (EC) 1231/2010 [15] mandate EU citizenship, while France also requires EU citizenship. Furthermore, some countries such as Austria, Czechia, Denmark, France, Germany, Ireland, Netherlands, Poland, Spain, and Sweden necessitate the presentation of personal ID for EHIC/PRC verification.

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

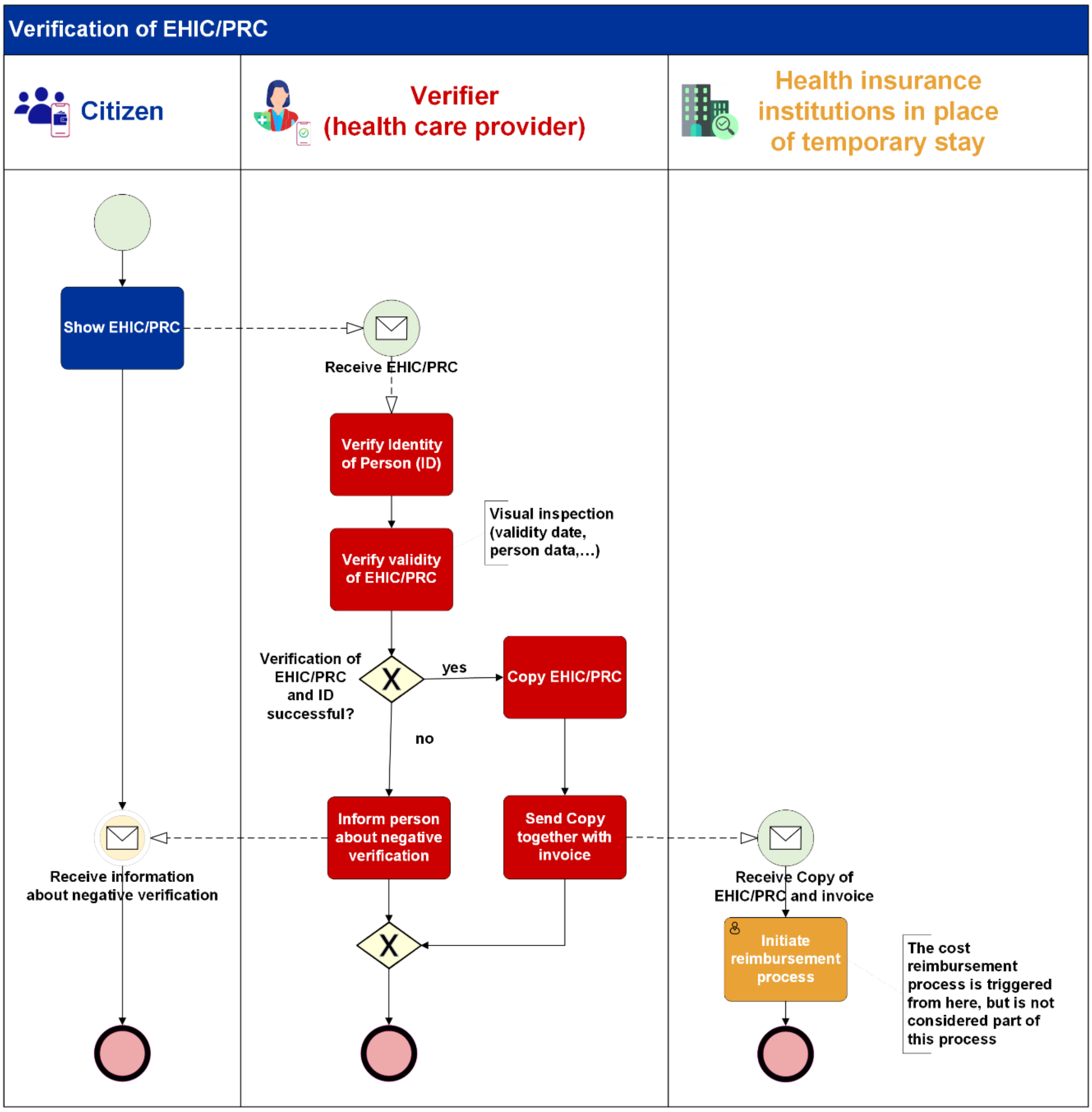

Verification of EHIC/PRC
Citizen
Verifier
(health care provider)
Health insurance institutions in place of temporary stay
Show EHIC/PRC
Receive EHIC/PRC
Verify Identity of Person (ID)
Visual inspection (validity date, person data,…)
Verify validity of EHIC/PRC
Verification of EHIC/PRC and ID successful?
yes
no
Copy EHIC/PRC
Inform person about negative verification
Send Copy together with invoice
Receive information about negative verification
Receive Copy of EHIC/PRC and invoice
Initiate reimbursement process
The cost reimbursement process is triggered from here, but is not considered part of this process

FIGURE 9: VERIFICATION OF EHIC/PRC

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

2.4.3.1. Documentation Process

Documentation of Identity Verification

Seven countries (Austria, Germany, France, Latvia, Poland, Spain, Sweden) mandate identity verification for EHIC/PRC usage. Five countries (Czechia, Denmark, Ireland, Netherlands, Portugal) allow for optional identity verification. No country has explicitly stated that identity verification is unnecessary. Regarding documentation of the identity verification process, six countries (Austria, Czechia, France, Latvia, Spain, Sweden) document the process, while four countries (Germany, Ireland, Netherlands, Poland) do not. The remaining one country (Denmark) did not provide a response.

Documentation of EHIC Verification

Thirteen countries (Austria, Switzerland, Czechia, Germany, Denmark, Finland, France, Ireland, Latvia, Netherlands, Poland, Spain, Sweden) document the verification of EHICs or PRCs. Spain and Portugal do not follow this practice. Typically, a copy of the EHIC or PRC is retained as evidence. In most cases, this documentation is stored and provided upon request. The duration for which these records are retained varies, with the most common approach being to store them until the completion of the cost settlement period.

2.4.3.2. Central Repository for EHIC/PRC Verifiers

Thirteen countries (Austria, Belgium, Czechia, Denmark, France, Germany, Ireland, Latvia, Netherlands, Poland, Portugal, Spain, Sweden) have confirmed the existence of a central national repository for healthcare providers. Finland did not provide any response.

These repositories contain information about healthcare providers who are accredited to accept EHICs and PRCs. This information is used to verify the eligibility of individuals to use their EHICs or PRCs when receiving healthcare services in another EU MS.

2.4.4. Onboarding Use Cases for EHIC

This subchapter outlines the existing onboarding processes for issuers and verifiers of EHICs (as-is). Chapter 7, Onboarding, addresses the proposed future processes for onboarding issuers and verifiers (to-be). Issuers are CIs qualified to issue EHICs. Verifiers, who are health care providers authorised at a national level, are responsible for validating EHICs. They are also required to initiate a reimbursement process for the services they provide.

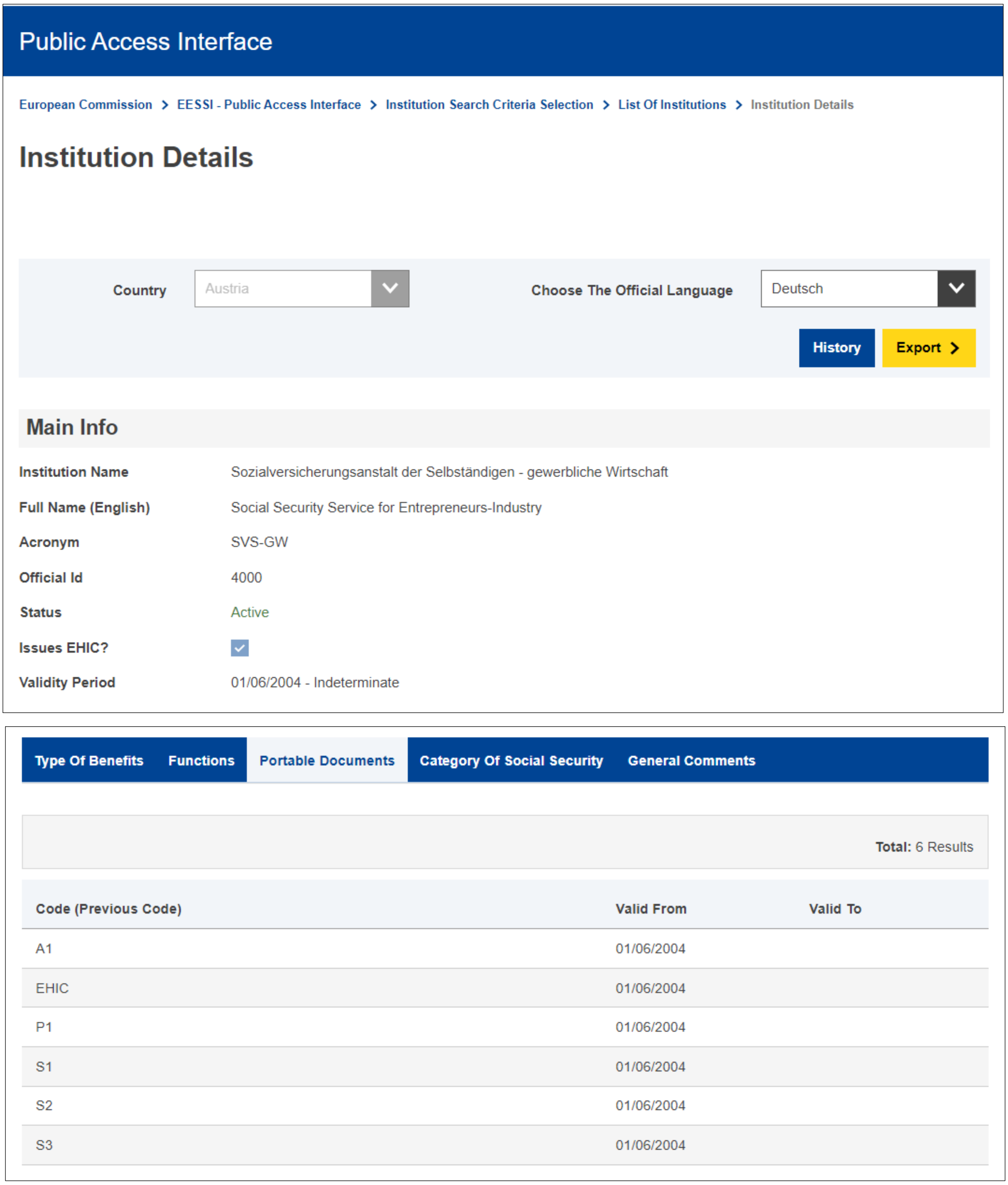
2.4.4.1. Onboarding Issuers

Onboarding of Issuers

In most MSs, there is currently no formal process for onboarding new issuers of EHICs and PRCs. This is due to the fact that there is a limited number of issuers, and the number of issuers has been relatively stable. The authorisation to issue EHICs and PRCs is primarily governed by national law. A new institution must be entered in the IR. If a completely new institution is added to the IR, a substantial change must be notified to the EC one month in advance. Whether an institution issues EHICs is listed in the IR under the “Main Info” and the section "Portable Documents". If an institution is qualified to issue EHICs (no matter if it is a newly added institution or an existing institution), no substantial change is necessary. The relevant portable document must be added to this section by the IR-SPOC.

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



Public Access Interface

European Commission > EESSI - Public Access Interface > Institution Search Criteria Selection > List Of Institutions > Institution Details

Institution Details

Country: Austria

Choose The Official Language: Deutsch

Main Info

Institution Name	Sozialversicherungsanstalt der Selbständigen - gewerbliche Wirtschaft
Full Name (English)	Social Security Service for Entrepreneurs-Industry
Acronym	SVS-GW
Official Id	4000
Status	Active
Issues EHIC?	☑
Validity Period	01/06/2004 - Indeterminate

Total: 6 Results

Code (Previous Code)	Valid From	Valid To
A1	01/06/2004	
EHIC	01/06/2004	
P1	01/06/2004	
S1	01/06/2004	
S2	01/06/2004	
S3	01/06/2004	

FIGURE 10: THE EESSI INSTITUTION REPOSITORY – PUBLIC ACCESS INTERFACE – ISSUER OF PORTABLE DOCUMENTS. SOURCE: [11]

Extension of Authorisation

Currently, there is no formal process for extending the authorisation of EHIC issuers. This is because the authorisation is typically granted for an unlimited period. However, in some cases, the national competent authority may need to review the eligibility of an issuer and decide whether to renew the authorisation.

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

Changes in Issuer Data

When there are changes in the name or identifier of an EHIC issuer, the issuer is required to update their records in national registries and the IR. This changes also must be notified to the EC by substantial change one month in advance and entered accordingly in the IR by the IR-SPOC to ensure that healthcare providers can access the correct information about the issuer. In some cases, the national competent authority may need to be informed or approve the changes. New EHICs may need to be issued if the issuer's name or identifier is changed.

Merger of Issuers

When two or more EHIC issuers merge, the merged entity is required to update its records in national registries and the IR. If two or more institutions in a country are merged, this must be notified to the EC by substantial change one month in advance and entered accordingly in the IR by the IR-SPOC. In some cases, the merger may need to be authorised by a supervisory body. New EHICs may need to be issued to reflect the merger. Agreements can be made to allow old cards to remain valid until they are replaced.

Deactivation of Issuers

When an EHIC issuer ceases to operate, the issuer is required to deregister from national registries and the IR. The deactivation of an institution must be notified to the EC one month in advance by substantial change. Furthermore, a successor institution must be notified and entered in the IR by the IR-SPOC to take over responsibility for issuing EHICs to insured persons who were previously covered by the deactivated issuer. Insured persons may need to cancel or change their health insurance coverage themselves. New EHICs will be issued by the new issuer. Agreements can be made to allow a transition period during which insured persons are still treated as holding the card of the deactivated issuer.

Steps for IR Maintenance

When changes to issuer data or other aspects of the EHIC system occur, the national competent authority informs the IR-SPOC. The SPOC promptly performs the required changes in the IR in accordance with [10].

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

2.4.4.2. Onboarding Verifiers

Onboarding of Verifiers

Onboarding new verifiers involves registering them in national registries and establishing a contractual relationship with insurance institutions. A national legal framework governs their operations, ensuring adherence to regulatory standards. The current onboarding process covers only the registration of verification bodies (i.e. health care providers) rather than registering individual clerks.

Extension of Authorisation

In most MS, there is no formal process for extending authorisation for verifiers as the authorisation period is typically unlimited. Renewal of contracts applies to expired authorisations.

Changes in Verifier Data

Regular updates to national registries with verifier data are essential. In some cases, changes may require approval from a supervisory authority. Existing contracts may need adjustments to reflect these changes.

Merger of Verifiers

Upon merging, national registries must be updated to reflect the new entity. In some cases, changes may require approval from a supervisory authority, and existing contracts may need adjustments.

Deactivation of Verifiers

Deactivation of verifiers involves revoking their license, removing them from national registries, and terminating their contractual relationships with all insurance institutions.

Maintaining the National Repository

Responsibilities for maintaining national repositories vary among MS. In Germany, each Federal State is responsible for updating their registry.

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. BASIC REQUIREMENTS

3.1. INTRODUCTION

DC4EU WP 6 aims to create a sustainable solution for the attestation of attributes for social security coordination within a cross border context. The requirements for this solution are primarily sourced from the social security coordination business processes which will be transformed into a digital equivalent. This means that the requirements must be integrated into the eIDAS ecosystem, which is based on the new eIDAS 2.0 regulation.

The **eIDAS 2.0** regulation is an enhanced framework that aims to augment the effectiveness of the original eIDAS. A core aspect of this regulation is the implementation of European Digital Identity Wallets (EUDIW) which allows citizens and businesses to authenticate online and share their digital attributes across the EU. Such a wallet is defined as

> *"European Digital Identity Wallet' means an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals;" ([1] Art. 3, Paragraph 42, Letter j)*

Additionally, this is based on the provision of a digital identity with Level of Assurance (LoA) high, which must be accepted by all member states (MSs) of the EU.

The eIDAS 2.0 is underpinned by several key principles which strive to foster a 'high' level of trust in digital transactions across Europe (see also chapters 1.2 and 1.3). They can be summarised as follows:

EUDIW Onboarded with Base Identity (PID): The EUDIW is a digital wallet that provides a secure and user-friendly platform for European citizens and businesses to share necessary identity data for accessing digital services. The basic identity, which creates a digital identity of a citizen with LoA 'high', is provided by PID providers. These are trusted entities in this EUDIW ecosystem, responsible for verifying the identity of the EUDIW holder, and providing this digital identity for an owner of an EUDIW.

Trust Framework: The eIDAS 2.0 regulation provides a robust trust framework, ensuring that both public and private services can rely on trusted and secure digital identity solutions. It also guarantees that these solutions are linked to a diverse set of attributes, allowing for targeted sharing of identity data based on the specific needs of the requested service.

Secure Authentication and Proof of Legitimate Possession (Citizen): The EUDIW empower individuals to select, monitor, and control their identity, data, and (lawful owned) attestations that they share with third parties. In the context of social security, "legitimate possession" refers to the attestation of attributes issued to a digital identity with a 'high' LoA. These attestations are then used by the same digital identity or on behalf of this identity in a verification challenge.

Basic Processes: The core processes in the eIDAS 2.0 ecosystem revolve around the issuance and verification of digital identities and credentials. The ability to change and check the validity of a digital identity and its associated credentials plays a significant role.

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

Social Security Requirements: The eIDAS 2.0 and the EUDIW Toolbox are designed with flexibility and adaptability at its core, catering to a variety of requirements, including those specific to social security. However, the compatibility with social security systems would depend on the specific requirements of each system.

Technology Agnostic: eIDAS 2.0 and the EUDIW Toolbox are both technology-agnostic. They are designed to accommodate a broad spectrum of existing technologies while remaining receptive to future technological advancements. This approach helps to avoid the pitfalls associated with vendor lock-in and similar issues.

Offline Capabilities: The EUDIW is engineered to function offline. It can interface with devices for local storage and leverage offline communication channels such as Bluetooth Low Energy (BLE), WIFI Aware, and Near Field Communication (NFC).

Transferability: In the eIDAS 2.0 ecosystem, transferability is about putting the freedom of the citizen at the centre so that they have full control over to whom digital identities and credentials are presented or transferred. The EUDIW Toolbox must support this capability.

Selective Disclosure: The EUDIW supports selective disclosure, empowering users to control which parts (full or partial) of their identity or credential data they choose to share.

Identity Mapping: In the eIDAS 2.0 ecosystem, the role of identity mapping involves the identification and verification of the EUDIW holder’s identity and the secure and correct provision of digital attestations to that holder.

In the following, the basic concepts and requirements will be further explained.

3.2. GENERAL PRINCIPLES

There are overarching principles that must be considered for creating our solution:

3.2.1. Data Minimisation

An important advancement as compared to paper-based processes is the possibility to reduce data to the minimum required in every situation. To achieve this, first the information an attestation holds needs to be reduced to a reasonable set that is required.

In addition to this, the concept of selective disclosure is introduced. This is defined by eIDAS 2.0 as follows [1]:

> *“Selective disclosure is a concept empowering the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only such information as is necessary for the provision of a service requested by a user. The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. It should be technically possible for the user to selectively disclose attributes, including from multiple, distinct electronic attestations, and to combine and present them seamlessly to relying parties. This feature should become a basic design feature of European Digital Identity Wallets, thereby reinforcing convenience and the protection of personal data, including data minimisation.” (Preamble 59)*

Selective disclosure enables the possibility to present only a subset/reduced version of an attestation. Such a subset may be already requested by a relying party/Verifier. To enable this

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

capability, a consistent data model that aligns with the specified requirements serves as the foundational element.

An additional benefit is that an authentic source may only present/provide attestations of data points under their quality control while other data points may be acquired from various sources. In the long term, all data points shall only be provided and attested by an authentic source which has maximum assurance about this data. A credential like PD A1 would then be a combination of many separate attestations/credentials providing the maximum LoA for each data point.

By combining a credential like EHIC with the wallet as eID means (PID) in both the offline and online scenario, there even is no need to include identity data endpoints within the individual credential. This approach aligns with the principle of data minimisation, ensuring that only necessary data is included in the credentials. It also enhances privacy, as the user's identity data is not exposed every time a credential is shared. Instead, the PID represents the user's identity in the EUDIW ecosystem. It is a pillar of the single digital market for authentication and identification, and it adds capabilities and trust into the system. This makes digital solutions more efficient, secure, privacy-preserving, and trustworthy.

While selective disclosure with regards to data minimisation is regarded as a huge advancement, the specifics and extend of its use need to be further explored and will be addressed in future versions of the EUDIW Toolbox.

> *Any request by the relying party for information from the user of a European Digital Identity Wallet should be necessary for, and proportionate to, the intended use in a given case, should be in line with the principle of data minimisation and should ensure transparency as regards which data is shared and for what purposes. ([1], Preamble 56)*

For Relying Parties that cannot prove their permission, but also all other scenarios, the citizen may decide on their own what minimum data needs to be shared. This possibility to control data sharing is another important concept covered in the following chapter.

3.2.2. Self-Sovereignty

Self-Sovereignty is a term that is used in the DC4EU project to describe an important design concept, based on eIDAS 2.0. This concept aims, firstly, to enable transparency and secondly, to provide citizens with extensive control over their data at any time.

There are multiple paragraphs in the new regulation that address these goals.

> *"European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to: […] securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;" ([1], Art.5a, Paragraph 4, Letter c)*

By this generic definition it is evident that a user should be able to share and receive every attestation, including identity, between every EUDIW therefore also with other users. Nevertheless, through this definition it is not apparent what is meant by share and receive for example in regards of whether it is temporary or permanent. Specifics like this will be clarified

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

in future implementing acts (technical and regulatory details as announced in eIDAS 2.0) and the EUDIW Toolbox. Yet, the functionality needs to be secure, transparent, and traceable to prevent misuse and to help the user to comprehend all actions even in retrospect. One approach [1] to this is a monitoring dashboard as part of the wallet:

> *“[…] common dashboard embedded into the design, in order to ensure a higher degree of transparency, privacy and control of the users over their personal data. That function should provide an easy, user-friendly interface with an overview of all relying parties with whom the user shares data, including attributes, and the type of data shared with each relying party.” (Preamble 13)*

Other aspects of the regulation concern this concept but shall be out of scope such as the use of pseudonyms:

> *“Reliance on the legal identity should not hinder European Digital Identity Wallet users to access services under a pseudonym, where there is no legal requirement for legal identity for authentication.” (Preamble. 19)*

Pseudonyms are disregarded for Social Security Use Cases since real identities are required according to regulations and national law.

3.2.3. Non-Traceability

> *“The technical framework of the European Digital Identity Wallet shall: not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user;” ([1], Art. 5a, Paragraph 16, Letter a)*
>
> *“[…] enable privacy preserving techniques which ensure unlinkability, where the attestation of attributes does not require the identification of the user.” ([1], Art. 5a, Paragraph 16, Letter b)*
>
> *“[…] not provide any information to trust service providers of electronic attestations of attributes about the use of those electronic attestations;” ([1], Art. 5a, Paragraph 5, Letter b)*

In addition, privacy-preserving technologies like zero knowledge proofs shall be considered. This technology allows a relying party to validate that a given statement based on the person’s identification data and attestation of attributes is true, without revealing any data this statement is based on, thereby ensuring the privacy of the user. In terms of social security an example of zero knowledge proof is whether the attestation is valid in a specific country or not (yes or no) without any other information to be presented.

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

3.2.4. Data Protection

[16] **General Data Protection Regulation (GDPR)** applies to the processing of personal data. The credentials and personal attributes necessary for identity verification (authentication) are considered personal data under the scope of the GDPR. Data Protection is therefore an important topic in the scope of the EUDIW. This becomes especially apparent as many core principles of GDPR are indirectly addressed in the eIDAS 2.0 regulation.

For the **protection of personal data and the privacy of data subjects**, the GDPR states six principles that aim to safeguard the fundamental rights of natural persons:

- **Lawfulness, fairness, and transparency**: Personal data should always be processed in a transparent, fair, and lawful manner in relation to the data subject.
- **Purpose limitation**: The personal data should be collected for legitimate purposes that are explicit and specified and should not be reused or further processed than consented.
- **Data minimisation**: Only personal data that is necessary, relevant, and adequate should be processed. Unnecessary data should not be collected.
- **Accuracy:** Personal data should be accurate and kept up to date when necessary. Reasonable steps should be taken to correct or erase incorrect data.
- **Integrity and confidentiality**: Data that identifies data subjects, should not be stored for longer than what is necessary. Personal data may be stored for longer periods, as long as it is in accordance with Article 89(1) of the GDPR.
- **Accountability:** Personal data should be processed securely using appropriate organisational and technical measures. It should be protected from unauthorised or unlawful access, as well as accidental loss, damage, or destruction.

The principles need to be considered in any interaction with personal data during issuing, operation, and verification. The previous chapters show how eIDAS 2.0 supplements these principles to comply the specific needs of the EUDIW Use Cases. As it covers specific personal data processing operations its regulations take precedence over GDPR. These are the personal data processing operations such as the creation, verification and validation, preservation and management of electronic signatures, seals, timestamps, and certificates. It also includes archiving electronic documents, which can include personal data.

For piloting or testing that involves natural persons instead of mock data, these persons must be notified of how their data will be used, processed, and stored, for any use case.

They must be rightfully informed of data collection in accordance with the GDPR. Besides information regarding data collection, a request for consent should be sent to the data subject in due course. Consent mechanisms should be implemented to allow for data subjects in pilots or tests to easily provide and withdraw their consent as required by the GDPR.

Consent is only valid when the obtained consent is freely given, specific, informed, and unambiguous.

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

3.3. PERSONAL IDENTITY DATA

The key factor of the European Digital Identity Framework is a secure and reliable authentication and identification of citizens using the EUDIW ecosystem. For DC4EU – social security coordination only natural persons are in scope:

> *“ […] The European Digital Identity Wallet should provide natural and legal persons across the Union with a harmonised electronic identification means enabling authentication and the sharing of data linked to their identity.” ([1], Preamble 7)*
>
> *“European Digital Identity Wallets shall be provided under an electronic identification scheme with assurance level high.” ([1], Art. 5a, Paragraph 11)*
>
> *“When acting as relying parties for cross-border services, Member States shall ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets.” ([1], Art. 11a, Paragraph 1)*
>
> *“This Regulation lays down an obligation for qualified trust service providers to verify the identity of a natural or legal person to whom the qualified certificate or the qualified electronic attestation of attribute is issued based on various harmonised methods across the Union.” ([1], Preamble74)*

The main function of the EUDIW is therefore being an electronic identification means – it must be “on-boarded” with a “strong” identity. This on-boarding

> *“[…] should be facilitated by relying on electronic identification means issued at assurance level high.” ([1], Preamble 28)*
>
> *“Electronic identification means issued at assurance level substantial should be relied upon only where harmonised technical specifications and procedures using electronic identification means issued at assurance level substantial in combination with supplementary means of identity verification will allow the fulfilment of the requirements set out in this Regulation as regards assurance level high.” ([1], Preamble 28)*

The base identity in the EUDIW ecosystem is called “Person Identification Data” (PID). The PID is provided to the EUDIW in a harmonised common format by trusted entities responsible for verifying the identity of the EUDIW holder. The **PID is designed to represent identity** in a way that supports the goals of the European Union (EU), including interoperability, compliance with EU regulations, provision of cross-border services, establishment of a trust framework, and facilitation of EU-wide **digital identity verification with LoA ‘high’**.

> *“Cross-border reliance on European Digital Identity Wallets:*
> *Where Member States require electronic identification and authentication to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets that are provided in accordance with this Regulation.” ([1], Art 5f; Paragraph 1)*

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

In more detail, the PID is defined as

> *"[…] person identification data' means a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person." ([1], Art. 3a; Paragraph 3)*

A PID is issued by a (Qualified) Trust Service Provider ((Q)TSP), based on national processes and specifics. These PID Providers are trusted entities responsible to verify the identity of the EUDIW holder in compliance with LoA 'high' requirements. The PID Providers may e.g., be the same organisations that today issue official IDs, electronic identity means, or also the EUDIW Providers themselves. It must be ensured that a PID

> *"[…] uniquely represents the natural person, legal person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet;" ([1], Art. 5a; Paragraph 5, Letter f)*

Attestation of attributes for a citizen must be issued to a digital identity which is identified with LoA "high".

> *"[…] All Union citizens, and residents in the Union as defined by national law, should be empowered to securely request, select, combine, store, delete, share and present data related to their identity and request the erasure of their personal data in a user friendly and convenient way, under the sole control of the user, while enabling selective disclosure of personal data." ([1], Preamble 15)*
>
> *"Public service providers use the person identification data available from electronic identification means pursuant to Regulation (EU) No 910/2014 to match the electronic identity of the users from other Member States with the person identification data provided to those users in the Member State performing the cross-border identity matching process." ([1], Preamble 41)*
>
> *"When acting as relying parties for cross-border services, Member States shall ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets." ([1], Art. 11a; Paragraph 1)*
>
> *"To ensure that qualified certificates and qualified electronic attestations of attributes are issued to the person to whom they belong and that they attest the correct and unique set of data representing the identity of that person, qualified trust service providers issuing qualified certificates or issuing qualified electronic attestations of attributes should, at the moment of the issuance of those certificates and attestations, ensure with complete certainty the identification of that person." ([1], Preamble 74)*

Regarding the abovementioned data minimisation principle, eIDAS 2.0 also speaks about the

> *"[…] a reference to a minimum set of person identification data necessary to uniquely represent a natural or legal person, or a natural person representing another natural person or a legal person, which is available from electronic identification schemes;" ([1], Art 12, Letter c)*

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 following mandatory attributes are proposed (Annex VI) [1]:

- *Current Family Name*
- *Current First Names*
- *Date of Birth*

Additionally, there are also optional/possible additional attributes mentioned that can be applied on behalf of each MSs decision:

- *Name(s) at Birth*
- *Place of Birth*
- *Current Address*
- *Gender*
- *Nationality*
- *Optional attributes used at national level, e.g. tax number, social security number etc.*

In addition to these attributes, it is required that a PID contains metadata like the dates of issuance/expiration and information about the issuing authority (PID provider). The possibility of whether the PID can contain a portrait (relevant for face-to-face validation) is currently under discussion.

According to the eIDAS regulation digital attestation of attributes issued by public bodies must fulfil the following requirements ([1], Annex V a) for the data model:

REQUIREMENTS FOR ELECTRONIC ATTESTATION OF ATTRIBUTES ISSUED BY OR ON BEHALF OF APUBLIC SECTOR BODY RESPONSIBLE FOR AN AUTHENTIC SOURCE
An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall meet the following requirements: *(* *(a) those set out in Annex VII;* *(b) the qualified certificate supporting the qualified electronic signature or qualified electronic seal of the public sector body referred to in Article 3, point (46), identified as the issuer referred to in point (b), of Annex VII, containing a specific set of certified attributes in a form suitable for automated processing and:* *(i) indicating that the issuing body is established in accordance with Union or national law as the responsible for the authentic source on the basis of which the electronic attestation of attributes is issued or as the body designated to act on its behalf;* *(ii) providing a set of data unambiguously representing the authentic source referred to in point (i); and* *(iii) identifying the Union or national law referred to in point (i).*

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

3.4. TRUST FRAMEWORK

One of the main goals of eIDAS 2.0 is to create services

> *"[...] relying on an improved ecosystem for trust services and on verified proofs of identity" ([1], Preamble 7)*

For this, a "Trust Framework" must be designed and implemented – every actor has to be able to trust the relevant aspects of the interactions.

3.4.1. Relevant Roles

The part of the Trust Framework which covers the citizens (EUDIW providers, Conformity Assessment Bodies (CAB), PID providers etc.) is worked out on higher level and therefore out of scope for this work package – based on that, Social Security Issuers and Verifiers must be able to perform basic checks to validate the citizens.

More directly relevant for this work package is the requirement to create and implement Trust Frameworks for Credential Issuers and Verifiers (to be validated by citizens). Regarding this part the following roles are relevant (see also chapter 1.2):

- **Authentic Source:** "A repository or system, held under the responsibility of a public sector body or private entity that contains attributes about a natural or legal person and is considered to be the primary source of that information or recognised as authentic in national law."
- **Issuer:** "A Person Identification Data Provider issuing PID or a (Qualified) Trust Service Provider issuing (Q)EAA. In the case of the EUDIW there may be multiple Providers for PID and (Q)EAA."
- **National Accreditation Bodies** (NAB): "National Accreditation Bodies (NAB) under [17] are the bodies in member states that perform accreditation with authority derived from the State."
- **Attestation Provider**: "It means any provider that is able to issue an attestation, it includes PID Provider EAA and QEAA provider."
- **Trust Service Provider** (TSP): "A natural or a legal person who provides one or more Trust Services, either as a qualified or as a non-qualified Trust Service Provider".
- **Relying Party:** "A natural or legal person that relies upon an electronic identification or a Trust Service."
- **Verifier:** "A role an entity performs by receiving one or more VCs inside a Verifiable Presentation (VP) for processing. Other specifications might refer to this concept as a Relying Party."

> *"Member States may require the supervisory body designated pursuant to paragraph 1 to establish, maintain and update a trust infrastructure in accordance with national law." ([1], Art 46b, Paragraph 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

3.4.2. Relying Parties

A relevant point is the new focus on “mutual authentication” of actors – which means not only an authentication between the citizen and a credential issuer, but in general also the authentication of all relying parties (and therefore also verifiers) towards the holder. It is important to mention that in the credential issuing process the issuing institution is also a relying party – as it requests, obtains, and verifies the citizen’s or holder’s person identity data. In a verification situation, the holder must be able to check if the verifier is allowed to conduct the requested verification process: “*Where relying parties intend to rely upon European Digital Identity Wallets issued in accordance with this Regulation, they shall identify themselves to the holder of the European Digital Identity Wallet*”. The Relying Parties need an authorisation to receive and verify data from a holder based on a corresponding registration – following the basic principles of data protection and data minimisation, the verifiers “*shall not request any data beyond what they have registered for*”.

The basic requirements for creating a Trust Framework for Relying Parties are outlined as follows:

> *“The registration process shall be cost-effective and proportionate-to-risk. The relying party shall provide at least: (Art. 5b, Paragraph 2)*
>
> *“Member States shall, without undue delay, notify to the Commission the names, addresses and accreditation details of the conformity assessment bodies referred to in paragraph 1 and any subsequent changes thereto. The Commission shall make that information available to all Member States;” ([1], Art. 20, Paragraph 1b)*
>
> *“The registration process shall be cost-effective and proportionate-to-risk.” ([1], Art. 5b, Paragraph 2)“Member States shall make the information referred to in paragraph 2 publicly available online in electronically signed or sealed form suitable for automated processing.” ([1], Art. 5b, Paragraph 5).*

3.4.3. Credential Issuers

It must be ensured that the source of the credential is or acts on behalf of an authentic source. In this context, a list of valid issuers for a specific credential type is needed. Regarding the issuing of credentials, eIDAS 2.0 states three types of credential providers which must be considered and chosen accordingly for an Issuer Trust Framework: Besides EAA and QEAA providers, the new type of *“electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source”* (Art. 45f) is introduced. The basic principles are:

> *“The Member State where public sector bodies referred to in Article 3, point (46), are established shall ensure that the public sector bodies that issue electronic attestations of attributes meet a level of reliability and trustworthiness equivalent to qualified trust service providers in accordance with Article 24.” ([1], Art. 45f; Paragraph 2)*
>
> *“Member States shall notify public sector bodies referred to in Article 3, point (46), to the Commission. That notification shall include a conformity assessment report issued by a conformity assessment body confirming that the requirements set out in paragraphs 1, 2 and 6 of this Article are met. The Commission shall make available to the public, through a secure channel, the list of public sector bodies referred to in Article 3, point*

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

> *(46), in electronically signed or sealed form suitable for automated processing." ([1], Art. 45f; Paragraph 3)*

3.4.4. Implementation Aspects

After the framework has been defined, the registrations shall be executed – in order to provide services in a trusted ecosystem with adequately onboarded actors. In the end, there must be a "*free-of-charge validation mechanisms*" for EUDIW holders to

> *"[…] allow users to verify the authenticity and validity of the identity of relying parties registered in accordance with Article 5b." ([1], Art. 5a; Paragraph 8, Letter b).*

- but also, such validation mechanisms for the other actors involved. The details are outlined in the following chapters.

3.5. SECURE AUTHENTICATION, CREDENTIAL ISSUANCE, AND USAGE

Regarding the processes of using an EUDIW for authentication, but also for the processes of issuance and usage of credentials, the following basic requirements must be met:

Identity Verification: Issuers of (Q)EAAs are obliged to verify the identity of the person to whom a credential will be issued. This includes a technical validation of the compliance of their EUDIW instance.

Authentication with PID: The PID serves as a key component for verifying the user's identity. It is issued by trusted entities and is used to authenticate the user's identity across various services in the EU.

In all situations of requesting a credential, including the PID, from a EUDIW holder.

> *"[…] in the case of the electronic attestation of attributes with embedded disclosure policies, implement the appropriate mechanism to inform the user that the relying party or the user of the European Digital Identity Wallet requesting that electronic attestation of attributes has the permission to access such attestation;" ([1], Art. 5a; Paragraph 5, Letter e)*

This is therefore required for issuers, acting as verifiers of a PID and verifiers in general.

Identity mapping: The different configurations of national PIDs must be considered in the user authentication part during the issuance process of other VCs – here the importance of "identity mapping" comes into place:

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

QEAA providers must "*ensure with **full certainty** the identification of that person*" (E36e). For this purpose, public service providers should

> *"[…] use the person identification data available from electronic identification means pursuant to Regulation (EU) No 910/2014 to match the electronic identity of the users from other Member States with the person identification data provided to those users in the Member State performing the cross-border identity matching process." ([1], Preamble 41)*

Because of the minimal data requirement for the PID, in many cases there are "*specific complementary unique identification procedures to be performed at national level*". MSs are therefore required

> *"[…] to take specific online measures to ensure unequivocal identity matching when users intend to access online crossborder public services." (Preamble 41)*

As a conclusion, identity mapping covers two aspects: First, the Authentication of EUDIW holder from other MSs, and second the mapping of this 'high-level', general identity to internal identifiers (e.g. a social security number).

Issuance and Linking of PID: Once the PID is authenticated and unambiguously mapped to an internal person identifier, it can be technically linked to various credentials, including the EHIC and PD A1. This option respects the user's privacy and ensures that the credentials are tied to a verified identity to increase trust and support future verification purposes. When a holder presents a digital credential and their PID, the Relying Party can in the optimal scenario verify both the authenticity of the credential and the identity of the holder in a single step. This simplifies the verification process and ensures that digital credentials are being presented by the rightful owner and thereby reduce the risk of fraud.

The issued credentials must be properly created and signed/sealed to enable citizens and relying parties to validate their authenticity and the issuer's/authentic source's authorisation to issue such a credential.

Processing of results: Finally, for the application of the use cases it must be considered that verification results may need to be processed and stored in internal systems to comply with regulations or perform additional steps (e.g. reimbursement). This plays a crucial role in the proper processing and completion of many use cases and is thus considered as a basic requirement.

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

3.6. ADDITIONAL REQUIREMENTS

The following additional requirements have to be considered:

3.6.1. Offline Usage

The eIDAS regulation states that the EUDIW can be used for

> *"[…] containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service; (Art. 3; Paragraph 2, Letter a)*

The offline use is described as

> *"[…] as regards the use of European Digital Identity Wallets, an interaction between a user and a third party at a physical location using close proximity technologies, whereby the European Digital Identity Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction." (Preamble 57)*

For social security, a need for such an offline verification use case combined with the wallet as an electronic identification means are relevant (see business processes in chapter 0).

3.6.2. Revocation

Revocation is a feature marking a significant advancement over traditional paper documents as it can be carried out in near real time and be effective from a specific point in time. According to the eIDAS regulation where

> *"[…] a qualified electronic attestation of attributes, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued." (Art. 24; Paragraph 1)*

Every (Q)EAA shall contain

> *"the information or location of the services that can be used to enquire about the validity status of the qualified attestation." ([1], Annex V, Letter i)*

implying that during any verification it shall be possible to retrieve the revocation status.

While the business decision to revoke a credential lies with the Authentic Source the subsequent technical revocation shall be conducted by the credential issuer (e.g. QTSP).

- It can be triggered by various alterations in the underlying conditions, such as a change in personal information or a citizen´s misconduct. Revocation ensures that the digital credentials accurately reflect the status at any point in time, maintaining their relevance and reliability.

Every status change must be transparently communicated to the user by the EUDIW, ensuring that it accurately processes changes in a credential's validity.

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

3.6.3. Flexibility

Following the self-sovereignty principle, eIDAS 2.0 has several passages about a “flexible” use of the EUDIW and the attestations in it – this covers many aspects like an extensive use of Selective Disclosure, the user’s right to “data portability”, or the use of different identities/pseudonyms.

Since the Social Security Use Cases mostly rely on highly regulated processes associated with an identity with a ‘high’ LoA, our approach to flexibility includes recommendations and basic functionalities.

3.6.4. Technical Neutrality

DC4EU WP 6 is agnostic towards the choice of technology. This is backed by the technical neutrality approach in eIDAS 2.0. Nevertheless, we require the new architecture to be a modern solution without media break considering aspects like performance, usability, interoperability, security, and privacy.

3.6.5. Other basic requirements not in scope

There are other requirements currently not in scope which may have an impact for social security coordination. Those requirements must be preliminary covered by basic EUDIW capabilities and the impact on the social security use cases must be considered at a certain stage:

- Special wallet features like a privacy dashboard (including the capability to request to a relying party to delete personal data according to GDPR).
- Usability measures for the EUDIW.
- Backup and restore of credentials.
- Special archiving solutions.
- Credential usage related to third countries.
- Special accessibility measures for the EUDIW.
- Alternative solutions for people opting not to use an EUDIW will be considered, but only on a conceptual basis.

Non-functional requirements concerning the handling e.g. of expired credentials as well as the digital identity (PID) during verification processes in another MS must be meticulously defined within the business domain. This is akin to the conventional paper-based system where regulations exist for scenarios such as not having an EHIC or PD A1 at hand, or the identification of the citizen is absent or invalid. It is incumbent upon the citizen to comply with these prerequisites, whether in the physical world or when opting for the digital alternative, the EUDI wallet solution. It is essential not to overlook the need for a valid digital identity during the verification process. This responsibility extends to ensuring that the identity remains valid, even during temporary stays abroad.

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

3.7. CONCLUSIONS FOR SOCIAL SECURITY

Overall, the goal of DC4EU WP 6 is to create a sustainable solution for Social Security based on the above-mentioned requirements. For the social security use cases, this means:

Data Modelling: The development of a consistent data model is instrumental in supporting various facets of social security processes. It is crucial to establish clear data standards across the entire business domain.

Data Minimisation: To address this aspect, DC4EU will propose lean data models together with a consistent use case design for the piloting activities. Additionally, we will clarify the role of digital identity (PID) and selective disclosure, which will be used to ensure and prove the correct usage of attestations in the EUDIW ecosystem.

Self-Sovereignty: We prioritise a citizen centric approach to empower possibilities of choice while balancing this with usability, social security requirements including the acceptance by all stakeholders, data minimisation and use case relevance.

Non-Traceability: This aspect will be considered in the conceptual architecture. The issuers of credentials must not receive information of the use of their credentials. The aspects of decentralisation may play a crucial role.

Data Protection: By the nature of the organisations and use cases in social security, the lawful processing of personal data is of utmost importance and must be considered in every step of the use case.

Using PID as Identification Means: In the social security context, the use of a digital identity with LoA “high” (PID) is crucial for citizens, issuers, and verifiers to authenticate and identify citizens in a secure and reliable way, in on- and offline scenarios. This includes the process of issuing as well as the proof of correct usage of an attestation in social security.

Trust Framework: The trust frameworks of eIDAS 2.0 and social security coordination must be mapped (e.g. authentic source = competent institution). This will be done in the trust framework design and in the corresponding onboarding processes (See chapter 0)

Secure Authentication, Issuance, and Usage of Credentials: In order to meet the requirements of eIDAS 2.0 and the toolbox process, more detailed aspects have to be considered in each step of the use cases (e.g. authentication LoA ‘high’, mutual authentication, proof of legitimate possession etc.).

Offline-Usage: The relevance of offline verification processes for digital credentials in social security coordination must be considered when designing the use cases.

Revocation: Revocation mechanisms play a crucial advancement for social security as for other use cases by increasing institutions’ capabilities and increasing reliability in credentials. The design needs to be considered with care as revocation shall not compromise data privacy requirements.

Flexibility: The basic impacts of the requirements of eIDAS/ EUDIW Toolbox (e.g. delegation of credentials) must be analysed and considered for a user-friendly, privacy preserving and secure solution.

Technical Neutrality: DC4EU WP6 is agnostic to technology, but requires a modern, future proof solution in accordance with the eIDAS approach. Specific Use Cases and requirements of social security shall be feasible with the technology with the fewest possible compromises.

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

Social Security regulation: The new solution must fulfil **social security coordination regulations** and grant **compatibility with back office processes –** the latter one means that the processes and data models have to be designed in a way that they support established further processes (like the settlement process between MSs for EHIC).

In conclusion, the above-mentioned requirements correspond to the endeavours of WP 6 social security and need to be applied in the concrete solution design. The following chapters can be perceived as first approach accordingly while decisions and specifications outside this work package and consortium will affect technical and lawful feasibility. In addition, national decisions (e.g. on the PID and QTSPs) must be carefully monitored in future iterations of the project.

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. CONCEPTUAL ARCHITECTURE

4.1. INTRODUCTION

The **European Union Digital Identity Wallet (EUDIW)** ecosystem is a ground-breaking approach to digital identity in Europe. Its conceptual architecture is designed to streamline identity verification processes, fostering trust and convenience in digital transactions.

The EUDIW is a digital application that enables European citizens and businesses to store and share identity data and attestation of attributes. In social security coordination these attestations are essential for proving social security rights and entitlements for accessing services and benefits. It is a part of the proposed eIDAS 2.0 regulation, which will provide all European citizens access to a trusted digital identity provided by their government and accepted in all signatory states.

The ecosystem dealing with attestations of attributes in social security coordination comprises several key entities and components:

Citizen: The holder of an attestation of attributes in the EUDIW ecosystem in context of European Social Security Coordination. These attestations are issued as (Qualified) Electronic Attestation of Attributes (Q)EAA to a digital identity representing this citizen.

EUDI Wallet: This is an application that allows citizens to store and present their identity data together with social security credentials in a cross-border use case. It must be accepted in the EU as an instrument for identification and authentication of digital identities with a 'high' Level of Assurance (LoA).

Verifiable Credential (VC): A VC data model for social security is used to represent a (Q)EAA and to allow the basic format which allows the presentation of attestations together with identity in a verifying situation.

Issuer: This represents the organisation that acts as (Q)EAA provider of social security credentials (See chapter 1.2). The authentic sources of these attestations of social security are competent institutions (CIs) of social security. They can directly act as an Issuer or can delegate this function to another (Qualified) Trust Service Provider ((Q)TSP) which will then act as the (Q)EAA provider. (Q)EAA providers in social security must fulfil certain obligations which also depends on whether they are public bodies or not.

Pickup System: A system where the citizen can initiate the process for downloading ("Pick up") the (Q)EAAS into the wallet. There may be multiple systems from different organisations or institutions where each can offer VCs of a specific type or domain.

Issuer System: A technical system designed to create and provide (Q)EAAs represented as VCs. This component will be provided by the DC4EU consortium to be integrated alongside the Pickup System.

Notification System: A national system that implements a protocol for notifying citizens about the status of their (Q)EAA in social security. There may be multiple systems from different organisations or institutions.

Download Service: A user-friendly service to streamline the process of issuing (Q)EAAs to digital identities represented as VCs. This is achieved by integrating a Pickup System, Issuer System, and Notification System into one workflow.

Relying Party: A relying party is a natural or legal person that relies upon an electronic identification or a trust service.

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

Verifier: In the social security context, a verifier is a relying party acting in a verification situation. The verifier facilitates the verification process by establishing a secure interface with and performing mutual authentication against the EUDIW using a verifier application.
Verifier Application: This software component assists a verifier in understanding the content of the credential attributes presented by the EUDIW and verifying their validity.
Registries: Public key repositories are essential for verifying attestations, while trusted registries play a crucial role in fostering trust among the various entities participating in the ecosystem. The management of the lifecycle of digital credentials is facilitated through the use of diverse types of **registries** and **verification services**.

In the following sections, we will delve into the conceptual architecture for Social Security, which will serve as the foundation for testing and executing Large-Scale Pilots (LSP) in DC4EU.

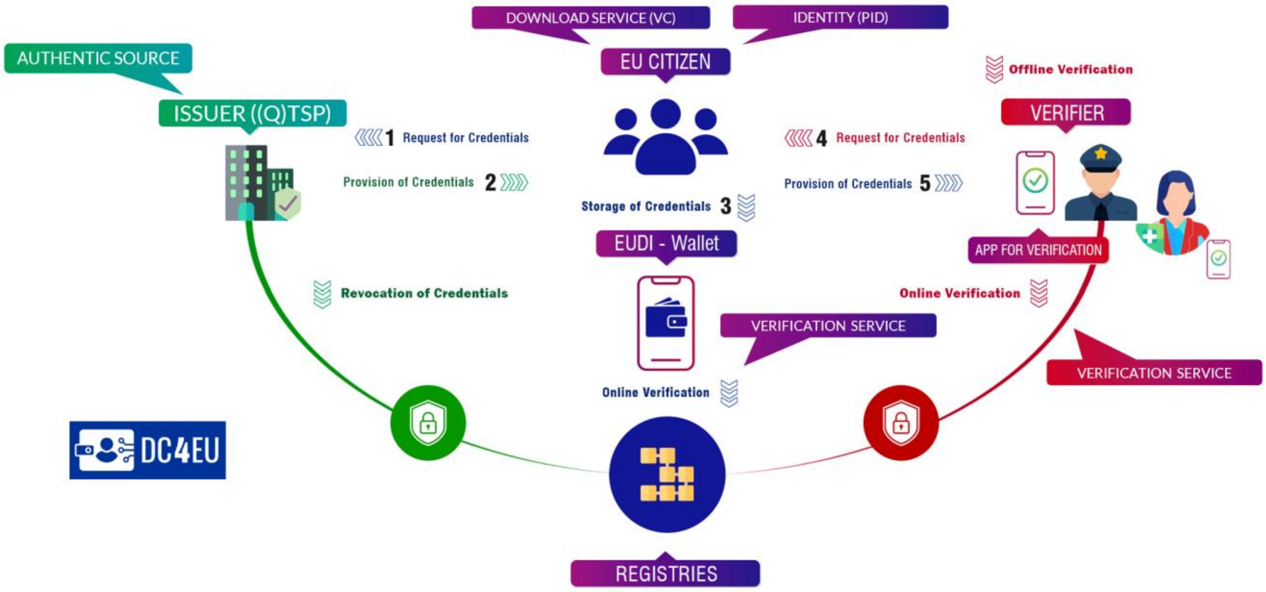


FIGURE 11: CONCEPTUAL ARCHITECTURE

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

4.2. KEY COMPONENTS

4.2.1. EUDI Wallet

The EUDIW plays a key role in its ecosystem by offering the following benefits:

- □ **Service Provision**: The EUDIW enables European citizens and businesses to securely present identity data and attestations of attributes that are necessary for accessing various digital services and benefits across the EU.
- □ **Interoperability and User Friendliness:** The EUDIW is user-friendly and interoperable with different platforms and devices. It follows the technical specifications outlined in the common EUDIW Toolbox, which ensures compatibility and consistency.
- □ **Security:** The EUDIW protects the identity data and attestations of attributes of its holder from unauthorised access and misuse. It also ensures secure transactions by using encryption and authentication mechanisms.
- □ **Compliance with Regulations**: The EUDIW adheres to the European Digital Identity Framework Regulation and the implementing and delegated acts adopted under that legal basis. It respects the principles of data minimisation, privacy by design and by default, and user consent.

4.2.2. Applications for Verification

In the EUDIW ecosystem, the **Verifier Application** plays a crucial role in the on- and offline verification process of attestations of attributes.

The Application of the verifier is used to verify the validity of an attestation of attributes presented by a citizen using his EUDIW. These attestations are initially provided by two types of providers: QEAA providers (issued by QTSPs) and Non-QEAA providers (issued by Public Service bodies in charge of an Authentic Source). (Q) EAA providers in the context of social security can be both types (e.g. for the EHIC). They issue various (Q) EAAs that are VCs linked to a user's digital identity, such as the EHIC and the PD A1.

The verification process involves supplying unbiased evidence to support the assertion that predetermined standards have been satisfied. This ensures that the transfer of data was carried out in accordance with the chosen techniques, protocols, standards, or laws. In social security this is member state specific.

In this context, the Verifier Application ensures the integrity and authenticity of these attestations, thereby enhancing the security of the EUDIW ecosystem. This process is crucial for maintaining a 'high' level of trust in digital transactions in Europe.

However, it is important to note that the development and implementation of such a Verifier Application would need to comply with the relevant legal and regulatory requirements in each MS. This includes ensuring the protection of customer information and personal data, as well as upholding customer privacy rights.

4.2.3. Public Key Repositories

Public key repositories are instrumental in the EUDIW ecosystem, particularly in the verification of attestations of attributes. These repositories, which are a key component of a Public Key (PKI), or Decentralized Public Key Infrastructure (DPKI) serve as verifiable databases housing the public keys for different entities. These public keys are used to verify identity and authorship, thus enhancing the security of the 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

Within the **EUDIW ecosystem**, public key repositories can store the public keys linked to the attestations of attributes. These attestations are provided by both QEAA providers and Non-QEAA providers.

When a **Relying Party**, such as a service provider, needs to verify an attestation of an attribute, it can access the corresponding public key from the repository. This key is then used to verify the digital signature on the attestation, ensuring the integrity and authenticity of the attestation and enhancing the overall security of the EUDIW ecosystem.

However, it is crucial to note that the development and implementation of such a public key repository must adhere to the relevant legal and regulatory requirements of each MS and the EU. This includes the protection of customer information and personal data, as well as the preservation of customer privacy rights. This adherence to regulations further strengthens the trust and reliability of the EUDIW ecosystem.

A public key repository may be a component of a trusted registry.

4.2.4. Trusted Registries

In the EUDIW ecosystem, trusted registries play a pivotal role in establishing trust among various entities such as credential providers, wallet holders, and relying parties (verifiers). These registries are part of the trust infrastructure, which can be implemented in different ways, and are essential for the target solution for social security coordination, as they establish and reinforce trust among the participants. These registries must have high availability and be online 24/7.

The trusted registries in the EUDIW ecosystem can be categorised into three types:

- **Trust Registries**: These registries foster trust among entities participating in the ecosystem, such as Issuers **(Issuer Registries),** Verifiers (**Verifier Registries**), and **EUDIW Providers**. They store and manage the public keys and other metadata of these entities and allow them to discover and authenticate each other.
- **Schema Registries**: These registries ensure that Issuers, Verifiers, and the EUDIW share a common understanding of the credentials' specific structure and content that are issued and verified. They store and manage the schemas and definitions of the credentials and allow them to validate and interpret the data. Additionally, they also include a ruleset governing who can issue and who is foreseen to request the data (**Disclosure Policy**).
- **Credential Status Registries**: These registries help to track and distribute information about the validity status of credentials. In social security only **Revocation Registries** are considered.

Data validation is crucial in this ecosystem. The data from the authentic source must be validated for its authenticity, correct formatting, and structure. Similarly, the data must be validated by the issuer before it is issued as a VC to a wallet or the trusted registries.

To ensure a clear understanding of the attributes in the credential among the authentic source, issuer, and verifier, a defined and agreed-upon schema or set of schemas is necessary. These schemas may vary based on the credentials and use case involved. Schemas also potentially enable agreement on selective disclosure between providers and relying parties.

To achieve interoperability in the wallet ecosystem, the issuer must consider different trust infrastructures in different MSs or contexts. Therefore, the issuer system aims to accommodate different types of credential profiles.

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

In most cases, the issuer, rather than the authentic source, keeps track of the status of the issued credentials. However, the decision to revoke a credential is a business decision taken by the authentic source who originally decided on the issuance of the credential.

4.2.5. Issuing of Credentials

In the EUDIW ecosystem, the issuing of credentials involves several key actors and components such as **an Authentic Source, a Pickup System, an Issuer System,** and a **Notification System** (See chapter 4.1). A Schema registry is ensuring that issuers adhere to agreed-upon data models specific to social security.

All services are combined to create a **member state** specific **Download Service** which is designed for the user to streamline the process of issuing (Q)EAAs, represented as a VC, issued to a digital identity with LoA 'high'.

4.2.6. Requesting Credential Issuance

In the EUDIW ecosystem used in social security, the process of a citizen requesting a credential from an issuer unfolds as follows:

Notification Protocol: The citizen is informed via a Notification System that a credential is ready for download. It gives a reference to a Pickup System. The Notification Protocol is activated when an authentic source makes a business decision to issue a credential. This decision is typically driven by an application for an entitlement or an automatic issuance process.
Credential Request: The citizen, who is the owner of a valid EUDIW, initiates the process by requesting the download of a specific credential from a previously authorised Issuer System. This request is executed from the EUDIW and is typically triggered by a Pickup System.
Entitlement Check: When downloading a VC, the EUDIW requesting the credential on behalf of the citizen must possess proper authorisation. Conversely, the issuer must ensure a 'high' LoA when issuing the VC to the correct identity associated with this EUDIW. In a fully digital workflow designed for social security coordination, authentication, and identification via electronic means (PID) between the EUDIW and the Issuer System are essential.

Credential Creation: If the identity of the citizen, who is the owner of the wallet, is authenticated and identified by electronic means with level of assurance (LoA) high, the issuer system can confidently and securely provide the VC for download.

Credential Transmission: The issuer system then transmits the VC to the EUDIW which requested the credential. The citizen, upon acceptance, becomes the holder of the attestation, which is achieved by finally storing the credential in the EUDIW.

It is important to note that the specifics of this process can vary depending on the use case, the security policies in the MSs, and the model for integrating the authentic source. The identification of the citizen, as the requester of the credential, plays a crucial role in this process to establish trust.

Moreover, the process must adhere to the relevant legal and regulatory requirements in each MS, including the eIDAS regulation. This regulation sets out the rules for electronic identification and trust services for electronic transactions in the internal market, ensuring 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

protection of the citizen's information and personal data, as well as upholding their privacy rights.

4.2.7. Presenting Credentials

In the **EUDIW ecosystem**, the holder of attestations, who is the citizen, who owns a EUDIW to whom the attestation is issued, plays a significant role. The holder possesses the attestations, which are provided by the Issuer. The EUDIW is a secure and anticipated tool to store, show and present identity data and its attributes.

Verifiable Presentations (VPs) can prove the holder's digital identity and their attributes in a verifiable digital format during a verification process.

The holder presents these VPs to relying parties, such as public authorities, when asked and necessary. The process of presenting credentials based on a common agreed data schema typically unfolds as follows:

- **Request for credential**: A verifier requests by electronic means from the citizen the provision of a specific credential based on a predefined credential schema.
- **Consent**: Authenticity of the requesting verifier may be checked by the citizen. The citizen agrees to share the requested credential with the verifier, using his EUDIW.
- **Presentation of credential**: The citizen presents a VP, which is a cryptographically signed message that contains a combination of credentials or a subset of their attributes to the verifier.

4.2.8. Verifying Credentials

The verifier has an essential role in the EUDIW ecosystem. It can be either a software application controlled by a person or a device that communicates with the EUDIW automatically. The Verifier verifies the digital credentials presented using the EUDIW and displays or logs the results in a user-friendly manner. Verifiers verify credentials in various situations.

- **Software Application:** For instance, a university's online system verifying a diploma presented by a student.
- **Person in the Field:** For example, an inspector verifying a PD A1 credential at a construction site. This is the proximity supervised scenario which can be both off- and online.
- **Device to machine interaction:** Such as a Near Field Communication (NFC) terminal verifying an EHIC at a doctor's office. This are the non-proximity and proximity unsupervised scenarios.

All these situations require assistance to interact with the new standards used in the EUDIW ecosystem. To facilitate this, DC4EU WP7 aims to build an open-source verifier software application. This software serves as a solution, enabling relying parties to interact with and verify credentials in the EUDIW ecosystem during the testing and piloting phase.

In the EUDIW ecosystem, the process of verification typically unfolds as follows:

- **Verification of credential**: The Verifier verifies the authenticity, the entitlement to issue a credential and the validity of the credential and its issuer, using the public keys and other information available in trusted registries that supports the EUDIW ecosystem. The Verifier also checks the digital identity of the holder which is an identity with LoA 'high'.

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

4.2.9. EUDIW Conceptual Data Model

Credentials in paper or plastic format, such as the EHIC or the PD A1 have several drawbacks. They are prone to loss, theft, damage, or unauthorised duplication. VCs are digital and cryptographically secured containers of physical credentials that digitally prove something about a user, such as their digital identity or a qualification earned [18].

VCs are issued to a digital identity, which is a digital representation of a person, organisation, or thing. The holder of a VC can present it to a verifier, who can verify the authenticity of the credential and the identity of the holder as well as the relation of the holder and the subject, if they are not the same. The process of issuing a VC involves binding an issuer statement about a subject to the subject's identifier using cryptographic proofs. Once issued, a VC can be held for potentially long periods of time and presented for multiple purposes and in multiple ways.

The Issuers can transform their physical credentials into a digital format, allowing to store them in the EUDIW which guarantees identification and authentication of digital identities in the EU.

VCs offer a more secure, convenient, and privacy-preserving alternative to physical credentials and they will be a standard supported by the EUDIW ecosystem:

- **Non-duplicable**: VCs cannot be cloned (simply copied) and are secured against fraud and error.
- **High Security**: They are extremely difficult to steal as an attacker would need both your electronic device and your authentication method.
- **Privacy-Preserving**: They support selective disclosure, allowing the citizen to disclose only a portion of the verifiable data.
- **Enhanced Security**: They adhere to the principle of least privilege, granting permissions only for essential information required in the verification process.
- **Delegable**: The citizen can delegate VCs by electronic means to others for use. This creates a new credential changing the holder of the credential, while maintaining the original binding to the identity to which it was originally issued.

The subsequent sections provide an overview of the concepts used for **VCs**:

- The components that constitute a VC.
- The components that constitute a VP.
- An ecosystem where VCs and VPs are expected to be beneficial.

4.2.10. Verifiable Credential (VC)

A Credential is defined as a set of one or more claims made by an issuer. This Credential in the EUDIW ecosystem is issued to a digital identity onboarded in the EUDIW (PID).

In the physical world, a credential might consist of [18]:

- Information related to identifying the subject of the credential.
- Information related to the issuing authority.
- Information related to the type of credential this is.
- Information related to specific attributes or properties being asserted by the issuing authority about the subject.
- Evidence related to how the credential was derived.
- Information related to constraints on the credential.

A VC can represent all the same information that a physical credential represents. It could be defined as a tamper-evident credential that can be cryptographically verified.

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

VCs can be used to build VPs, which can also be cryptographically verified. Holders can then share these VPs with verifiers to prove they possess VCs with certain characteristics.

4.2.11. VC Ecosystem

A number of entities and roles are involved in the VC ecosystem embedded in the EUDIW ecosystem. These entities and roles are shown in figure 1.

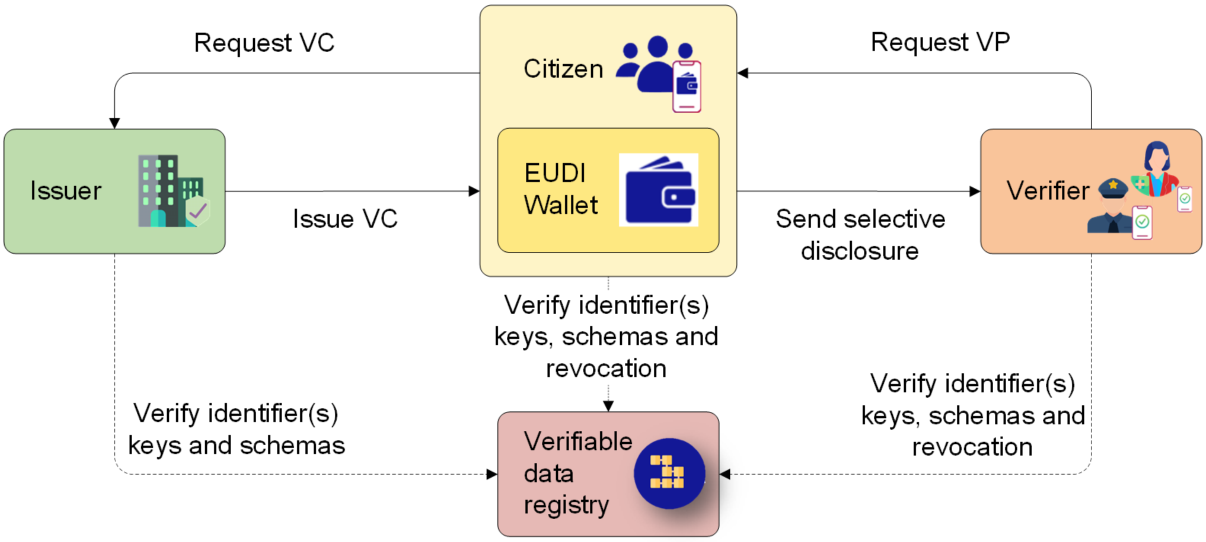

Request VC
Citizen
Request VP
Issuer
EUDI Wallet
Verifier
Issue VC
Send selective disclosure
Verify identifier(s) keys, schemas and revocation
Verify identifier(s) keys and schemas
Verify identifier(s) keys, schemas and revocation
Verifiable data registry

FIGURE 12: THE ROLES AND INFORMATION FLOWS FORMING THE BASIS FOR THIS SPECIFICATION [18].

The components of the VC architecture are as follows [18]:

- □ **Issuer**—The entity that issues VCs, which represent (Q)EAAs. These entities are the authentic sources (competent institutions) in social security coordination or entities acting on behalf of the authentic sources.
- □ **Subject**— is defined as a set of objects that contain one or more properties that are each related to a subject of the VC.
- □ **Holder**—The entity that is currently holding the VC and presents it to the verifier. It could be the citizen but also another authorised natural or legal person.
- □ **Verifier**—The entity that receives the VCs from the holder via a presentation and provides services and benefits in return.
- □ **EUDIW**—The entity that holds the VCs for the holder including the software that interacts with the EUDIW ecosystem on behalf of the holder.
- □ **Trust Registries**— Conceptually, an internet-accessible registry that holds all the essential data and metadata that enables the VC ecosystem to operate.

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

4.2.12. Core Data Model

The W3C has defined the following core data model concepts in its specification [18]. These concepts enable a consistent structuring of data and the creation of a logical data model for presenting and verifying credentials in an on- or offline situation:

1. **Claims**: These represent specific pieces of information or attributes associated with a credential.
2. **Credentials**: Credentials are used to assert certain facts about an entity, such as EHIC and PD A1 for a citizen.
3. **Presentations**: Presentations allow the combination of multiple credentials into a single package for presentation or verification.
4. **Contexts**: Contexts provide a framework for interpreting the meaning of terms and properties within a credential.
5. **Identifiers**: Identifiers uniquely identify e.g. a credential or a subject.
6. **Types**: Types define the category or purpose of a credential such as the EHIC type.
7. **Credential Subject**: The subject of a credential, typically an individual or an entity.
8. **Issuer**: The entity that creates and issues the credential.
9. **Issuance Date**: The date when the credential was issued.
10. **Proofs (Signatures)**: Cryptographic proofs ensure the integrity and authenticity of the credential.
11. **Expiration**: Specifies the validity period of the credential.
12. **Status**: Indicates whether the credential is valid or revoked.

These concepts are integral to the W3C's VCs Data Model (VCDM). The W3C's 1.1 & 2.0 specification provides additional details on these concepts.

A **claim** is an assertion made about the subject. It can be expressed using ***subject*-*property*-*value*** relationships:

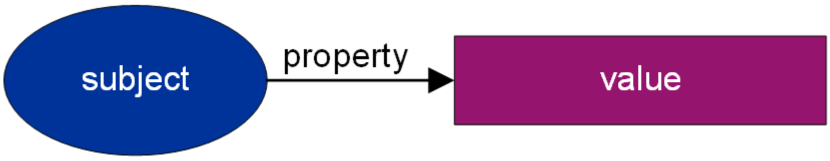


FIGURE 13: THE BASIC STRUCTURE OF A CLAIM

The data model for claims, illustrated in Figure 13 above can be used to express a large variety of statements (logical data models). For example, whether someone is insured at a CI can be expressed as shown in Figure 14.

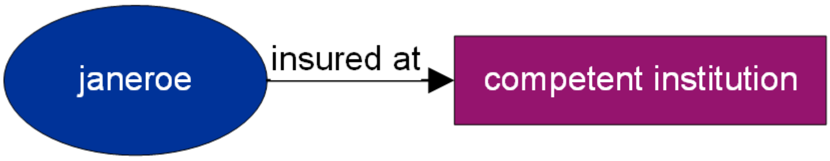


FIGURE 14: CLAIM STRUCTURE: JANEROE IS INSURED AT THE COMPETENT INSTITUTION

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

Individual claims can be merged to express a **graph** of information about a subject. For example:

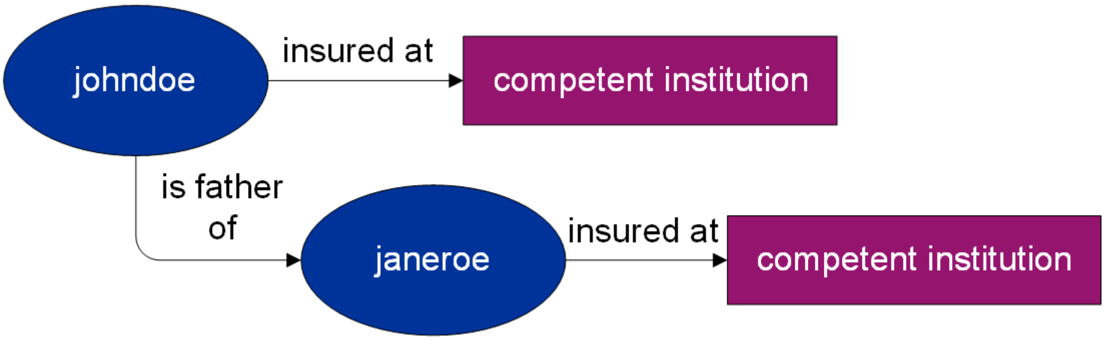


FIGURE 15: CLAIM STRUCTURE: JOHNDOE IS FATHER OF JANEROE AND JANEROE IS INSURED AT COMPETENT INSTITUTION

However, to be able to trust claims, more information is expected to be added to the graph.

4.2.13. VC Building Blocks

A VC is a set of tamper-evident **claim(s), metadata** that e.g. assert who issued it and proof(s) as e.g. the issuer signature.

Its basic building blocks are:

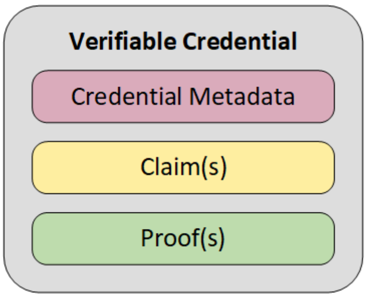


FIGURE 16: BASIC COMPONENTS OF A VERIFIABLE CREDENTIAL.

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

Or represented in a more extended way:

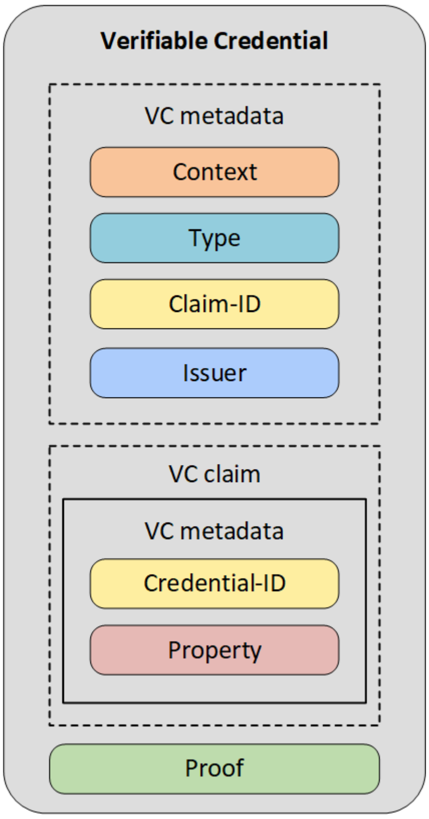


FIGURE 17: DETAILED DEPICTION OF A VERIFIABLE CREDENTIAL ([19, PP. 164-194]

The contents of each of these properties are described next:

Context—When people communicate, they need to use the same language and vocabulary to understand each other. Similarly, when computers communicate with each other, they need to use a common language and vocabulary to exchange information. The context is a sequence of one or more Uniform Resource Identifiers (URIs) that define the vocabulary used in a digital document. Ideally, each URI should point to a machine-readable document containing a vocabulary that a verifier can automatically download and configure.

Property—is the statement about the **subject**

However, it is important to note that context on its own may provide more information (vocabulary) than a verifier wishes to use. Therefore, the VC Data Model also contains a type property that can be used to specify which parts of the context should be used by the verifier.

Type—the type property contains a list of URIs that assert what type of VC this is. The first type must always be [18], which can be abbreviated to VC using the JavaScript Object Notation for Linked Data (JSON- LD) at context mechanism. Verifiers can read the list of types and quickly determine if they can understand and process this VC. If the VC is a type the verifier does not recognise, the verifier can immediately reject it without further processing.

ID—the credential ID property is the unique identifier of this VC, created by the issuer. It consists of a single URI. This allows any entity to unambiguously reference this VC.

Issuer—the issuer property uniquely identifies the issuer. It can be an URI. This URI can point to a registry that fully describes the issuer and this verifiable data registry can contain further details about the issuer, such as e.g. its public-key certificate.

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

Proof—for a credential to be verifiable, it needs a signature, referred to 'more generally in the VC Data Model specifications' as a proof. This cryptographically proves that the issuer issued this VC and that it has not been tampered since issuance. There is no single standard for the proof property's contents since several different types of proof are envisaged.

The figure below shows a more complete depiction of a VC, which is normally composed of at least two information graphs. The first graph expresses the VC itself, which contains credential metadata and claims. The second graph expresses the digital proof, which is usually a digital signature.

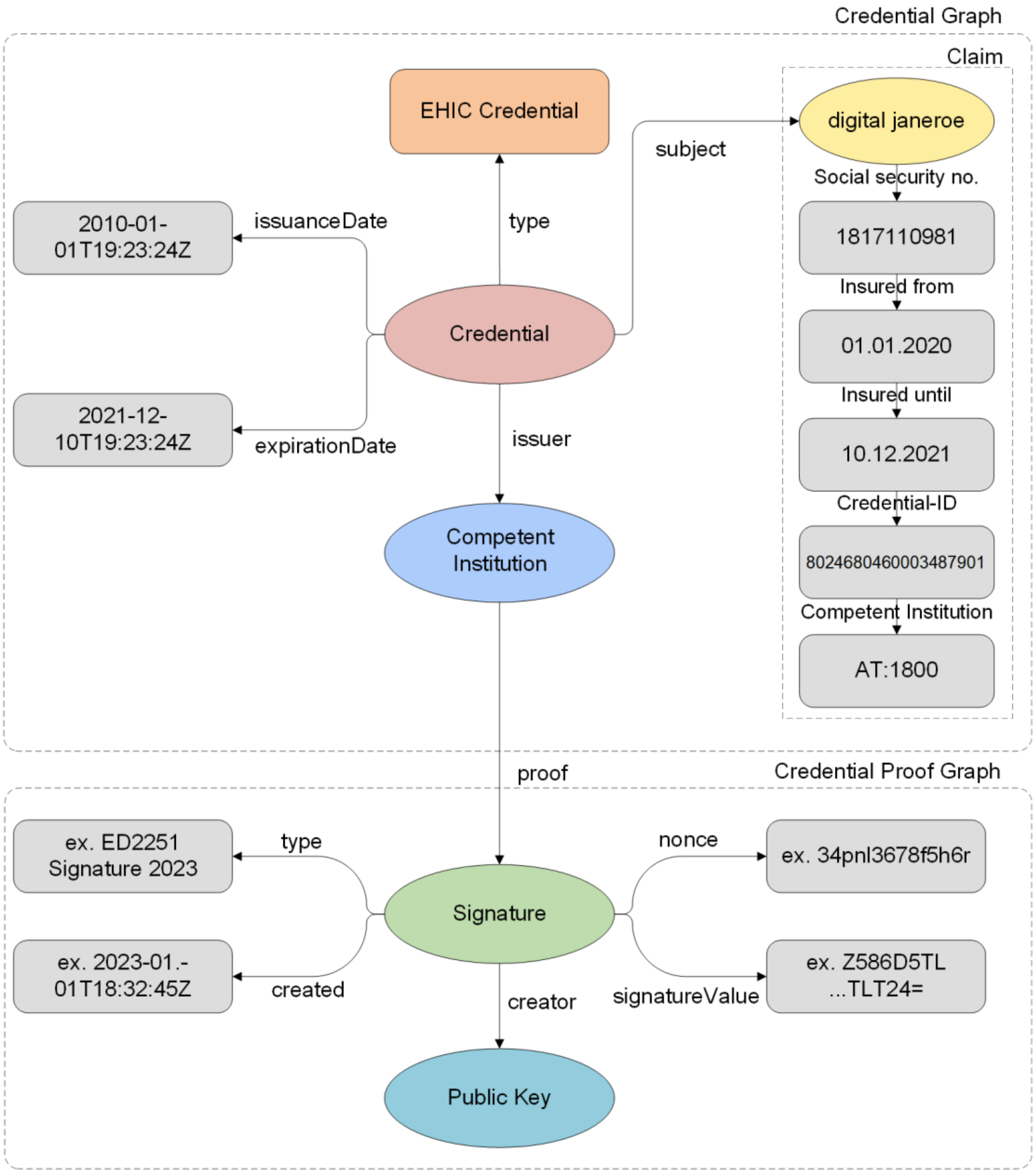


FIGURE 18: INFORMATION GRAPHS ASSOCIATED WITH A BASIC VERIFIABLE CREDENTIAL [18].

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

4.2.14. VP Building Blocks

A VP is the format for presenting one or multiple VCs, normally to a verifier. Like a VC it has its own **metadata and proof(s)**, but these are created by the holders EUDIW rather than an issuer. The Metadata is mainly information for technical interpretation of the received data at the verifier. The Proof(s) in the EUDI wallet ecosystem can be the signature of the 'holders' EUDIW and enables the presentation to be tamper-proof and the verifier to verify that the credentials in the presentation are sent from the digital identity they were initially issued to. A presentation as mentioned before can contain one or multiple credentials.

To support the principle of data minimisation, selective disclosure technology is utilised. It allows a credential to be presented partially, without disclosing the full set of claims. This means that a presentation can include one or multiple VCs, each with all its claims or just a subset, depending on the use case and choice of the holder. While doing so, the partial credential including its proof(s) stays fully valid and can be verified.

Selective disclosure technology enables users to present (e.g. self-presentation) only the information they choose with non-qualified verifiers, while keeping the rest of their sensitive data private. This is particularly useful when a user needs to prove a specific claim but does not want to share all the information contained in their credential. If a citizen is in a verification situation with an authorised verifier selective disclosure is not appropriate in social security coordination since services and benefits may not be provided if only a subset of information is provided. For non-authorised verifiers selective disclosure can play a role.

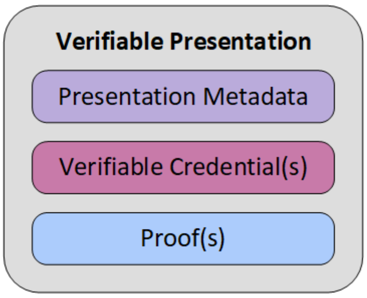


FIGURE 19: BASIC COMPONENTS OF A VERIFIABLE PRESENTATION [18].

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

Or:

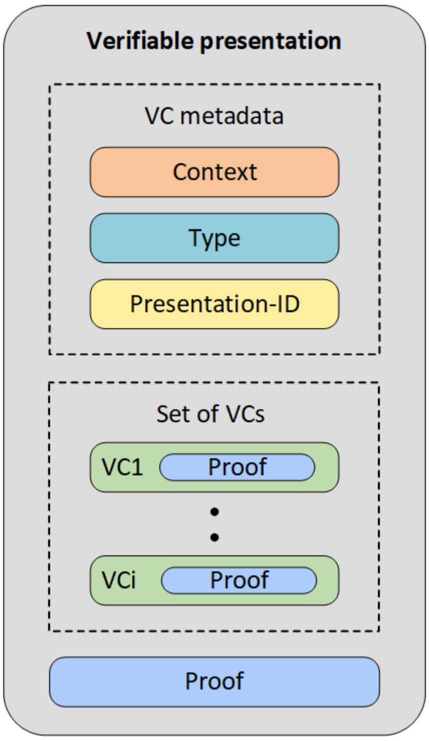


FIGURE 20: DETAILED DEPICTION OF A VERIFIABLE PRESENTATION [19, PP. 164-194].

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

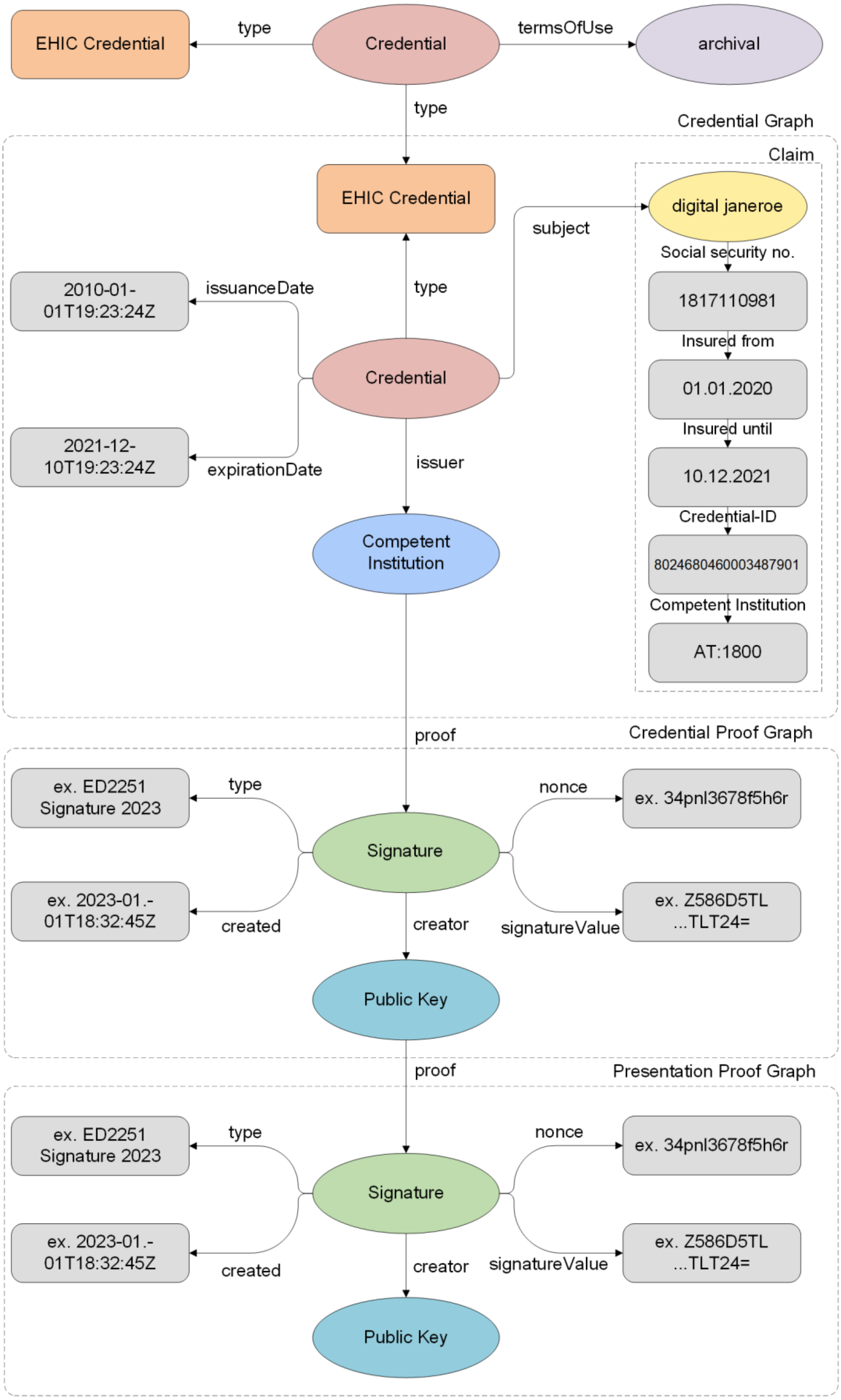


FIGURE 21: INFORMATION GRAPHS ASSOCIATED WITH A BASIC VERIFIABLE PRESENTATION [18].

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 first of these information graphs, the Presentation Proof Graph, expresses the VP itself, which contains presentation metadata. The VC property in the Presentation Graph refers to one or more VCs, each being one of the second information graphs, i.e., a self-contained Credential Graph, which in turn contains credential metadata and claims. The third information graph, the Credential Proof Graph, is usually a digital signature. The fourth information graph, the Presentation Proof Graph, expresses the presentation graph proof, which is usually a digital signature.

4.3. VALIDITY

The EUDIW ecosystem requires the implementation of a Digital Identity with a 'high' LoA (PID) in combination with the QEAA which will be implemented using different standards (e.g., W3C 1.1 +). This combination facilitates seamless identity verification across Europe, adhering to a standard that is mandated for endorsement by all EU MSs.

It ensures not only the authenticated possession and validity of digital attestation of attributes but also guarantees their appropriate usage. The implementation of this identity framework and the linkage between QEAA and the identity to whom it is issued will be specified by the EUDIW Toolbox and the related eIDAS implementing acts. In the context of EU regulations, implementing acts play a crucial role in ensuring that EU laws are effectively put into practice.

The EUDIW Toolbox and upcoming implementing acts will provide insights into how the validity of a credential issued to a digital identity will be considered and how the binding will be implemented. Especially the validity of a credential linked to an invalid identity is of major concern.

The digital verification process considered in the EUDIW ecosystem system includes digital identity check and validity check for (Q)EAAs in a verifying challenge between the EUDIW and a Verifier App. The following situations can occur:

"Red"	**QEAA is invalid**
"Yellow"	**QEAA is valid but digital identity (PID) is invalid**
"Green"	**QEAA and digital identity (PID) are valid and digitally verified**

In terms of the status "Yellow", the attestation presented by a wallet with no digital identity context (no PID) may be considered as an acceptable attestation.

It is important to note that attributes related to identity do not inherently contribute to the validity of a credential. Even if the digital identity (PID in the EUDI wallet) to whom the credential was issued is invalid, the credential itself remains valid.

If the identity to whom the credential was issued (which will be digital identity (PID) in the EUDI wallet) is invalid the credential will stay valid but the digital identity context is lost.

Such a credential presented only by an operational EUDI wallet might be accepted on a local level but not on a European level. Adding local identity attributes (e.g. social security identity) in the credential and making it a "self-contained" credential does not help since it still misses the context to the (true) digital identity it was issued to. Such credentials are presented by an application which has no identity context. It may be presented by anything but a EUDI wallet,

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

just a wallet which claims to be a trustworthy wallet. A situation which MSs may want to avoid in terms of fraud and error, and a situation which must not be accepted by the involved relying parties. Adding naming attributes does not add trust in a verifying situation but provides the possibility to match local identity data from the credential presented by a non-trustworthy wallet with data from an ID card which might also not be trustworthy in a European context. While this is comparable to the current paper-based methods, digital solutions should improve the situation and establish a higher trust level.

The acceptance of a social security VC in a cross-border context is determined by its validity and a proof of correct usage of the digital credential, which in turn supports the rights of citizens to access services and benefits in social security coordination, as per the regulations. The hypothesis of DC4EU is that this mandatory acceptance will be achieved by using valid EUDI wallets and the related trust framework provided. If the citizen does not accept the digital solution and the prerequisites that come with this solution, they can still use the permanent alternative in paper or plastic. Please check chapter 1.4 on Scope and Scenarios for Large Scale Pilots (LSP) in DC4EU.

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. BUSINESS SCENARIOS AND USER JOURNEYS

5.1. INTRODUCTION

The European Digital Identity Wallet (EUDIW) ecosystem is a pioneering digital platform designed to simplify the management and accessibility of crucial social security documents such as the EHIC and PD A1. The pilot project, which incorporates EHIC and PD A1, aims to evaluate the system's functionality, efficiency, and user-friendliness.

User Journeys

The user journey starts with the use case of onboarding European citizens to the EUDIW platform. Once registered, citizens can request their EHIC or PD A1 to be digitally stored in their EUDIW. The issuer system then liaises with the competent institution (CI) to create digital versions of these documents. This enables citizens to present these documents at any time and place to avail social security benefits and services.

Business Scenarios

The pilot project encompasses various business scenarios to ascertain the robustness of the EUDIW ecosystem. These scenarios include:

- **Initial Issuance**: This scenario involves testing the process of issuing EHIC or PD A1 to first-time users, including automatic issuance upon registration or birth, and issuance upon request.
- **Re-Issuance**: The system's capability to handle re-issuance requests, such as in cases of loss, theft, changes in data, changes in insurance, and expiration of validity, will be evaluated. Re-Issuance in social security coordination is always a process of revocation and issuing.
- **Revocation/Deactivation**: The process of deactivating or revoking EHIC or PD A1 in the national registries/databases will be assessed.
- **Verification**: The process of verifying a digital EHIC or PD A1 credential in a verification situation by an authorised verifier will be evaluated. This also includes the process of handing proof records to back-office systems.

The pilot project seeks to validate the EUDIW ecosystem's ability to handle these scenarios efficiently and securely, thereby enhancing the user experience and fostering the adoption of digital solutions in the EU. The insights gained from the pilot will be instrumental in refining the EUDIW ecosystem and preparing it for a wider rollout.

In the subsequent sections, the necessary user journeys and business scenarios will be explained in a generic manner so that they can be applied to a portfolio of documents in social security coordination. The pilot project will adhere to all relevant regulations and data protection standards.

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

5.2. GENERAL BUSINESS REQUIREMENTS FOR SOCIAL SECURITY COORDINATION

The General Principles in chapter 3.2 are the basic requirements that need to be followed. In addition to these principles the following requirements must be fulfilled to successfully implement the defined use cases in social security.

- □ **Issuer Onboarding:** The system should facilitate onboarding of CI or organisations who act on behalf of CI in social security. This can be achieved by the reuse of European registries like the Institution Repository (IR). Once registered, issuers should be able to issue credentials to a digital identity according to a specific social security credential schema.
- □ **Verifier Onboarding**: The system should facilitate onboarding of Verifiers in social security. This can be achieved by the reuse of national registries. Once registered, verifiers should be able to verify attributes presented by a EUDIW according to their legal mandate in social security legislation. The ruleset and the capability of this service strongly depends on the recommendation and the implementing acts for the EUDIW ecosystem. The testing and piloting phases will test these capabilities to check the feasibility for social security.
- □ **Issuing of Credentials**: The issuer system should communicate with the authentic source (i.e.CI) to create digital versions of documents in social security coordination. This will enable citizens to present these documents at any time and place to avail social security benefits and services.
- □ **Initial Issuance**: The system should be capable of issuing EHIC or PD A1 to existing wallet holders. This includes automatic issuance upon registration or birth, and issuance upon request. This initial issuance may include issuing to holders which are not identical to the subject (e.g. parent\child).
- □ **Revocation**: The system should be able to handle revocation of EHIC or PD A1 in the national registries/databases.
- □ **eIDAS Compliance**: This implies the use of the EUDIW ecosystem for the execution of the business scenarios.

The EUDIW ecosystem should be designed to meet these combined requirements to ensure secure and seamless electronic interactions. Compliance with both social security and eIDAS requirements, along with principles of self-sovereignty and data minimisation is crucial for fostering trust among citizens and promoting the adoption of digital solutions in the EU.

5.3. USE CASE 1: ONBOARDING OF THE EUDI WALLET

5.3.1. General Description

In this specific use case, a citizen wants to install an EUDIW on their smartphone to present digital entitlement documents such as the PD A1 and EHIC while working or traveling abroad.

The EUDIW is a secure and convenient way for European citizens and businesses to share identity data needed for accessing digital services.

The PID Provider is responsible for verifying the identity of the EUDIW holder, maintaining an interface to securely provide PID to the EUDIW, and making information available for Relying Parties to verify the validity of the PID, without receiving any information about the PID's use.

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

5.3.2. Prerequisites Related to the Use Case

To be able to use the EUDIW a citizen will need a device that supports the EUDIW App and an available PID provider.

Additionally, an internet connection is required to download and use the EUDIW App.

5.3.3. Roles, Activities and Tasks

Citizen	**App selection** The citizen searches for the EUDIW of their choice in platform-specific stores and installs it on their device.
App Store	**App Provision/Installation** The App store provides the selected EUDIW App to the citizen. The citizen installs it on their device.
Citizen	**Personalisation** The citizen opens the EUDIW and follows the onboarding process for their PID using the wallet's capabilities and the member state (MS)-specific guidelines.
Citizen	**Start** The citizen's EUDIW is now ready to download digital credentials and present them in a verifying challenge.

TABLE 5: ONBOARDING OF THE EUDIW - ROLES, ACTIVITIES AND TASKS

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

5.3.4. BPMN Diagram

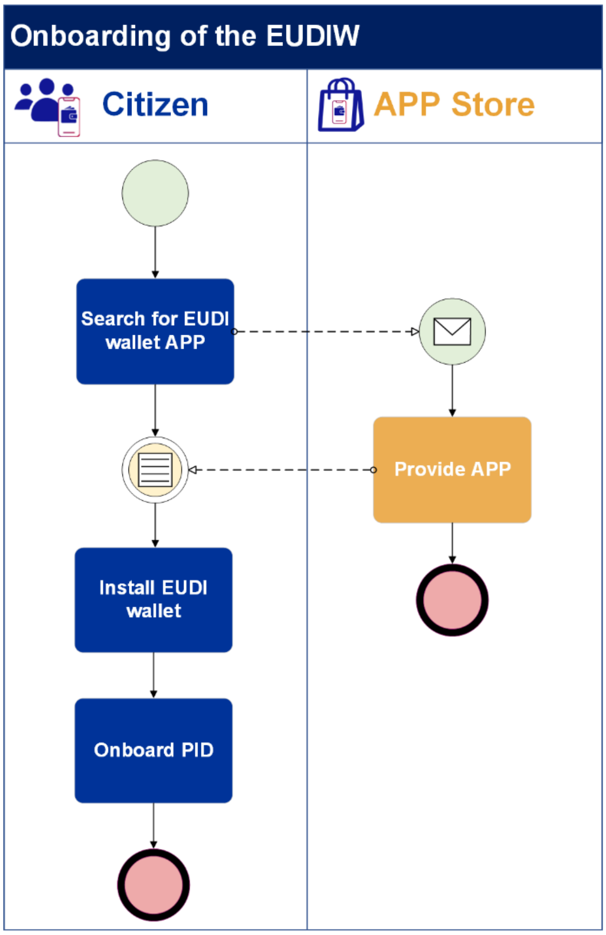


FIGURE 22: ONBOARDING OF THE EUDIW

5.3.5. High Level Requirements

In the subsequent text, you will encounter capitalised terms such as “MUST” and “SHOULD”. These terms have been assigned specific definitions:

- **MUST**: This term, or its synonyms “REQUIRED” or “SHALL”, signifies that the definition is an unequivocal requirement of the specification.
- **SHOULD**: This term, or the adjective “RECOMMENDED”, implies that while there could be valid reasons to disregard a particular item in certain situations, the full implications need to be comprehended and judiciously considered before opting for an alternative path.

ONB01: A digital identity with Level of Assurance (LoA) ‘high’ (PID) MUST be associated with an operational Wallet Instance to create a valid EUDIW. The citizen represented by this PID is successfully onboarded within the EUDIW ecosystem for social security coordination and can use a EUDIW as an electronic identification means.

ONB02: An onboarded citizen MUST be entitled to verify their identity and related attributes by electronic means at anytime and anywhere when using a valid EUDIW as an electronic identification means, particularly during a verification challenge with a relying party (verifier), such as the EHIC or the PD A1 use case.

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

5.4. USE CASE 2: ISSUANCE OF VERIFIABLE CREDENTIALS

5.4.1. General Description

This use case involves issuing VCs for social security through different customer platforms for the citizen. The issuance process is closely tied to national e-government practices, which can vary from country to country. Our goal is to create a generic approach that can be used in any country by any competent institution (CI). This approach will enable the issuance of VCs that are secure, privacy-respecting, and machine-verifiable. This process is carried out by CI (public or private bodies) who are qualified according to the standards set by the eIDAS regulation.

The use case within the boundaries of DC4EU starts with a request from the CI to an issuer system for the issuance of a VC. This request serves as the triggering event for the use case.

The process covers several stages, such as notifying the citizen to download specific items.

All steps involving the competent national institutions are described for a better understanding and completeness of the overall process, but do not fall within the scope of the Large-Scale Pilots (LSPs) and their implementation is of national concern.

Additionally, the steps for applying for a VC at the CI by the citizen/employer, as pictured in the status quo processes do not fall within the scope of the LSPs. They may differ depending on the type of the credential requested and their implementation is of national matter.

5.4.2. Prerequisites Related to the Use Case

The following requirements must be met so that the issuing process can be carried out smoothly:

- □ **eIDAS Levels of Assurance (LoA)**: To ensure high assurance authentication for accessing the VC using a download service, the eIDAS LoA must be used.
- □ **Schema Registry**: The issuance must be conducted according to a registered schema for a given credential type.
- □ **Download Service Accessibility**: The Download Service, as introduced in chapter 4.1, combining a Pickup System, Issuer System, and Notification System into a user-friendly workflow, should be accessible from the citizen's device and can be implemented as native mobile app or as an application running in a browser.
- □ **Internet Connection**: An internet connection on the citizen's device is necessary to execute the workflow for downloading the credential.
- □ **EUDIW Installation and Functionality**: The EUDIW must be installed, functional, and the PID must be onboarded on the citizen's device.
- □ **Business Decision:** The business decision about the issuance of a credential has been made.

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

5.4.3. Roles, Activities and Tasks

CI	**National Demand for Digital Credential** The CI creates a demand for issuance of a digital credential and sends it towards the issuer system.
Issuer System	**Receive Demand** The Issuer System, upon receiving a demand from a CI to issue a digital credential, initiates the process. The request is processed within the issuer system, during which relevant attributes are securely stored. Upon completion of this process, the issuer system activates a notification protocol aimed at the citizen.
CI	**National Notification Protocol** The CI is responsible for initiating the notification service towards the citizen. This notification, generated within a national or institutional framework, serves to inform the citizen of the successful issuance of their digital credential.
Citizen	**Receive Notification** Upon successful preparation of the digital credential, the citizen is notified via a notification framework. This notification includes a reference to a Pickup System, which is part of a national or institutional download service designed specifically for the secure download of digital credentials.
Citizen	**Pickup System Authentication** Upon using the reference, the citizen is directed to the Pickup System. Here, the citizen is required to authenticate themselves. Once authenticated, they can proceed with downloading digital credentials.
Issuer	**Provide Download Link** When the citizen accesses the Pickup System via a smartphone, they are presented with a direct link for downloading, provided by the issuer system. Conversely, if the citizen is using a secondary device, a quick response (QR) code is made available.
Citizen	**Download Credential** Using the download link or scanning the QR code from a secondary device, the pre-installed EUDIW is started, and after authentication of the EUDIW the download process is initiated

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

Issuer	**Provide Credential** The issuer system issues the digital credential to the citizen.
Citizen	**Store Credential** Before downloading the digital credential, the citizen can view the credential type and data. This allows the citizen to decide if they accept the credential to be stored. Once downloaded, the digital credential is securely stored within the citizen's EUDIW. The user-friendly interface of the EUDIW allows the citizen to select and view the digital credential, providing them with the ability to verify the information contained within it as well as cryptographic validity. This ensures, that the citizen has full control and visibility of their digital credentials. This full control is enhanced by an EUDIW dashboard (see [1])

TABLE 6: ISSUANCE OF VERIFIABLE CREDENTIALS – ROLES, ACTIVITIES AND TASKS

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

5.4.4. BPMN Diagram

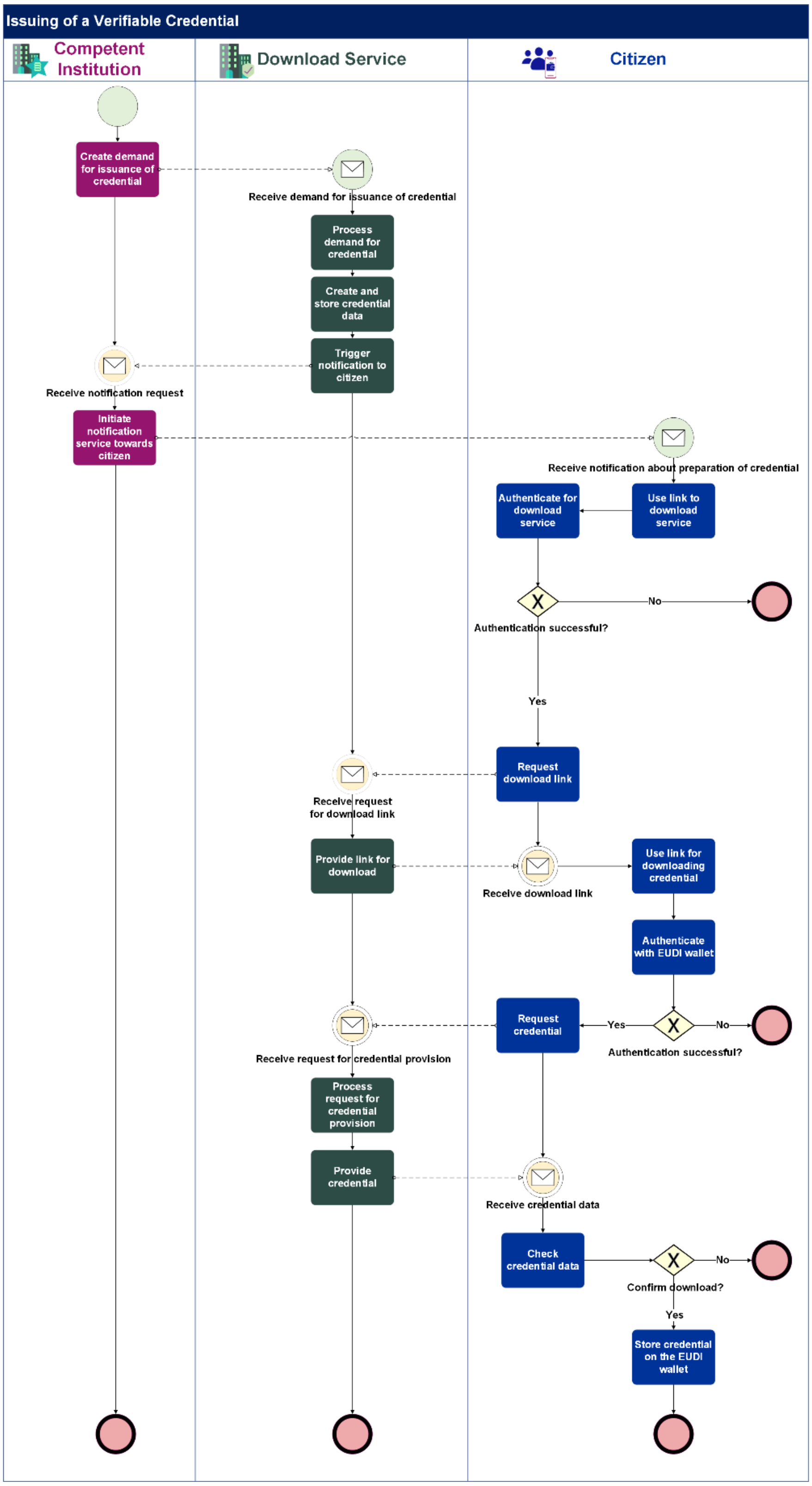

Issuing of a Verifiable Credential
Competent Institution
Download Service
Citizen
Create demand for issuance of credential
Receive demand for issuance of credential
Process demand for credential
Create and store credential data
Trigger notification to citizen
Receive notification request
Initiate notification service towards citizen
Receive notification about preparation of credential
Use link to download service
Authenticate for download service
Authentication successful?
No
Yes
Request download link
Receive request for download link
Provide link for download
Receive download link
Use link for downloading credential
Authenticate with EUDI wallet
Authentication successful?
Yes
No
Request credential
Receive request for credential provision
Process request for credential provision
Provide credential
Receive credential data
Check credential data
Confirm download?
No
Yes
Store credential on the EUDI wallet

FIGURE 23: ISSUANCE OF A VERIFIABLE 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

5.4.5. High Level Requirements

ISS01: A Verifiable Credential (VC) MUST be issued to the correctly onboarded citizen. It MUST be guaranteed that when an onboarded citizen requests a VC using a valid EUDIW, that this citizen receives the correct VC that has been authorised for issuing by an authentic source.

ISS02: A VC MUST be issued in a manner that ensures **cross-border** acceptance without restrictions by all relying parties. It MUST possess the equivalent legal validity as attestations in physical form, such as those governed by social security regulations.

ISS03: A VC issued by an issuer MUST be associable with the citizen, which is represented by the digital identity that requested the digital credential during the issuing process.

ISS04: A VC issued by an issuer MUST be associable with the subject, which is an individual about whom statements are made by the issuer.

ISS05: An association between the VC and its holder MUST be established in a manner that is unambiguously verifiable by a relying party (verifier) through digital means.

ISS06: An association between the VC and the holder of that VC MUST be implemented in a manner that it has no impact on the validity status of the VC when used in a verification process. Invalid identity MUST not invalidate the credential, but MAY affect the acceptance of the credential by relying parties (verifiers).

ISS07: The implementation of the association between a VC and its holder must be such that it allows unrestricted presentation and verification of data within the EUDIW ecosystem.

ISS08: A VC MUST be issued in accordance with a protocol that guarantees the execution of a disclosure policy of social security. This policy MUST be custom-made by social security to the credential type at hand. Furthermore, it is imperative that this policy delineates the relying parties that are authorised to request a specific data schema.

ISS09: A VC MUST be issued in a manner that fulfils social security coordination regulations, adheres to GDPR principles, and aligns with security, data minimisation, and privacy principles as defined in the eIDAS regulation.

ISS10: A VC MUST be issued in a manner that allows the verification of its authenticity and integrity by digital means when used within the EUDIW ecosystem.

ISS11: A VC MUST include all the necessary business information to guarantee the successful execution of a verification process between the valid EUDIW and an application used by a qualified verifier. A successful execution MUST ensure that the rights of a citizen are secured according to social security coordination, eIDAS and other EU wide regulations.

ISS12: A VC MUST be issued in such a way that it can be revoked, and that this status information can be retrieved and processed by digital means in the EUDIW ecosystem.

ISS13: A VC MUST be issued in such a way that it can be delegated to another EUDIW, and this delegation MUST be based on a verifiable consent from the original credential owner.

ISS14: A VC MUST be issued in such a way that a user's right to data portability, as defined in the eIDAS regulation, can be exercised.

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

5.5. USE CASE 3: REVOCATION OF CREDENTIALS

5.5.1. General Description

The revocation process is an essential feature in the realm of VCs, marking a significant advancement over traditional paper documents. This process involves three primary roles: the issuer, the CI, and the citizen. The issuer is responsible for generating and, if necessary, revoking VCs, while the citizen is the recipient of these credentials. The CI is responsible for making the business decision to revoke a previously issued credential. The revocation process empowers the issuer to invalidate the digital VCs if they cease to be valid, thereby ensuring the security and trustworthiness of the digital VCs.

In a specific scenario, an issuer may need to revoke a previously issued EHIC or a PD A1, belonging to a citizen. Such revocation is triggered by alterations in the underlying conditions, such as a change in the citizen's social security status. This ensures that the digital VCs accurately reflect the correct status, maintaining their relevance and reliability.

5.5.2. Prerequisites Related to the Use Case

The following prerequisites ensure that the process of revoking digital VCs is efficient and secure:

- **Issuer System**: An issuer system capable of handling revocation must be established.
- **Revocation Registry**: A revocation registry is available and accessible.
- **EUDIW Installation and Functionality**: The EUDIW must be installed, functional, and the PID must be onboarded on the citizen's device.
- **Issued VC**: A previously issued credential must be available (at least at the issuer system, but desirably on the citizens EUDIW) in order to execute the revocation process.
- **Internet Connection**: An internet connection on the citizen's device is necessary to execute the whole workflow (including notification and self-verification) correctly.
- **Notification Services**: It notifies the citizen when a credential has been revoked.
- **Business Decision:** The business decision about the revocation of a credential by the respective CI has been made.

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

5.5.3. Roles, Activities and Tasks

CI	**National Demand for Revocation** The CI creates a demand for revocation of a credential and sends it towards the issuer system.
Issuer System	**Receive Demand** The Issuer System receives a demand from a CI to revoke a credential for a citizen. This demand is then processed within the system. The credential is revoked by updating a dedicated revocation registry. Upon completion of this process, the issuer system activates a notification protocol aimed at the citizen.
CI	**National Notification Protocol** The CI is responsible for initiating the notification service towards the citizen. This notification, generated within a national or institutional framework, serves to inform the citizen of the revocation of their digital credential.
Citizen	**Receive Notification** The citizen is notified via a notification framework, that their credential has been revoked.
Citizen	**Self-Verification (optional)** The citizen optionally initiates the EUDIW and triggers a check for the revocation status of their credential using the revocation registry. Following this, any necessary updates are made to the data stored within the EUDIW, ensuring that the citizen's credentials are always up to date.
Citizen	**Information** The citizen's wallet shows whether the credential has been revoked or not.

TABLE 7: REVOCATION OF CREDENTIALS – ROLES, ACTIVITIES AND TASKS

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

5.5.4. BPMN Diagram

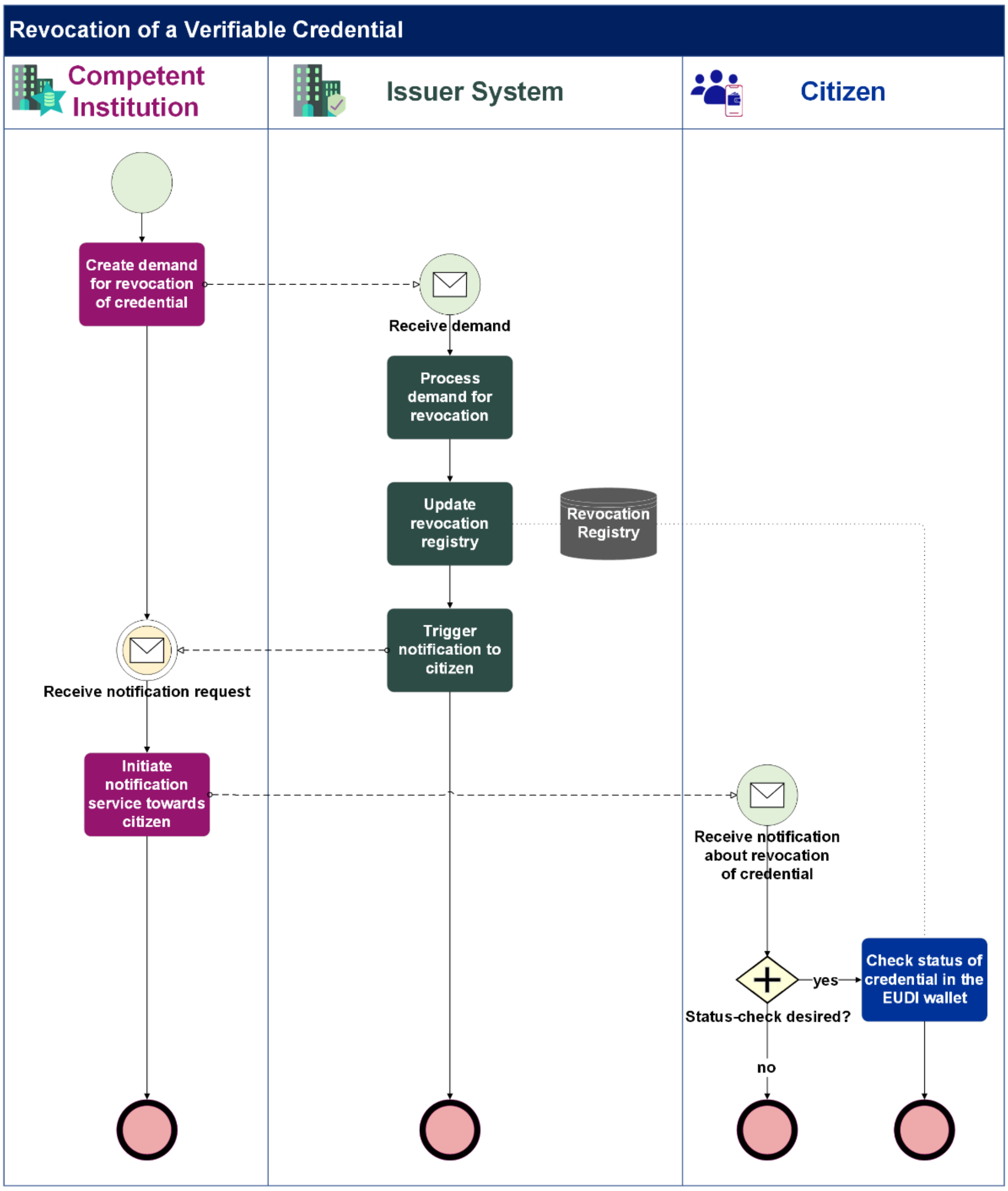

Revocation of a Verifiable Credential
Competent Institution
Issuer System
Citizen
Create demand for revocation of credential
Receive demand
Process demand for revocation
Update revocation registry
Revocation Registry
Trigger notification to citizen
Receive notification request
Initiate notification service towards citizen
Receive notification about revocation of credential
Status-check desired?
yes
no
Check status of credential in the EUDI wallet

FIGURE 24: REVOCATION OF A VERIFIABLE 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

5.5.5. High Level Requirements

REV01: A digital credential MUST be revocable. Only the authentic source or the QTSP which originally demanded the issuing of the credential MAY revoke the credential.

REV02: A VC MUST be revocable in (near) real-time.

REV03: The revocation status of a VC MUST be retrievable and processable for both relying parties and the holder of the credential.

REV04: The revocation registry MUST have electronic trust mechanisms in place to make sure it is trustworthy.

REV05: The revocation SHOULD be possible at any time (24/7).

REV06: To grant transparency also for a former validity status, the revocation registry MUST record information when (date & time) the VCs have been revoked. Retroactive revocation of business decision MUST NOT be possible.

REV07: The revocation registry MUST be available over the internet using standardised endpoints. Having access to a specific network or service MUST NOT be required.

REV08: The revocation registry SHOULD NOT require the verifier to authenticate itself to query the registry. User tracking by the registry provider MUST be minimised.

REV09: The revocation registry SHOULD NOT require the credential owner to authenticate itself to query the registry. User tracking by the registry provider MUST be minimised.

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

5.6. USE CASE 4: VERIFICATION OF CREDENTIALS AND IDENTITY

5.6.1. General Description

The paramount use case in this context is the verification of credentials. This process is carried out by verifiers who are qualified according to the standards set by the eIDAS regulation. It is crucial to have mutual trust in the relying party acting as Verifier, and their qualifications must be subject to verification by the EUDIW holder.

For instance, in the context of PD A1, a verifier could be the financial police or CI. They have the authority to request proof of the PD A1 credential and verify the identity of the citizen/holder. Similarly, in the context of the EHIC, a verifier could be a healthcare provider. These examples underscore the importance of the role of registered verifiers in maintaining the integrity of the VC system especially since person related, sensitive data is processed.

5.6.2. Prerequisites Related to the Use Case

The prerequisites for the successful implementation of the verification process are as follows:

- **EUDIW Installation and Functionality**: The EUDIW must be installed, functional, and the PID must be onboarded on the citizen’s device.
- **Stored Credentials**: The credentials must already be stored in the wallet and bound to the holder.
- **Registered Verifier**: The verifier must be registered in the system and qualified.
- **Service Accessibility**: All necessary services must be reachable from all the devices.
- **Verifier Application**: The verifier must have a Verifier Application installed.
- **Internet Connection:** A stable internet connection on the verifier’s device is required for the real-time revocation check. If this is not ensured, the revocation check can only be carried out for a past point in time (last date of synchronisation with the verifier’s device).

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

5.6.3. Roles, Activities and Tasks

Citizen	**Verification Situation** The citizen is temporarily staying or pursuing work outside the competent MS. The citizen needs to prove an attestation of social insurance and that they are the holder of the attestation.
Verifier	**Request Information** The Verifier opens their Verifier Application. The Verifier requests a VP and proof of the attestation to the citizen starting a Verifier App to EUDIW verification process. The Verifier identifies themself as a representative of an authorised entity.
Citizen	**Receiving Request** The citizen receives the request for presenting one or more specific credential(s) to the verifier. The EUDIW verifies the verifiers authenticity as well as their qualification to process the requested credential information and to check identity information.
Citizen	**Consent** The EUDIW records the presentation activity. The citizen accepts the request. The EUDIW presents the credential(s).
Verifier	**Verification** The Verifier App checks the EUDIW presentation and executes several verification steps: Issuer authenticity, issuer validity, identity binding, revocation. The Verifier App shows the results of the verifications in a user-friendly and consistent way. In case of a negative check the reasons should be visible.
Verifier	**Documentation** The Verifier App records a verification proof. If required, the Verifier App pushes a verification proof to a national institution for further procedures.
Institution	**Receive proof record (optional)** The national institution optionally receives a record of the proof of verification for further processing.

TABLE 8: VERIFICATION OF CREDENTIALS AND IDENTITY – ROLES, ACTIVITIES AND TASKS

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

5.6.4. BPMN Diagram

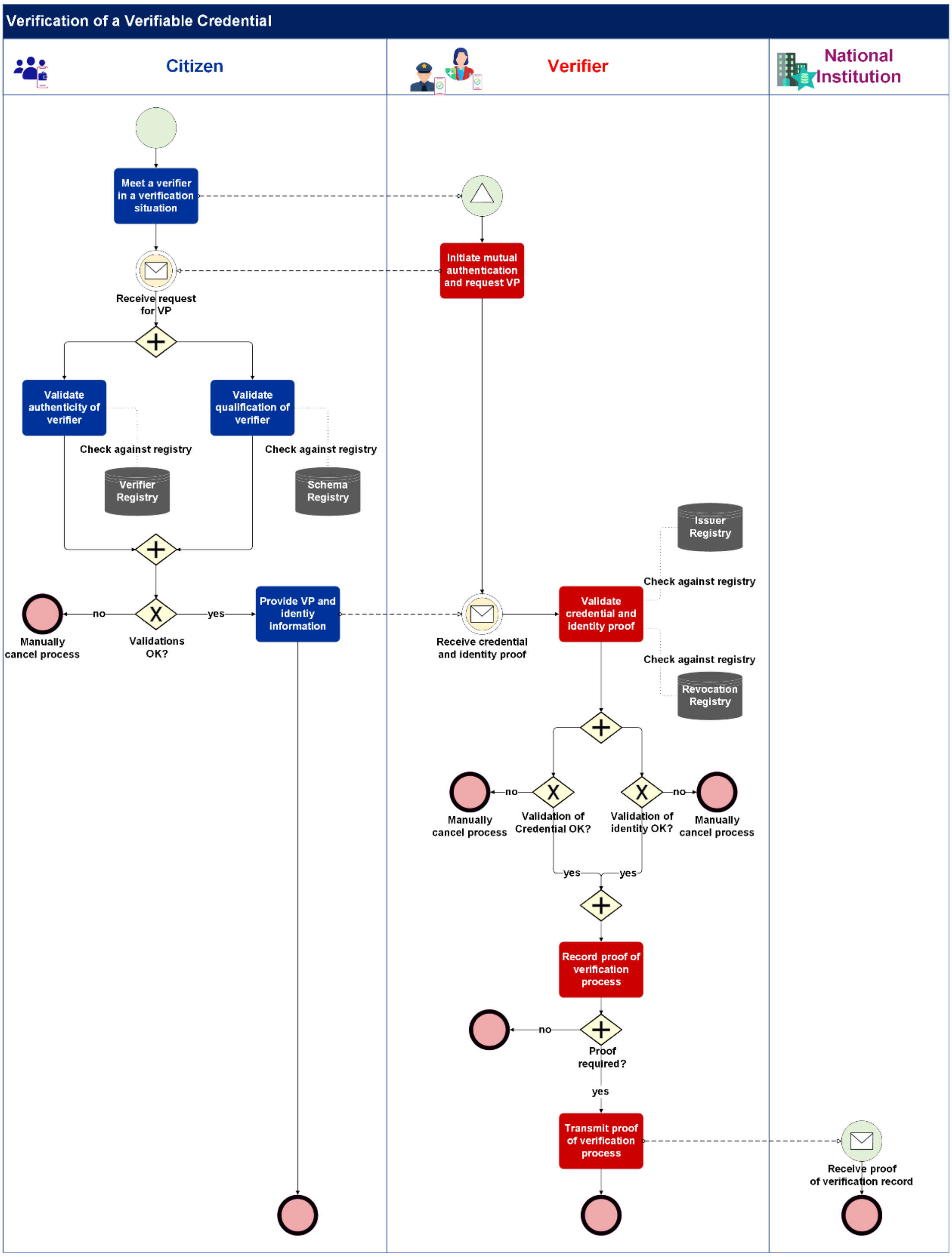

Verification of a Verifiable Credential
Citizen
Verifier
National Institution
Meet a verifier in a verification situation
Initiate mutual authentication and request VP
Receive request for VP
Validate authenticity of verifier
Validate qualification of verifier
Check against registry
Check against registry
Verifier Registry
Schema Registry
Issuer Registry
Check against registry
Manually cancel process
no
Validations OK?
yes
Provide VP and identiy information
Receive credential and identity proof
Validate credential and identity proof
Check against registry
Revocation Registry
Manually cancel process
no
Validation of Credential OK?
Validation of identity OK?
no
Manually cancel process
yes
yes
Record proof of verification process
no
Proof required?
yes
Transmit proof of verification process
Receive proof of verification record

FIGURE 25: VERIFICATION OF A VERIFIABLE 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

5.6.5. High Level Requirements

VER01: A seamless and trusted digital verification process MUST be initiated through a digital request for information from a verifier using a verifier application to a EUDIW.

VER02: The request for information from a qualified verifier application MUST be in accordance with the disclosure policy of social security coordination (see ISS08) and the eIDAS regulation.

VER03: The disclosure policy and the qualification of the verifier MUST be transparent to the EUDIW involved in the verification process.

VER04: A verifier application MUST have access to a rulebook defining the schemas, the disclosure policy for a specific credential type and other qualifications required to generate trust in the verification process.

VER05: The user MUST be able to verify the identity and qualifications of the verifier and verifier application involved in the verification process.

VER06: The user MUST consent by electronic means before presenting the information requested by the verifier application, either explicitly or implicitly by selecting the presentation to share in the EUDIW.

VER07: The user MUST be entitled to verify their identity and digital credential ownership by using a EUDIW as an electronic identification means.

VER08: The qualified verifier MUST have the possibility to digitally verify the validity and authenticity of the digital credential when the attributes from this digital credential are presented by a EUDIW.

VER09: The qualified verifier MUST be able to request necessary attributes about the credential owner, that are available in the VC to effectively execute the verification process.

VER10: The qualified verifier MUST be able to verify the legitimate possession/ownership of the digital credential solely by digital means when attributes about the digital credential owner are presented by a valid EUDIW.

VER11: The qualified verifier MAY process attributes supplied by a EUDIW, if it abides by regulated procedures anticipated in the context of social security coordination.

VER12: If a digital credential has been delegated to another valid EUDIW, this authorized delegation MUST be transparent to the verifier, when attributes from the delegated digital credential are presented by the EUDIW.

VER13: The qualified verifier MUST be able to verify the authorised delegation of a digital credential solely through digital means when attributes regarding a digital credential owner are presented by a EUDIW.

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

5.7. USE CASE 5: DELEGATION OF CREDENTIALS

5.7.1. General Description

This chapter describes possible scenarios which require the **delegation or transfer** of credentials. This can be achieved by considering the relationships between a subject, which is the digital identity to whom the credential is issued, and a holder, who stores the credential in their EUDIW.

The most common relationship is when a subject is equal to the holder. In this case, a verifier can easily deduce that a subject is the holder if the VP is digitally signed by the holder, and all contained VCs are about a subject that can be identified to be the same as the holder.

For **delegation** we consider the following **paradigm** defined by the ARF*: "As an EUDIW user, I want to delegate another EUDIW user to access specific services on my behalf, allowing them to represent me in transactions or interactions that I authorise."*

5.7.2. Subject Passes the Verifiable Credential to a Holder

Usually, VCs are presented to verifiers by the subject, which is the digital identity to whom the credential was issued. However, in some cases, the subject might need to transfer the VC to another holder. For example, if a patient is not able to use his/her EHIC, a relative can use a transferred EHIC to provide the necessary insurance status at a hospital.

The same model can be used to transfer the credential between two EUDIW owned by the same holder but having different digital identities (PIDs).

This case can be implemented by allowing the credential holder to issue a new VC and give it to the new holder, who can then present both VCs to the verifier (see non normative section of [18]).

If and how this special issuing capability will be implemented in the EUDIW is open and up to the EUDIW Toolbox. In DC4EU this scenario will be considered at a later stage.

The VC Data Model supports the holder acting on behalf of the subject in at least the following ways (see non normative section of [18]). The:

- Issuer can include the relationship between the holder and the subject.
- Issuer can express the relationship between the holder and the subject by issuing a new VC, which the holder utilises.
- Subject can express their relationship with the holder by issuing a new VC, which the holder utilises.

The delegation paradigm does not include the case where an issuer establishes a relationship between a subject and a different holder by issuing a new VC. In this case the new VC is referred to as representation credential and the data model for the credential must include the relationship between the holder and the subject to attest this claim. Requirements for representation are also included in the following.

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

5.7.3. High Level Requirements

DEL01 (ISS13): A verifiable digital credential MUST be issued in a way that it can be delegated to another EUDIW, and this delegation MUST be based on a verifiable consent from the original credential owner.

DEL02 (VER11): If a VC has been delegated to another EUDIW, this authorised delegation MUST be transparent to the verifier, when attributes from the delegated digital credential are presented by a EUDIW.

DEL03 (VER12): The qualified verifier MUST be able to verify the authorised delegation of a digital credential solely through digital means when attributes regarding a digital credential owner are presented by a EUDIW.

DEL04: The delegation of a verifiable digital credential MUST be authorised by the credential owner. Therefore, the transfer of rights MUST not be permissible.

DEL05: When delegating a digital VC, it MUST be mandatory to specify the validity period. This MAY be achieved either through user preferences for limited validity periods or by fixed duration.

DEL06: The relation between the holder and subject of a digital credential MUST be revocable by the authentic source that initially requested the issuing of a representation credential.

DEL07: The credential owner's authorisation of delegation MUST be recorded together with an identifier of the VC.

New requirements about the transfer of credentials between two EUDIWs of the same holder will be added if the EUDIW implementation and the ARF will be clearer and a secure and standardised process will be promoted, which ensures data integrity, privacy, and user consent.

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

6. PHYSICAL DATA MODEL

6.1. INTRODUCTION

VCs are especially useful for social security coordination, which is the process of ensuring that people who move within the EU do not lose their social security rights, such as pensions, health care, or unemployment benefits. Social security coordination is based on common rules (regulations) that are established at the EU level. These rules require different entities, such as social security institutions, employers, or health care providers, to exchange information about the social security status and entitlements of the people who move.

To make this information exchange easier, faster, and more secure, VCs will be used to digitally represent and verify the social security data of the people who move.

VCs will improve the efficiency, transparency, and security of the information exchange, as well as empower the users to control their own data and identity. To achieve these benefits, a consistent and well-defined data model for VCs for social security coordination is needed, which can be based on the EUDIW ecosystem and its related methods and technologies such as the identity framework.

A logical data model for VCs for social security coordination holds significance as:

- It enables the **interoperability and compatibility** of VCs across different systems, platforms, and domains in the EU, such as social security institutions, employers, and health care providers.
- It ensures the **security and trustworthiness** of VCs, by using cryptographic methods, distributed technologies, and legal frameworks to verify the authenticity and validity of the credentials and their issuers.
- It **enhances the user experience** and convenience of VCs, by allowing users to manage their own digital identities and credentials, and access social security services and benefits, using the EUDIW app and service.
- It supports the innovation and development of VCs, by providing a **common and standardised data model** that can be extended and customised for different use cases and scenarios in the social security domain.
- **Interoperability** between the different data models used in the social security domain should be achieved (e.g. EESSI).
- **Machine-verifiable exchange:** VCs are designed for fast machine-verifiable exchange of identity data and identity-related information without direct interaction between issuers and verifiers.

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

6.2. LOGICAL DATA MODEL

The logical data model is a structured way of describing all possible statements about a subject to be combined and processed in an issuing or verification process of social security credentials.

A data model for VCs in social security embedded in the EUDIW ecosystem is a way of presenting and sharing digital proofs of identity and social security entitlements, using the European Union Digital Identity (EUDI) framework. This framework is a set of standards and protocols that enable citizens, businesses, and government/public institutions to present and process identity data across the EU.

VCs in social security can be issued, stored, and verified by different entities, such as social security institutions, employers, or health care providers, using the EUDIW ecosystem.

A verification proof must be generated out of the data model and further processed by back-end systems.

The data model for VCs in social security embedded in the EUDIW ecosystem must follow the same structure and syntax as the W3C standard (see chapter 4.2), but with some specific features and extensions, such as:

- The use of the **eIDAS** framework to ensure the legal recognition and cross-border interoperability of the digital identities and VCs in the EU.
- The use of the **Trusted Registries** infrastructure to provide capabilities for the VCs, such as issuing, revoking, and verifying them in a secure way. This can be achieved by decentralised or centralised repositories.
- The use of defined business processes (see chapter 0) and data models (see chapter 6) for the VCs in the social security domain, such as the EHIC and the PD A1.
- The use of the **OpenID4VC** specification family to enable the authentication and authorisation of the subject of VCs using the OpenID Connect protocol.

Following the eIDAS regulation an Electronic Attestation of Attributes (EAAs) issued by or on behalf of a public body responsible for an authentic source shall contain:

1. an indication, at least in a form suitable for automated processing, that the **attestation has been issued as an electronic attestation of attributes issued by or on behalf of a public body** responsible for an authentic source.
2. a set of **data unambiguously representing the public body** issuing the electronic attestation of attributes, including at least, the member state (MS) in which that public body is established and its name and, where applicable, its registration number as stated in the official records.
3. **a set of data unambiguously representing the entity which the attested attributes are referring to**; if a pseudonym is used, it shall be clearly indicated.
4. the **attested attribute or attributes**, including, where applicable, the information necessary to identify the scope of those attributes.
5. details of the **beginning and end of the attestation's period of validity.**
6. the **attestation identity code**, which must be unique for the issuing public body and if applicable the indication of the **scheme of attestations** that the attestation of attributes is part of.
7. the **qualified electronic signature or qualified electronic seal** of the issuing body.
8. the information or location of the services that can be used to enquire about the validity status of the qualified attestation.

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

A VC data model for social security credentials consists of the following components which must be mapped with the components required above:

- □ A **context** property that provides information about the data model and vocabulary used in the credential. In the social security domain, this could take the form of the Schema (**Point 6, Point 1**) registry and a reference to a data dictionary which includes translations.
- □ An **ID** property that uniquely identifies the credential (**Point 6**).
- □ A **type** property that specifies one or more types of the credential, such as VC or a more specific type, such as “PD A1 Credential” or “EHIC Credential” (**Point 4, Point 1**).
- □ An **issuer** property that identifies the entity that issued the credential, such as a reference to an Issuer Repository. In social security it can be a reference to the IR with the Institution Code used in the IR (**Point 2**) is a promising candidate.
- □ An **issuanceDate** property that indicates when the credential was issued, such as a date-time string (**Point 5**).
- □ A **expirationDate** property that indicates when the credential expires, such as a date-time string (**Point 5**).
- □ A **credentialSubject** property that contains the claims and statements about the subject of the credential such as the reference to the digital identity to whom the credential was issued (**Point 3**).
- □ A **proof** property that contains cryptographic evidence that the credential is authentic and has not been tampered with, such as a digital signature or a zero-knowledge proof (**Point 7**).

To generate **zero knowledge proofs**, the data model of a credential must contain data which allow the generation of proofs of statements about the data, such as equality, inequality, or range.

To implement lean and user-oriented workflows for selective disclosure and zero knowledge proofs, the content should be structured in data blocks (claims), each of which should mirror a certain statement about the subject.

Social Security VCs are modelled in a way that identity information is exposed to any verifier by using the digital identity onboarded in the EUDIW (see chapter 5.3). That identity can be (optionally) presented in a verification challenge together with other optional attributes from a national PID schema (e.g. photo). Requesting PID data as a verifier needs a justified basis under GDPR.

Since the PID is bound to a EUDIW instance the data presented represents the identity of the person onboarded to the wallet and being the authorised holder of the VC (in figure 27 and figure 28 this is indicated by the block coloured in orange). The data, that is present in the PID can vary in different MS. The element 1.4 "Other element(s)" (see figure 27 and figure 28) represents the various elements, that different MS might have in their PID data. As per legal definitions, Person Identification Data (PID) is a set of data, but it is not itself an electronic identification means (on the contrary, PID is contained in an eID means). It is the EUDIW which is an electronic identification means, like others such as identity cards with enhanced security features (as per [20]).

The PID data together with the EUDIW serves as an identification means in a machine-verifiable process between a EUDIW and a verifier application. Additionally, the EUDIW capabilities will allow the verification of the identity of the holder as well as the holder/owner relationship by electronic means without the necessity to provide identity data points for identification.

The subject is the identity to whom the credential has originally been issued. The credential holder can be the subject of the credential or any other authorised person to whom the credential has been delegated for possible presentation. This delegation shall be executed

Co-funded by the European Union

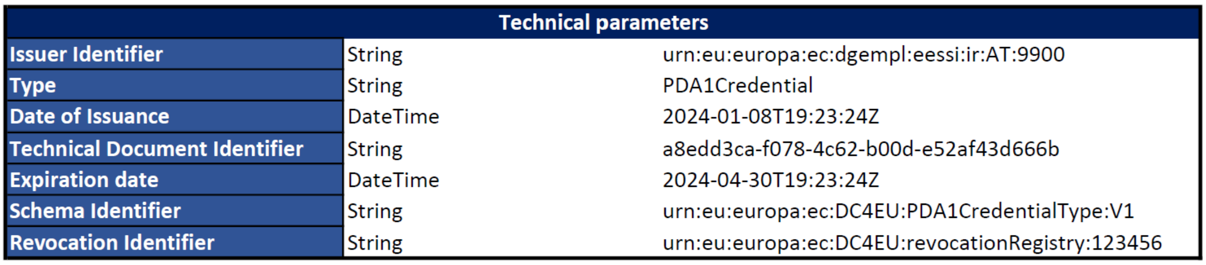
The DC4EU project is Co-funded by the European Union’s Digital Europe Programme under Grant Agreement no. 101102611

electronically by either issuing a credential out of an issuer system (representation credential) or by a EUDIW-to-EUDIW interaction based on the consent of the credential owner (delegation), see chapter 5.7.

A verification challenge shall not require any exposure of identity data in paper form. VCs stored in a EUDIW together with the wallet as an electronic identification means eliminate the need for extensive disclosure of identity data while ensuring authenticity. Consequently, **there are no requirements to have redundant information on personal identification attributes in the social security VC itself.**

The machine-verifiable processes are enforced by different data points and proofs included in the VC data model.

This is outlined through the following technical parameters required to construct a robust and Verifiable Presentation (VP) for social security coordination.



Technical parameters		
Issuer Identifier	String	urn:eu:europa:ec:dgempl:eessi:ir:AT:9900
Type	String	PDA1Credential
Date of Issuance	DateTime	2024-01-08T19:23:24Z
Technical Document Identifier	String	a8edd3ca-f078-4c62-b00d-e52af43d666b
Expiration date	DateTime	2024-04-30T19:23:24Z
Schema Identifier	String	urn:eu:europa:ec:DC4EU:PDA1CredentialType:V1
Revocation Identifier	String	urn:eu:europa:ec:DC4EU:revocationRegistry:123456

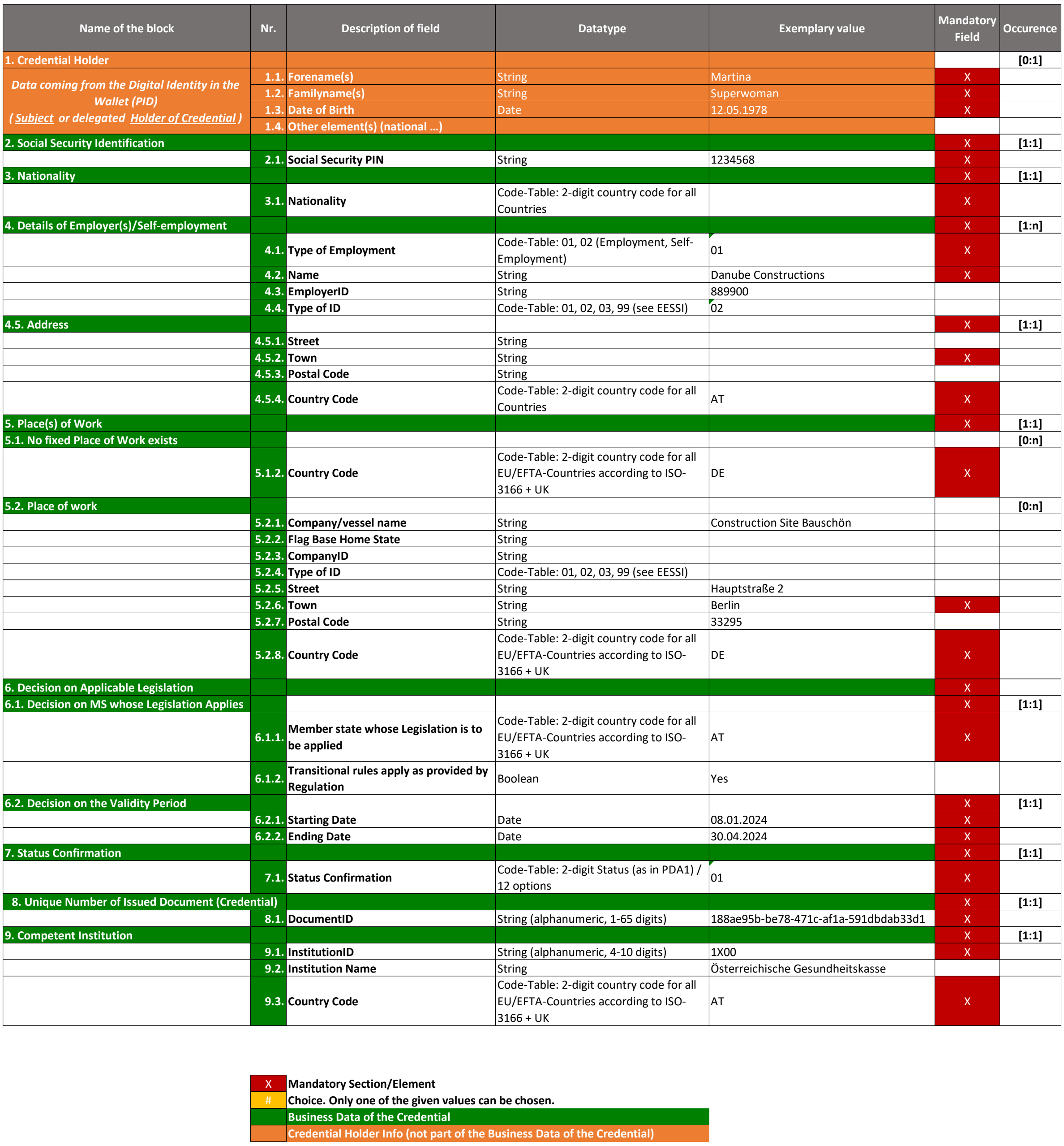
FIGURE 26: TECHNICAL PARAMETERS FOR THE VC DATA MODEL

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

6.3. DATA MODEL FOR THE PD A1

In the PD A1 Use Case, a representation scenario was not identified, hence there is no need for expressing the relationship between the holder and the subject.



Name of the block	Nr.	Description of field	Datatype	Exemplary value	Mandatory Field	Occurence
1. Credential Holder						[0:1]
Data coming from the Digital Identity in the Wallet (PID) *(Subject or delegated Holder of Credential)*	1.1.	Forename(s)	String	Martina	X	
	1.2.	Familyname(s)	String	Superwoman	X	
	1.3.	Date of Birth	Date	12.05.1978	X	
	1.4.	Other element(s) (national ...)				
2. Social Security Identification					X	[1:1]
	2.1.	Social Security PIN	String	1234568	X	
3. Nationality					X	[1:1]
	3.1.	Nationality	Code-Table: 2-digit country code for all Countries		X	
4. Details of Employer(s)/Self-employment					X	[1:n]
	4.1.	Type of Employment	Code-Table: 01, 02 (Employment, Self-Employment)	01	X	
	4.2.	Name	String	Danube Constructions	X	
	4.3.	EmployerID	String	889900		
	4.4.	Type of ID	Code-Table: 01, 02, 03, 99 (see EESSI)	02		
4.5. Address					X	[1:1]
	4.5.1.	Street	String			
	4.5.2.	Town	String		X	
	4.5.3.	Postal Code	String			
	4.5.4.	Country Code	Code-Table: 2-digit country code for all Countries	AT	X	
5. Place(s) of Work					X	[1:1]
5.1. No fixed Place of Work exists						[0:n]
	5.1.2.	Country Code	Code-Table: 2-digit country code for all EU/EFTA-Countries according to ISO-3166 + UK	DE	X	
5.2. Place of work						[0:n]
	5.2.1.	Company/vessel name	String	Construction Site Bauschön		
	5.2.2.	Flag Base Home State	String			
	5.2.3.	CompanyID	String			
	5.2.4.	Type of ID	Code-Table: 01, 02, 03, 99 (see EESSI)			
	5.2.5.	Street	String	Hauptstraße 2		
	5.2.6.	Town	String	Berlin	X	
	5.2.7.	Postal Code	String	33295		
	5.2.8.	Country Code	Code-Table: 2-digit country code for all EU/EFTA-Countries according to ISO-3166 + UK	DE	X	
6. Decision on Applicable Legislation					X	
6.1. Decision on MS whose Legislation Applies					X	[1:1]
	6.1.1.	Member state whose Legislation is to be applied	Code-Table: 2-digit country code for all EU/EFTA-Countries according to ISO-3166 + UK	AT	X	
	6.1.2.	Transitional rules apply as provided by Regulation	Boolean	Yes		
6.2. Decision on the Validity Period					X	[1:1]
	6.2.1.	Starting Date	Date	08.01.2024	X	
	6.2.2.	Ending Date	Date	30.04.2024	X	
7. Status Confirmation					X	[1:1]
	7.1.	Status Confirmation	Code-Table: 2-digit Status (as in PDA1) / 12 options	01	X	
8. Unique Number of Issued Document (Credential)					X	[1:1]
	8.1.	DocumentID	String (alphanumeric, 1-65 digits)	188ae95b-be78-471c-af1a-591dbdab33d1	X	
9. Competent Institution					X	[1:1]
	9.1.	InstitutionID	String (alphanumeric, 4-10 digits)	1X00	X	
	9.2.	Institution Name	String	Österreichische Gesundheitskasse		
	9.3.	Country Code	Code-Table: 2-digit country code for all EU/EFTA-Countries according to ISO-3166 + UK	AT	X	

X	Mandatory Section/Element
#	Choice. Only one of the given values can be chosen.
🟩	Business Data of the Credential
🟧	Credential Holder Info (not part of the Business Data of the Credential)

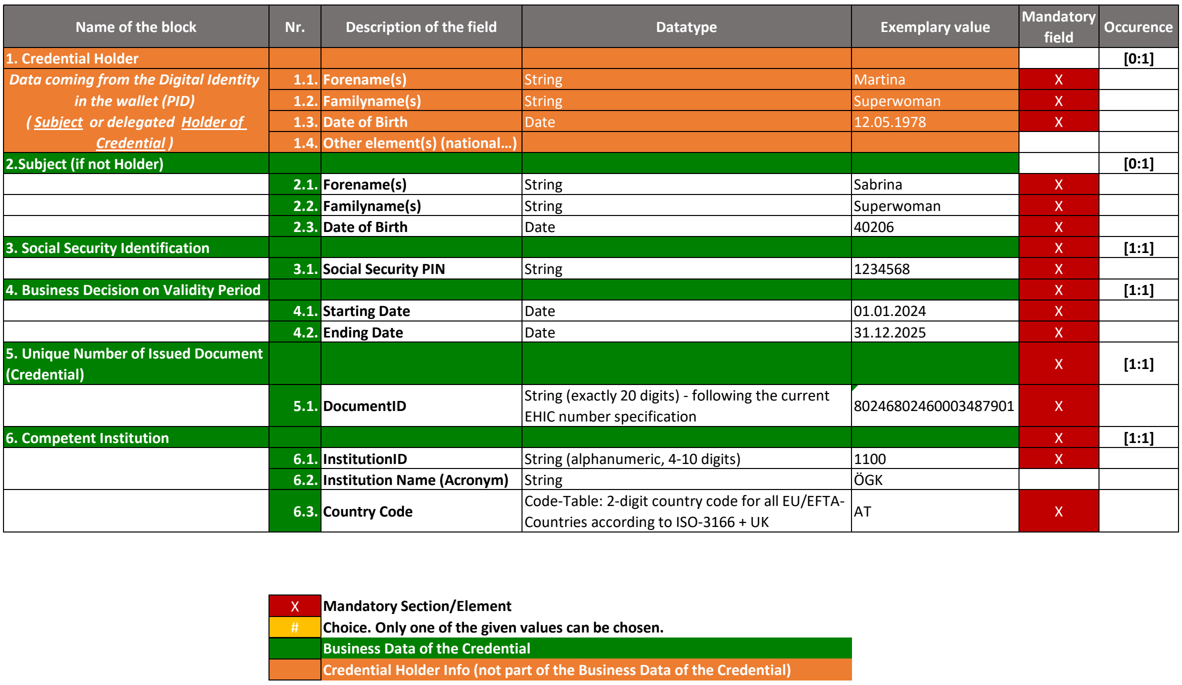
FIGURE 27: LOGICAL DATA MODEL FOR THE PD A1

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

6.4. DATA MODEL FOR THE EHIC

In the EHIC Use Case, a representation scenario was identified (e.g., parent/child), thus the expression of the relationship between the holder and the subject is modelled in the logical data model.



Name of the block	Nr.	Description of the field	Datatype	Exemplary value	Mandatory field	Occurence
1. Credential Holder						[0:1]
Data coming from the Digital Identity in the wallet (PID) (Subject or delegated Holder of Credential)	1.1.	Forename(s)	String	Martina	X	
	1.2.	Familyname(s)	String	Superwoman	X	
	1.3.	Date of Birth	Date	12.05.1978	X	
	1.4.	Other element(s) (national…)				
2.Subject (if not Holder)						[0:1]
	2.1.	Forename(s)	String	Sabrina	X	
	2.2.	Familyname(s)	String	Superwoman	X	
	2.3.	Date of Birth	Date	40206	X	
3. Social Security Identification					X	[1:1]
	3.1.	Social Security PIN	String	1234568	X	
4. Business Decision on Validity Period					X	[1:1]
	4.1.	Starting Date	Date	01.01.2024	X	
	4.2.	Ending Date	Date	31.12.2025	X	
5. Unique Number of Issued Document (Credential)					X	[1:1]
	5.1.	DocumentID	String (exactly 20 digits) - following the current EHIC number specification	80246802460003487901	X	
6. Competent Institution					X	[1:1]
	6.1.	InstitutionID	String (alphanumeric, 4-10 digits)	1100	X	
	6.2.	Institution Name (Acronym)	String	ÖGK		
	6.3.	Country Code	Code-Table: 2-digit country code for all EU/EFTA-Countries according to ISO-3166 + UK	AT	X	

X	Mandatory Section/Element
#	Choice. Only one of the given values can be chosen.
🟩	Business Data of the Credential
🟧	Credential Holder Info (not part of the Business Data of the Credential)

FIGURE 28: LOGICAL DATA MODEL FOR THE EHIC

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

7. ONBOARDING OF ACTORS

7.1. INTRODUCTION

This chapter delves into the onboarding business process for institutions in the context of the EHIC and the PD A1. In this chapter we aim to provide a framework for understanding and implementing the onboarding process, focusing on defining a robust trust framework, essential for the effective use of VCs. It navigates through the complexities of integrating existing structures and procedures (see chapter 2) and the eIDAS 2.0 trust framework (as already pointed out in chapters 1.2 and 3.4) into a coherent system. We also address the uniformity of the onboarding process for EHIC and PD A1, aiming to streamline the onboarding business process and ensure a seamless integration of institutions into the DC4EU project.

The framework needs to contain clear roles and processes on issuer, citizen, and verifier side. According to the phased approach of the project this document focuses on the issuer side. As there are no relevant differences on the onboarding process between the use cases, namely EHIC and PD A1, the process will be the same for both.

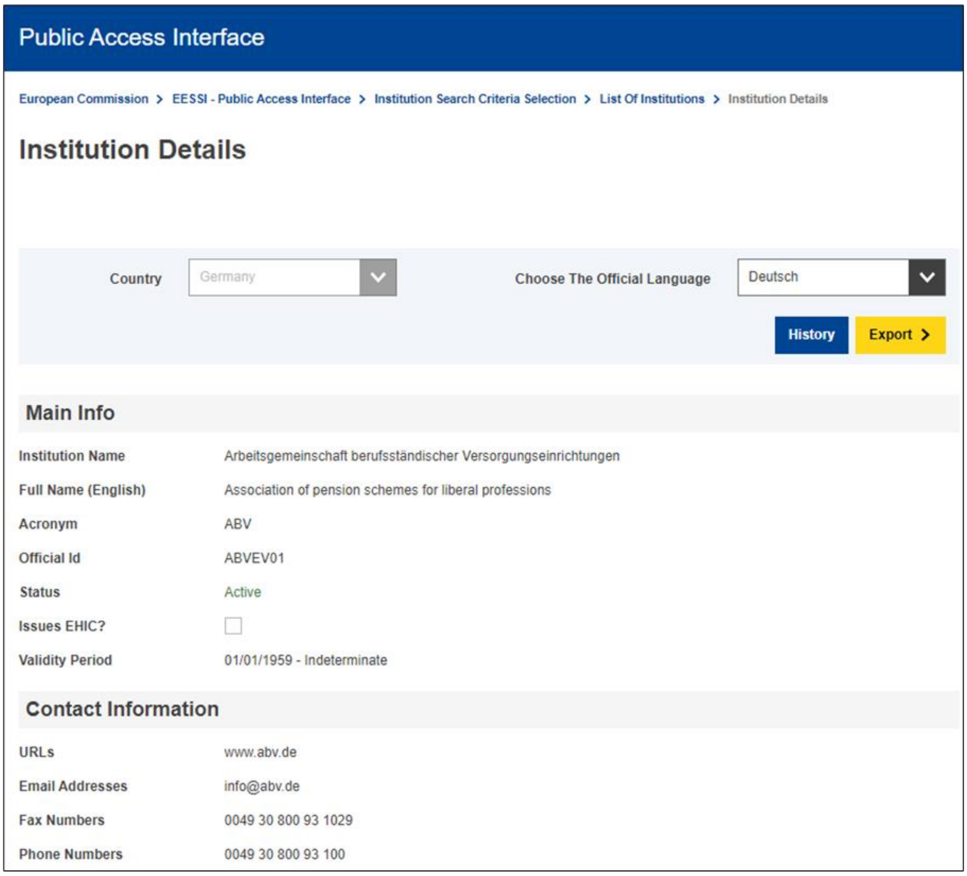
Regarding the definition of a trust framework for Issuers, the EESSI Institution Repository (IR) together with the eIDAS 2.0 trust framework are relevant and will be described in further detail below.

7.2. EESSI INSTITUTION REPOSITORY – A TRUST FRAMEWORK FOR SOCIAL SECURITY

Social security is a highly regulated domain with clear responsibilities defined through legal mandates. For the “EESSI” system a repository for trusted actors has already been established – the **EESSI IR**. The IR contains important aspects like official institution IDs, validity statuses, and (in-)direct rules regarding authorisations to issue certain 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


Public Access Interface
European Commission > EESSI - Public Access Interface > Institution Search Criteria Selection > List Of Institutions > Institution Details
History
Export >

Institution Details

Country: Germany

Choose The Official Language: Deutsch

Main Info

Institution Name	Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen
Full Name (English)	Association of pension schemes for liberal professions
Acronym	ABV
Official Id	ABVEV01
Status	Active
Issues EHIC?	□
Validity Period	01/01/1959 - Indeterminate

Contact Information

URLs	www.abv.de
Email Addresses	info@abv.de
Fax Numbers	0049 30 800 93 1029
Phone Numbers	0049 30 800 93 100

FIGURE 29: THE EESSI INSTITUTION REPOSITORY

New institutions that are to be added to the IR must be reported to the European Commission (EC) one month in advance by substantial change.

The IR also records whether an institution issues portable documents. In cases where an institution, already listed in the IR, is subsequently authorised to issue portable documents by law, this change can be communicated to the IR-SPOC, who will then update the IR to reflect this new capability.

The IR also records public keys for business certificates. These certificates are maintained to prove signatures in the EESSI data exchange.

7.3. EIDAS 2.0 TRUST FRAMEWORK

The ecosystem and trust framework of the EUDIW defines several key roles on the credential issuer side (see chapter 3.4).

All in all, issuers issue attestations based on their authorisation by National Accreditation Bodies (NAB) (**QEAA providers**) or based on their role as a public sector body responsible for an authentic source (**EAAPSB providers**) (thus creating a “chain of trust”). All those actors are overseen by Supervisory Bodies or Governmental structures. Attestation Providers/Issuers and Authentic Sources may be the same entity.

Those roles interact with other actors in the trust ecosystem which are not in special focus here – like Trusted List Providers, PID Providers and Wallet Providers. Besides that, it is relevant

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

to mention that in the credential issuing process the Issuer is also a Relying Party – as it requests, obtains, and verifies the citizen's personal identity data:

- **Relying Party**: *"A natural or legal person that relies upon an electronic identification or a Trust Service".*

The extent to which this impacts a distinct or a unified approach for (a) Trusted List(s) for Issuers and Verifiers needs to be examined (in collaboration with other work packages).

In any case, the Attestation Providers must be properly registered to allow the required secure "**mutual authentication**" towards the citizen – as the citizen has to be sure (or "trust") that the attestation they are requesting comes from an authorised institution. This authorisation should not only cover the fact that an institution is allowed to issue a credential – it should also state that an institution is allowed to issue the specific requested type of credential (such as the PD A1 or EHIC).

Relevant for the trust framework design is also the necessary or desired "level" of trust – here it has to be considered that eIDAS 2.0 states that the issuance of credentials can be done in a qualified and non-qualified way, but there are also special requirements for a new third type: "electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source" ([1], Art. 45da).

The different eIDAS roles, authorisations, and the relations towards each other must be covered by a DC4EU solution.

7.4. ONBOARDING IMPLEMENTATION

To implement the above outlined trust framework and to be able to issue and use credentials in a trustworthy environment, adequate onboarding services or mechanisms have to be defined and implemented according to the different options of the trust model.

7.4.1. Onboarding Issuers

As mentioned above, social security is a highly legally regulated area with clearly defined responsibilities that are determined by legal requirements.

A repository for trusted actors based on [4]Article 88 has already been set up for the "EESSI" system - the EESSI IR. The trusted actors are the bodies referred to in Article 1(m), (q) and (r) of the [3] and Article 1(2)(a) and (b) of the [4], and of the institutions designated in accordance with the [4].

Which institutions are authorised to issue EHIC/PD A1 is highly determined by national law.

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

Total number of EHIC and PD A1 issuing institutions in the IR:

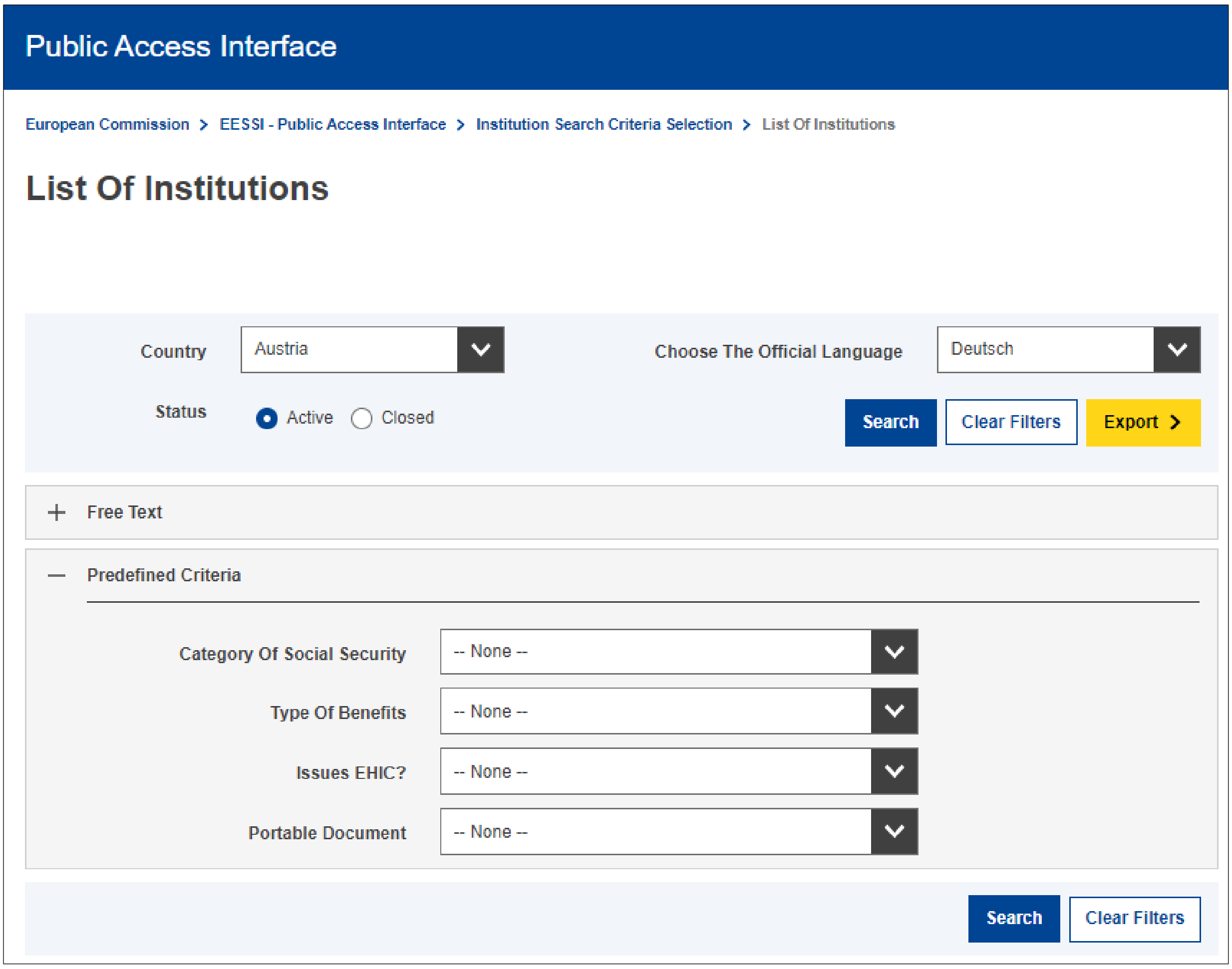
Country	EHIC	PD A1
AT	39	46
BE	49	4
BG	1	1
CH	0	95
CY	0	1
CZ	85	85
DE	96	116
DK	1	0
EE	1	1
EL	34	103
ES	80	56
FI	1	1
FR	309	242
HR	20	1
HU	20	20
IE	44	1
IS	1	1
IT	109	6
LI	3	2
LT	5	1
LU	4	1
LV	1	1
MT	1	2
NL	31	0
NO	1	0
PL	16	59
PT	23	23
RO	0	1
SE	1	1
SI	10	3
SK	3	88
UK	4	2
Total	**989**	**962**

TABLE 9: TOTAL NUMBER OF EHIC AND PD A1 ISSUING INSTITUTIONS IN THE INSTITUTION REPOSITORY

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 analysis of the issuers was done in the IR using the search function in each country. Search for "Issues EHIC? - yes/no" and search for "PD A1 and EHIC".



Public Access Interface

European Commission > EESSI - Public Access Interface > Institution Search Criteria Selection > List Of Institutions

List Of Institutions

Country: Austria

Choose The Official Language: Deutsch

Status: ● Active ○ Closed

Category Of Social Security: -- None --

Type Of Benefits: -- None --

Issues EHIC?: -- None --

Portable Document: -- None --

FIGURE 30: THE EESSI INSTITUTION REPOSITORY – PUBLIC ACCESS INTERFACE – SEARCH. SOURCE: [11]

DC4EU has to find a way to transfer this structure – and/or to onboard the participating institutions according to this repository – into a trusted list usable for our use cases. For this purpose, the “Issuer System” needs a designated onboarding service. To create an aligned solution for this, work package 6 delivers the relevant business input to the other involved work packages. Also, the use of a Public Key Infrastructure (PKI) for proving business signatures must be considered.

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

7.4.2. Onboarding Citizens

It is the EUDIW, together with the PID, which is an electronic identification means. The PID in the EUDIW is a unique set of identity data assigned to this digital identity. This digital identity is used to onboard citizens to the EUDIW ecosystem. Please find more details in chapter 5.

7.4.3. Onboarding Verifiers

As mentioned above, in this project phase our focus lies more on the Issuer than on the Verifier side. Nevertheless, DC4EU will briefly also design and implement the relevant procedures for Verifiers. The goal is to onboard the participating institutions as relying parties with certain authorities for verifying identity and specific credentials – combined with an ability to identify themselves towards a citizen. An onboarding service for the Verifier/Verifier System/Verifier App will also be elaborated and aligned in DC4EU using business input by WP 6. Additionally, it has to be embedded in the overall strategy for registering qualified verifiers in the EUDIW 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

8. LIST OF FIGURES

Figure 1: Roles and entities in the EUDIW ecosystem 4
Figure 2: Coverage by country 18
Figure 3: Issuance of PD A1........ 23
Figure 4: Verification of PD A1 25
Figure 5: The EESSI Institution Repository – Public Access Interface – Issuer of Portable Documents. Source: [11] 27
Figure 6: Automatic issuance of EHIC 34
Figure 7: Issuance of EHIC upon request 35
Figure 8: Issuance of PRC 36
Figure 9: Verification of EHIC/PRC 38
Figure 10: The EESSI Institution Repository – Public Access Interface – Issuer of Portable Documents. Source: [11] 40
Figure 11: Conceptual Architecture........ 60
Figure 12: The roles and information flows forming the basis for this specification [18]. 66
Figure 13: The basic structure of a claim 67
Figure 14: Claim Structure: janeroe is insured at the competent institution........ 67
Figure 15: Claim Structure: johndoe is father of janeroe and janeroe is insured at competent institution 68
Figure 16: Basic components of a Verifiable Credential. 68
Figure 17: Detailed depiction of a Verifiable Credential ([19, pp. 164-194] 69
Figure 18: Information graphs associated with a basic Verifiable Credential [18]. 70
Figure 19: Basic components of a Verifiable Presentation [18]. 71
Figure 20: Detailed depiction of a Verifiable Presentation [19, pp. 164-194]. 72
Figure 21: Information graphs associated with a basic Verifiable Presentation [18]. 73
Figure 22: Onboarding of the EUDIW 79
Figure 23: Issuance of a Verifiable Credential 83
Figure 24: Revocation of a Verifiable Credential........ 87
Figure 25: Verification of a Verifiable Credential........ 91
Figure 26: Technical parameters for the VC data model 98
Figure 27: Logical data model for the PD A1 99
Figure 28: Logical data model for the EHIC 100
Figure 29: The EESSI Institution Repository........ 102
Figure 30: The EESSI Institution Repository – Public Access Interface – Search. Source: [11]........ 105
Figure 31: EHIC Standard 121
Figure 32: EHIC Delegation........ 121
Figure 33: EHIC Representation 122
Figure 34: EHIC Delegation (Representation)........ 122
Figure 35: PD A1 Standard 123
Figure 36: PD A1 Delegation........ 124
Figure 37: Technical Integration of Authentic Source Backend System (Reference implementation). Issuer of Verifiable Credentials acts on behalf of one or more Authentic Sources. 125
Figure 38: Technical Integration of Authentic Source Backend System. The Authentic Source is also the Issuer of Verifiable Credentials 126

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

9. LIST OF TABLES

Table 1:Four basic scenarios of wallet and identity usage 9
Table 2: List of portable documents 13
Table 3: Return rate of the questionnaires EHIC & PD A1 17
Table 4: Central repository for PD A1 22
Table 5: Onboarding of the EUDIW - Roles, activities and tasks 78
Table 6: Issuance of Verifiable Credentials – Roles, activities and tasks 82
Table 7: Revocation of Credentials – Roles, activities and tasks 86
Table 8: Verification of Credentials and identity – Roles, activities and tasks 90
Table 9: Total number of EHIC and PD A1 issuing institutions in the Institution Repository 104

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

10. ABBREVIATIONS AND TERMS

Term	Description
(Qualified) Trust Service Provider (QTSP)	A Qualified Trust Service Provider (QTSP) is an entity legally recognized under EU law to provide trust services such as electronic signatures, seals, time stamps, and certificate validation. QTSPs must meet specific stringent security and compliance standards to ensure the authenticity and integrity of their services, helping enhance trust in electronic transactions across the EU.
Administrative Commission (AC)	The Administrative Commission for the Coordination of Social Security Systems in the EU is an official body that facilitates the consistent application of EU regulations on social security for workers moving within the EU. It provides guidance and clarification on the rules that protect the social security rights of these workers, ensuring they can access benefits like healthcare, pensions, and unemployment insurance while abroad. The commission also helps resolve disputes between member states regarding social security coverage and plays a key role in updating and adapting the rules in response to new legal and social developments.
Application for Credential	The process of applying for a credential from an authentic source, prior to issuance and pickup. This process will entail the registration of the person ID, most likely in the form of a local ID combined with an eID.
Architecture Reference Framework (ARF)	A set of common standards and technical specifications, and a set of common guidelines and best practices
Authentic Source	A repository or system, held under the responsibility of a public sector body or private entity, that contains attributes about a natural or legal person and is considered to be the primary source of that information or recognised as authentic in national law. Often synonymous with the competent institution (CI) that is behind a given business decision and the corresponding 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

Term	Description
Biometric Data	The data that forms the basis for comparison during biometric authentication, usually a stored template of a biometric trait. In the case of the EUDIW, most likely in the form of a portrait picture of the holder as part of the PID.
Claim	An assertion made about a subject which is a separately provable set of data points. The minimum granularity of a VP and VC.
Competent Institution (CI)	Institution that is behind a given business decision and the corresponding credential. It is the owner of the authentic source (System).
Conformity Assessment Bodies (CABs)	Conformity Assessment Bodies (CABs) are organizations authorized to evaluate whether products, services, systems, or personnel meet specified requirements outlined in regulations or standards. These assessments ensure compliance and are essential for certifying that products are safe and reliable before they reach the market.
Consent	During a verification challenge, the holder would need to give consent for their personal data to be processed. Upon consent, this involves selecting the necessary documents stored locally on their digital wallet to reply to a request. The selected information is then securely sent for verification. The process is designed to ensure the privacy and security of the holder's data, in line with the principles of the GDPR.
Credential Holder	A person or system that possesses and uses digital credentials, such as username and password, smart cards, or digital certificates, to authenticate and gain access to secure systems or services.
Credential Holder	The entity that is holding a wallet or the VCs and presents a VP to a verifier. It could be the VC subject but also another authorised natural or legal person.
Credential Offer	A link to an Issuers system, providing direct access to retrieve a specific VC. Access via the link is secured by the session within which the exchange takes place.
Data Point	The minimum granularity of identifiable information.

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

Term	Description
DC4EU	Digital Credentials for Europe
Device Binding	A cryptographical measure to ensure that a credential was issued to a specific device i.e. Smart Phone, Computer or Security Token. This binding is what provides the trust basis for uniqueness and coherence for credentials on the device. The device binding serves as an indirect binding between the credentials and the Identity bound to the device. [See “Holder Binding”]
eID	eID is a set of services provided by the European Commission (EC) to enable the mutual recognition of national electronic identification schemes (eID) across borders. It allows European citizens to use their national eID when accessing online services from other European countries. A national solution for electronic identification of natural and legal persons. In this context it is an eIDAS compliant notified eID scheme, allowing for cross-border activities. A somewhat contented part of the eIDAS amendment proposal is the requirement for a persistent globally unique identification element in all eID schemes.

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

Term	Description
Electronic Attestation of Attributes (EAA) **&** **Qualified Electronic Attestation of Attributes (QEAA)**	A distinction needs to be made between EAAs (electronic attestation of attributes) and QEAAs (qualified electronic attestation of attributes): EAAs can originate either from government-authorised sources or from sources that are not "authentic sources". However, EAAs from state-authorised registers automatically fulfil the value of a QEAA and can be issued directly into the Wallet, while other EAAs do not have the same evidential value as a paper certificate or ID. Attributes from sources not authorised by the state therefore only achieve the status of a QEAA if they have been checked and validated by a Qualified Trust Service Provider (QTSP). The attribute must be applied for via an eIDAS-compliant issuing process to be issued as a QEAA into the EUDIW.
EUDIW Toolbox	The EUDIW Toolbox is a set of technical standards and specifications that will provide a secure and convenient way for European citizens and businesses to share identity data needed for accessing digital services such as checking in at the airport, renting a car, opening a bank account, or when logging in to their accounts on large online platforms. The toolbox includes a technical Architecture and Reference Framework (ARF), a set of common standards and technical specifications, and a set of common guidelines and best practices.
European Digital Identity Wallet (EUDIW)	EUDIW is a product and service that allows the user to store identity data, credentials and attributes linked to their identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals. Each member state (MS) is required to provide at least one notified EUDIW solution for their citizens.
General Data Protection Regulation (GDPR)	The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Key elements include strict rules on data processing and consent, mandatory breach notifications, and significant penalties for non-compliance. It was implemented on May 25, 2018.

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

Term	Description
Holder / Identity Binding	An indirect relation between an Identity Credential and other VCs stored in a device. Control of the device and possibly biometric information held on the device, constitutes the holder binding. See device binding and biometric data.
Identity Context	In an EUDIW, the PID sets up a context around the credentials held in the wallet. This context allows for a secure combination of attestations from different credentials within the context. In the pure form, with only one identity in the wallet, the context is delegated to the device, such that the device ensures the validity of attestation combinations from the wallet. In a more natural situation, a EUDIW might hold credentials for more than one Identity (e.g. delegation), which would require multiple Identity Contexts within the EUDIW. Such a situation would require the Identity Context to be defined by both the device identifier and the relevant Identity for the Identity Context.
Identity Credential	A digital credential containing identity attestations at a certain Level of Assurance (LoA). Currently only the PID-credential has been designated in the EUDIW ecosystem as a Digital Identity Credential with LoA 'high'. Other credentials might be designated as identity credentials - notably various sector specific identity credentials.
Identity Holder Authentication	The process of verifying the identity of an individual or system seeking access to a secure service or resource, typically through the presentation of valid credentials.
Institution Repository (IR)	IR used in Electronic Exchange of Social Security Information (EESSI) for the qualification of CI in social security.
Institutional Repository-Single Point of Contact (IR-SPOC)	IR-SPOC used in EESSI for the maintenance of the IR.

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

Term	Description
Interoperability	The exchangeability between a range of products, or similar products from several different providers, or even between past and future revisions of the same product. Interoperability may be developed post-facto, as a special measure between two products, while excluding others, by using open standards. When a vendor is forced to adapt its system to a dominant system that is not based on open standards, it provides compatibility rather than interoperability.
Issuer	A role an entity can perform by asserting claims about one or more subjects, creating a VC from these claims, and transmitting the VC to a holder.
Issuer System	The System, responsible for producing a VC, operated by either an authentic source or an assigned trusted issuer. The process is to be performed at the time of collection by the recipient/subject, to ensure device binding.
Member States (MS)	refers to the member states of the European Union.
Minimal Credential	[See "Normalised Credential"].
National Accreditation Bodies (NABs)	National Accreditation Bodies (NABs) are organizations recognized by national governments to assess and accredit conformity assessment bodies (CABs) against international standards. NABs ensure that CABs are competent and capable of performing their services, which helps maintain the reliability and quality of certifications in various sectors.
Natural vs Legal Person	A natural person is a human being and living person. A legal person is being, real or imaginary whom the law regards as capable of rights and duties.
Near Field Communication (NFC)	Near Field Communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within a few centimetres of each other. NFC is used for a variety of applications, including contactless payments, access control, and quick data exchanges between devices.

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

Term	Description
OpenID Connect for Verifiable Credentials **(OIDC4VC)**	Open ID Connect for VCs is a protocol for the secure exchange of credential information. OpenID for VCs consists of three specifications: 1. OpenID for VC issuance – Defines an API and corresponding OAuth-based authorisation mechanisms for issuance of VCs (Editors' Draft) (Working Group Draft). 2. OpenID for VPs – Defines a mechanism on top of OAuth 2.0 to allow presentation of claims in the form of VCs as part of the protocol flow (Editors' Draft) (Working Group Draft) (Implementer's Draft). 3. Self-Issued OpenID Provider v2 – Enables users to use OpenID Providers (OPs) that they control (Editors' Draft) (Working Group Draft) (Implementer's Draft).
Person Identification Data (PID)	"Person Identification Data" means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established.
Personal Identification Number (PIN)	A National or sector specific identification scheme, such as a national social security number or pension ID.
Pre-authenticated Credential Offer	A link to an Issuers system, providing direct access to retrieve a specific VC. Often in the form of a QR Code. Access via the link is anonymous (pre-authenticated) and as such it must be protected by some out-of-band mechanism, such as one-time code. It is defined in the OpenID for VC issuance specification and only enables the option to define a PIN-Code, not related to the Personal Identification Number as defined previously, to be transmitted for authentication.
Primary Attestation Set	The main set of claims of a VP, as related to the circumstantial claims i.e. EHIC and associated identity.
Relying Party	A natural or legal person that relies upon an electronic identification or a trust service.

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

Term	Description
Repository	A database, such as a storage vault or personal VC wallet, that stores and protects access to the holder's VCs.
Selective Disclosure	The ability of a holder to make fine-grained decisions about what information to share. VCs enable selective disclosure, meaning that individuals can choose which credentials and/or data points to present to a verifier based on the context and the verifier's requirements. This enhances privacy and minimises the sharing of unnecessary personal information.
Self-Sovereign Identity (SSI)	VCs play a crucial role in decentralised and self-sovereign identity systems. In such systems, individuals have greater control over their personal information and can selectively share VCs with entities they trust, without revealing unnecessary or sensitive data.
User	Users of EUDIW are defined as natural or legal persons using the EUDIW to receive, store and share attestations (PID, QEAA or EAA) and attributes about the user, including to prove their identity. The EUDIW would enable users to create qualified electronic signatures and seals (QES). Who can be a user of a EUDIW depends on national law. The use of a EUDIW by citizens would not be mandatory under the legislative proposal. However, MSs would be obliged to offer the EUDIW to their citizens.
Validation	The assurance that a VC or a VP meets the needs of a verifier and other dependent stakeholders.
Verifiable Credential (VC)	A set of digitally signed, machine readable, attestations of attributes proving some facts about a subject. This is a piece of information or a claim about an individual or entity that can be cryptographically verified. It is a fundamental concept in the realm of digital identity and decentralised identity systems. VCs provide a way for individuals or organisations to assert and prove various attributes or qualifications about themselves without revealing unnecessary personal data.

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

Term	Description
Verifiable Presentation (VP)	Data derived from one or more VCs, issued by one or more issuers, that is shared with a specific verifier. A VP is a tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. [See "Shared Verifiable Presentation"]
Verification	The evaluation of whether a credential (or presentation) is an authentic and timely statement of the issuer or presenter, respectively. This includes checking that: the credential (or presentation) conforms to the specification; the proof method is satisfied; and, if present, the status check succeeds.
Verifier	A role an entity performs by receiving one or more VCs inside a VP for processing. Other specifications might refer to this concept as a relying party.
Electronic Identification, Authentication and Trust Services (eIDAS)	eIDAS, is a regulation set by the European Union to oversee electronic identification and trust services for electronic transactions within the EU. It establishes a legal framework to ensure that electronic interactions and transactions are secure, and it facilitates the use of electronic identification means and trust services across EU member states. This regulation helps increase the effectiveness and security of digital services and enables seamless electronic interactions between businesses, citizens, and public authorities across the EU.

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

11. REFERENCES

[1] The European Parliament and the Council, “Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework,” 30 04 2024. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401183. [Accessed 30 04 2024].

[2] E. Commission, “Forms that certify your benefits situation when moving within the EU,” European Commission, https://europa.eu/youreurope/citizens/work/unemployment-and-benefits/social-security-forms/index_en.htm, 2023.

[3] The European Parliament and the Council, “Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems,” EUR-Lex, 29 04 2004. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004R0883&qid=1705503929243. [Accessed 17 01 2024].

[4] The European Parliament and the Council, “Regulation (EC) No 987/2009 of the European Parliament and of the Council of 16 September 2009 laying down the procedure for implementing Regulation (EC) No 883/2004 on the coordination of social security systems,” EUR-Lex, 16 09 2009. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009R0987&qid=1705503518918. [Accessed 17 01 2024].

[5] The Administrative Commission for the Coordination of the Social Security Systems, “Decision No A1 of 12 June 2009 concerning the establishment of a dialogue and conciliation procedure concerning the validity of documents, the determination of the applicable legislation and the provision of benefits under Regulation (EC) No 883/2004,” EUR-Lex, 12 06 2009. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0424%2801%29. [Accessed 18 01 2024].

[6] The Administrative Commission for the Coordination of Social Security Systems, “Decision No A2 of 12 June 2009 concerning the interpretation of Article 12 of Regulation (EC) No 883/2004 on the legislation applicable to posted workers and self-employed workers temporarily working outside the competent state,” EUR-Lex, 12 06 2009. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0424%2802%29. [Accessed 17 01 2024].

[7] Decision No A3 of 17 December 2009, “ACT concerning the conditions of accession of the Kingdom of Norway, the Republic of Austria, the Republic of Finland and the Kingdom of Sweden and the adjustments to the Treaties on which the European Union is founded,” EUR-Lex, 17 December 2009. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:11994NN01/05/A3.

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

[8] The Administrativ Commission for the Coordination of Social Security Systems, “Recommendation No A1 of 18 October 2017 concerning the issuance of the attestation referred to in Article 19(2) of Regulation (EC) No 987/2009 of the European Parliament and of the Council,” EUR-Lex, 18 10 2017. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0529(01)&rid=7. [Accessed 17 01 2024].

[9] The Administrativ Commission for the Coordination of Social Security Systems, “Recommendation H2,” EUR-Lex, 10 10 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H0429(01)&from=EN. [Accessed 07 03 2024].

[10] The Administrative Commission for the Coordination of Social Security Systems, “Decision No E2 of 3 March 2010 concerning the establishment of a change management procedure applying to details of the bodies defined in Art.1 of Regulation (EC) No 883/2004 which are listed in the electronic directory which is an inherent part of EESSI,” EUR-Lex, 03 03 2010. [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:187:0005:0006:EN:PDF. [Accessed 16 01 2024].

[11] European Commission, “EESSI - Public Access Interface,” ec.europa.eu, [Online]. Available: https://ec.europa.eu/social/social-security-directory/pai/select-country/language/en). [Accessed 09 02 2024].

[12] The Administrativ Commission for the Coordination of Social Security Systems, “Decision No S1 of 12 June 2009 concerning the European Health Insurance Card,” EUR-Lex, 12 06 2009. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0424%2808%29. [Accessed 17 01 2024].

[13] The Administrative Commission for the Coordination of Social Security Systems, “Decision No S2 of 12 June 2009 concerning the technical specifications of the European Health Insurance Card,” EUR-Lex, 12 06 2009. [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:106:0026:0039:EN:PDF. [Accessed 09 02 2024].

[14] The Administrative Commission for the Coordination of Social Security Systems, “Decision No A2 of 12 June 2009 concerning the interpretation of Article 12 of Regulation (EC) No 883/2004 on the legislation applicable to posted workers and self-employed workers temporarily working outside the competent state,” EUR-Lex, 12 06 2009. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0424%2802%29. [Accessed 17 01 2024].

[15] The European Parliament and the Council,, “Regulation (EU) No 1231/2010,” EUR-Lex, 24 11 2010. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010R1231. [Accessed 07 03 2024].

[16] The European Parliament and the Council, 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) (Text with EEA

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

relevance),” EUR-Lex, 27 04 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed 16 01 2024].

[17] The European Parliament and the Council, “Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93,” EUR-Lex, 09 07 2008. [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32008R0765. [Accessed 20 01 2024].

[18] W3C, “Verifiable Credentials Data Model v1.1,,” https://www.w3.org/TR/2022/REC-vc-data-model-20220303/, 2022.

[19] Preukschat, Alex, Self-sovereign Identity: Decentralized Digital Identity and Verifiable Credentials, Manning Publications, 2021-06-01.

[20] The European Parliament and the Council, “Regulation (EU) 2019/1157 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement,” EUR-Lex, 20 06 2019. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R1157. [Accessed 12 03 2024].

Co-funded by the European Union

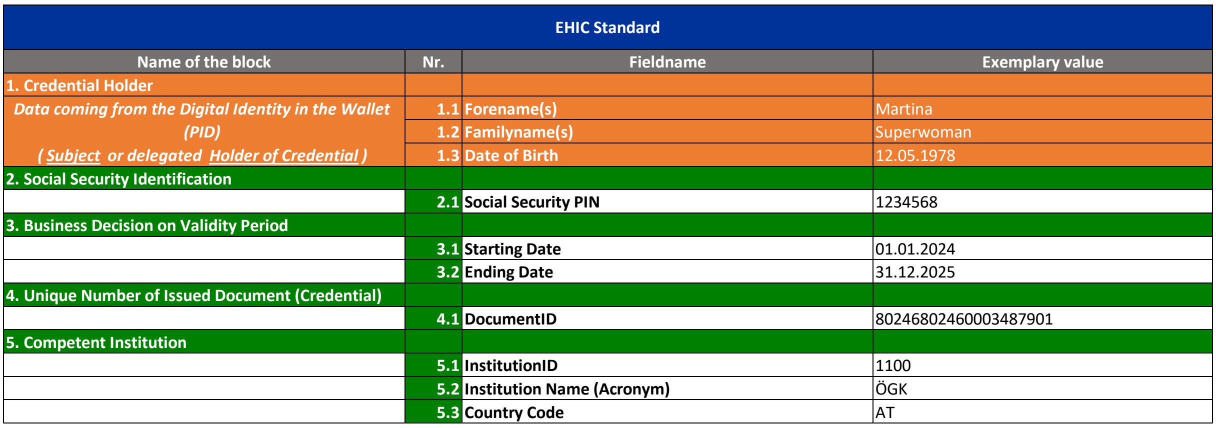
The DC4EU project is Co-funded by the European Union’s Digital Europe Programme under Grant Agreement no. 101102611

12. APPENDIX A – EXAMPLES OF THE DATA MODEL

To illustrate the application of the data models, you can find the following sample Verifiable Presentations (VPs) that can be used according to the different scenarios.

EHIC Standard

This presentation can be used, when an insured person presents their own EHIC in a verification challenge. The EHIC was issued to this person themselves.

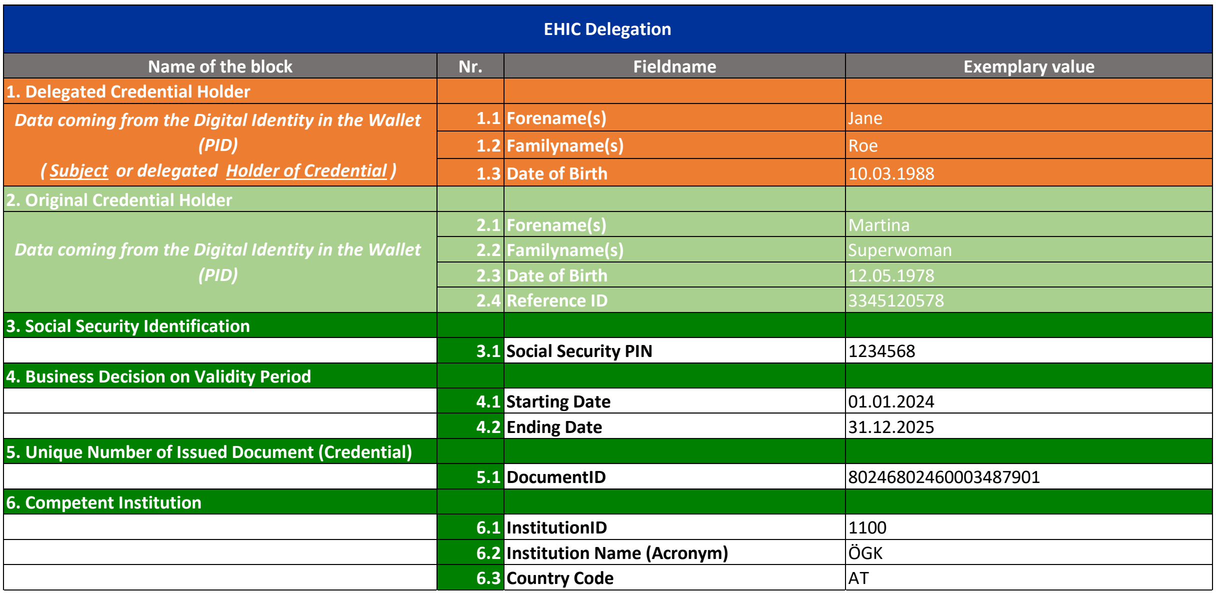


EHIC Standard			
Name of the block	Nr.	Fieldname	Exemplary value
1. Credential Holder			
Data coming from the Digital Identity in the Wallet (PID) *(Subject or delegated Holder of Credential)*	1.1	Forename(s)	Martina
	1.2	Familyname(s)	Superwoman
	1.3	Date of Birth	12.05.1978
2. Social Security Identification			
	2.1	Social Security PIN	1234568
3. Business Decision on Validity Period			
	3.1	Starting Date	01.01.2024
	3.2	Ending Date	31.12.2025
4. Unique Number of Issued Document (Credential)			
	4.1	DocumentID	80246802460003487901
5. Competent Institution			
	5.1	InstitutionID	1100
	5.2	Institution Name (Acronym)	ÖGK
	5.3	Country Code	AT

FIGURE 31: EHIC STANDARD

EHIC Delegation

This presentation can be used, when an EHIC of person A is delegated (out of the wallet from person A) to another person B. Person B can present the EHIC in a verification challenge on behalf of person A. The EHIC was issued to person A.



EHIC Delegation			
Name of the block	Nr.	Fieldname	Exemplary value
1. Delegated Credential Holder			
Data coming from the Digital Identity in the Wallet (PID) *(Subject or delegated Holder of Credential)*	1.1	Forename(s)	Jane
	1.2	Familyname(s)	Roe
	1.3	Date of Birth	10.03.1988
2. Original Credential Holder			
Data coming from the Digital Identity in the Wallet (PID)	2.1	Forename(s)	Martina
	2.2	Familyname(s)	Superwoman
	2.3	Date of Birth	12.05.1978
	2.4	Reference ID	3345120578
3. Social Security Identification			
	3.1	Social Security PIN	1234568
4. Business Decision on Validity Period			
	4.1	Starting Date	01.01.2024
	4.2	Ending Date	31.12.2025
5. Unique Number of Issued Document (Credential)			
	5.1	DocumentID	80246802460003487901
6. Competent Institution			
	6.1	InstitutionID	1100
	6.2	Institution Name (Acronym)	ÖGK
	6.3	Country Code	AT

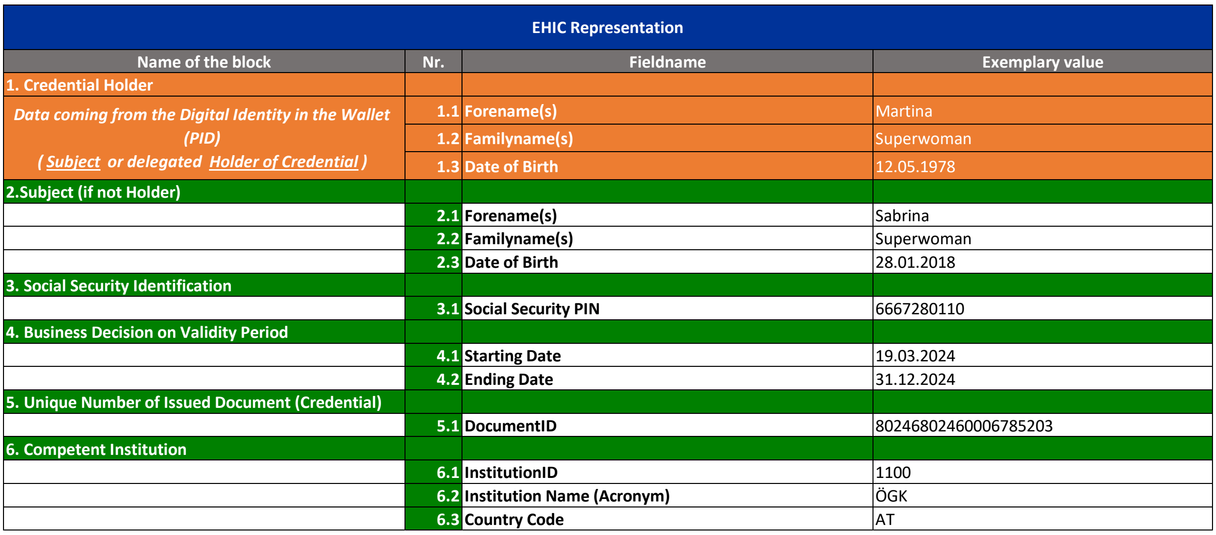
FIGURE 32: EHIC DELEGATION

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

EHIC Representation

This presentation can be used, when an EHIC for person A is issued to person B (due to a legal representation relationship). This relationship is modelled within the credential (the subject of the credential does not equal the holder of the credential). Person B can present the EHIC, which is stating claims about person A in a verification challenge.

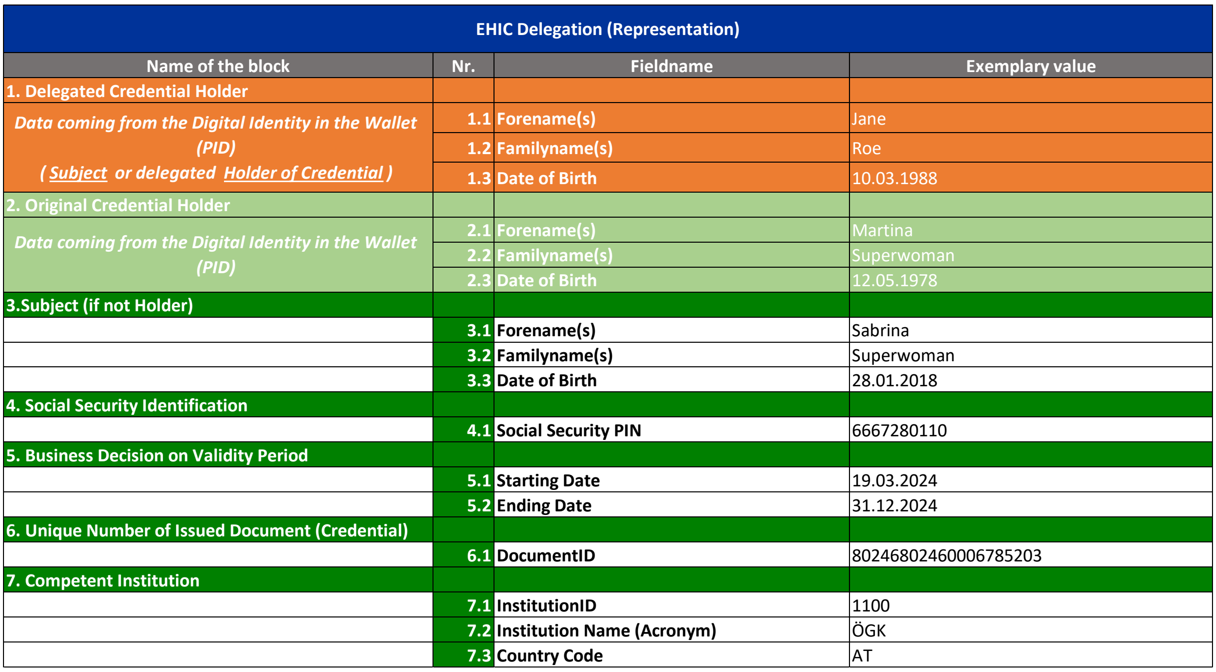


EHIC Representation			
Name of the block	**Nr.**	**Fieldname**	**Exemplary value**
1. Credential Holder			
Data coming from the Digital Identity in the Wallet (PID) ***(Subject or delegated Holder of Credential)***	1.1	**Forename(s)**	Martina
	1.2	**Familyname(s)**	Superwoman
	1.3	**Date of Birth**	12.05.1978
2.Subject (if not Holder)			
	2.1	**Forename(s)**	Sabrina
	2.2	**Familyname(s)**	Superwoman
	2.3	**Date of Birth**	28.01.2018
3. Social Security Identification			
	3.1	**Social Security PIN**	6667280110
4. Business Decision on Validity Period			
	4.1	**Starting Date**	19.03.2024
	4.2	**Ending Date**	31.12.2024
5. Unique Number of Issued Document (Credential)			
	5.1	**DocumentID**	80246802460006785203
6. Competent Institution			
	6.1	**InstitutionID**	1100
	6.2	**Institution Name (Acronym)**	ÖGK
	6.3	**Country Code**	AT

FIGURE 33: EHIC REPRESENTATION

EHIC Delegation (of Representation)

The EHIC for person A is issued to person B (due to a legal representation relationship). Person B can then delegate the credential (out of the wallet from person B) to another person C. Person C can present the EHIC in a verification challenge on behalf of person B.



EHIC Delegation (Representation)			
Name of the block	**Nr.**	**Fieldname**	**Exemplary value**
1. Delegated Credential Holder			
Data coming from the Digital Identity in the Wallet (PID) ***(Subject or delegated Holder of Credential)***	1.1	**Forename(s)**	Jane
	1.2	**Familyname(s)**	Roe
	1.3	**Date of Birth**	10.03.1988
2. Original Credential Holder			
Data coming from the Digital Identity in the Wallet (PID)	2.1	**Forename(s)**	Martina
	2.2	**Familyname(s)**	Superwoman
	2.3	**Date of Birth**	12.05.1978
3.Subject (if not Holder)			
	3.1	**Forename(s)**	Sabrina
	3.2	**Familyname(s)**	Superwoman
	3.3	**Date of Birth**	28.01.2018
4. Social Security Identification			
	4.1	**Social Security PIN**	6667280110
5. Business Decision on Validity Period			
	5.1	**Starting Date**	19.03.2024
	5.2	**Ending Date**	31.12.2024
6. Unique Number of Issued Document (Credential)			
	6.1	**DocumentID**	80246802460006785203
7. Competent Institution			
	7.1	**InstitutionID**	1100
	7.2	**Institution Name (Acronym)**	ÖGK
	7.3	**Country Code**	AT

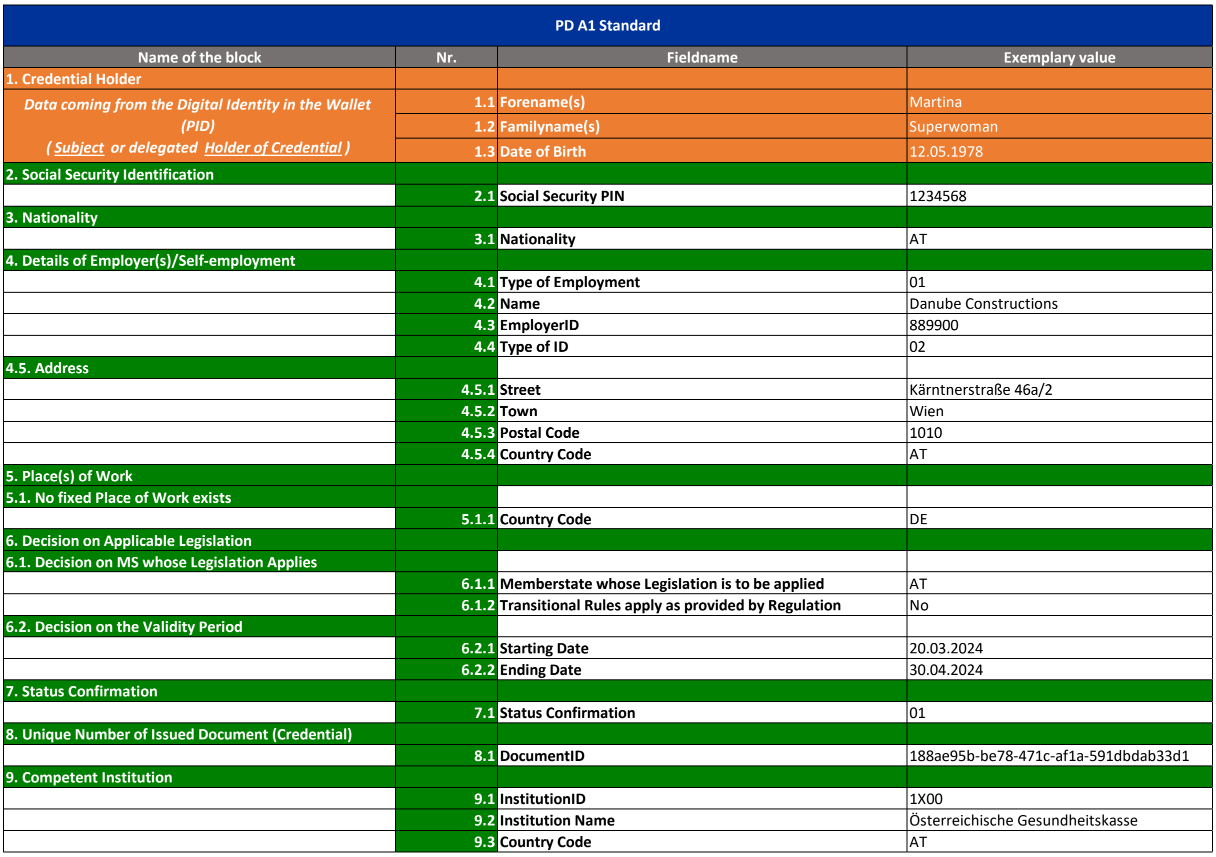
FIGURE 34: EHIC DELEGATION (REPRESENTATION)

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

PD A1 Standard

This presentation can be used, when an insured person presents their own PD A1 in a verification challenge. The PD A1 was issued to this person themselves.



PD A1 Standard			
Name of the block	Nr.	Fieldname	Exemplary value
1. Credential Holder			
Data coming from the Digital Identity in the Wallet (PID) *(Subject or delegated Holder of Credential)*	1.1	Forename(s)	Martina
	1.2	Familyname(s)	Superwoman
	1.3	Date of Birth	12.05.1978
2. Social Security Identification			
	2.1	Social Security PIN	1234568
3. Nationality			
	3.1	Nationality	AT
4. Details of Employer(s)/Self-employment			
	4.1	Type of Employment	01
	4.2	Name	Danube Constructions
	4.3	EmployerID	889900
	4.4	Type of ID	02
4.5. Address			
	4.5.1	Street	Kärntnerstraße 46a/2
	4.5.2	Town	Wien
	4.5.3	Postal Code	1010
	4.5.4	Country Code	AT
5. Place(s) of Work			
5.1. No fixed Place of Work exists			
	5.1.1	Country Code	DE
6. Decision on Applicable Legislation			
6.1. Decision on MS whose Legislation Applies			
	6.1.1	Memberstate whose Legislation is to be applied	AT
	6.1.2	Transitional Rules apply as provided by Regulation	No
6.2. Decision on the Validity Period			
	6.2.1	Starting Date	20.03.2024
	6.2.2	Ending Date	30.04.2024
7. Status Confirmation			
	7.1	Status Confirmation	01
8. Unique Number of Issued Document (Credential)			
	8.1	DocumentID	188ae95b-be78-471c-af1a-591dbdab33d1
9. Competent Institution			
	9.1	InstitutionID	1X00
	9.2	Institution Name	Österreichische Gesundheitskasse
	9.3	Country Code	AT

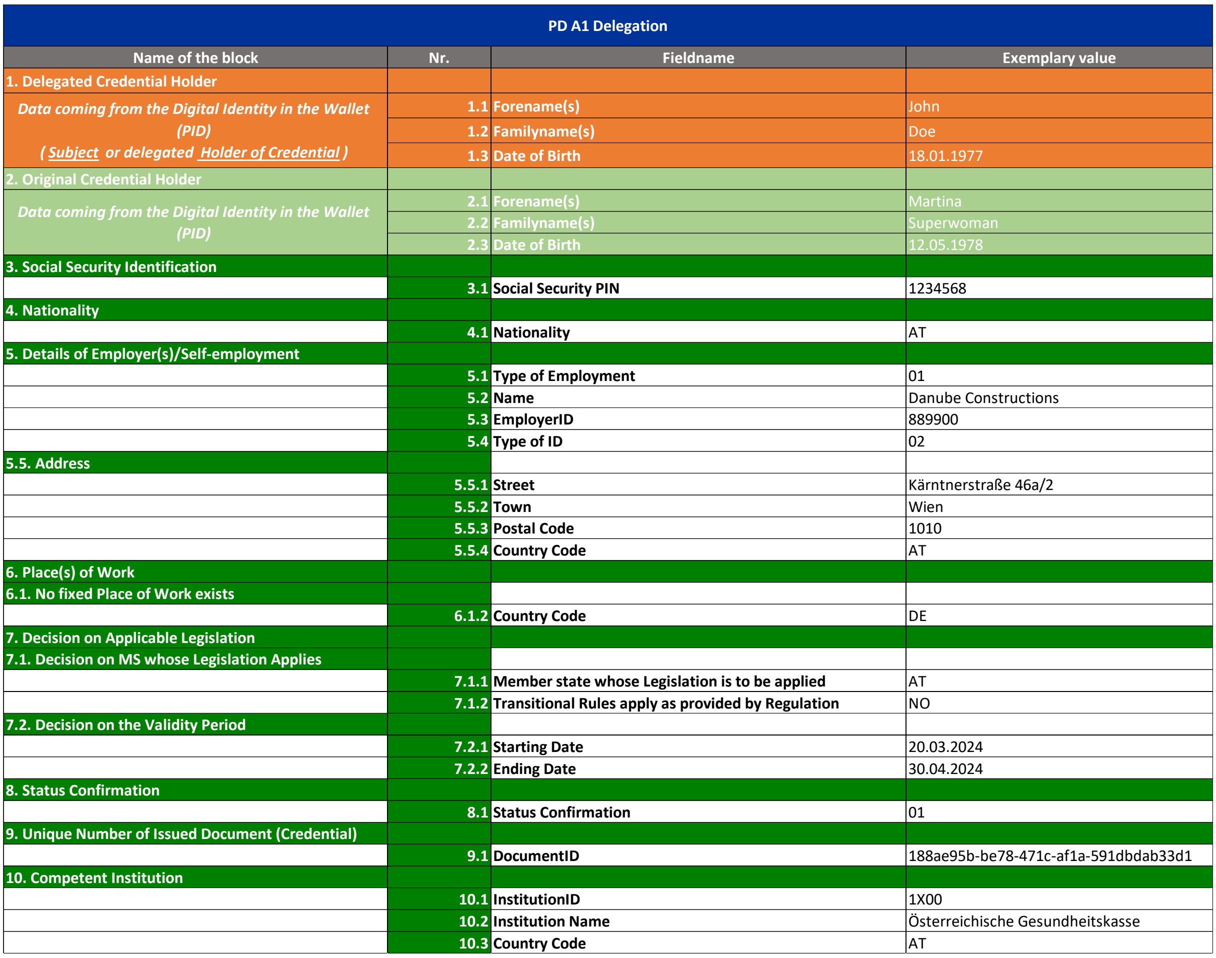
FIGURE 35: PD A1 STANDARD

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

PD A1 Delegation

This presentation can be used, when a PD A1 of person A is delegated (out of the wallet from person A) to another person B. Person B can present the PD A1 in a verification challenge on behalf of person A. The PD A1 was issued to person A.



PD A1 Delegation

Name of the block	Nr.	Fieldname	Exemplary value
1. Delegated Credential Holder			
Data coming from the Digital Identity in the Wallet (PID) *(Subject or delegated Holder of Credential)*	1.1	Forename(s)	John
	1.2	Familyname(s)	Doe
	1.3	Date of Birth	18.01.1977
2. Original Credential Holder			
Data coming from the Digital Identity in the Wallet (PID)	2.1	Forename(s)	Martina
	2.2	Familyname(s)	Superwoman
	2.3	Date of Birth	12.05.1978
3. Social Security Identification			
	3.1	Social Security PIN	1234568
4. Nationality			
	4.1	Nationality	AT
5. Details of Employer(s)/Self-employment			
	5.1	Type of Employment	01
	5.2	Name	Danube Constructions
	5.3	EmployerID	889900
	5.4	Type of ID	02
5.5. Address			
	5.5.1	Street	Kärntnerstraße 46a/2
	5.5.2	Town	Wien
	5.5.3	Postal Code	1010
	5.5.4	Country Code	AT
6. Place(s) of Work			
6.1. No fixed Place of Work exists			
	6.1.2	Country Code	DE
7. Decision on Applicable Legislation			
7.1. Decision on MS whose Legislation Applies			
	7.1.1	Member state whose Legislation is to be applied	AT
	7.1.2	Transitional Rules apply as provided by Regulation	NO
7.2. Decision on the Validity Period			
	7.2.1	Starting Date	20.03.2024
	7.2.2	Ending Date	30.04.2024
8. Status Confirmation			
	8.1	Status Confirmation	01
9. Unique Number of Issued Document (Credential)			
	9.1	DocumentID	188ae95b-be78-471c-af1a-591dbdab33d1
10. Competent Institution			
	10.1	InstitutionID	1X00
	10.2	Institution Name	Österreichische Gesundheitskasse
	10.3	Country Code	AT

FIGURE 36: PD A1 DELEGATION

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

13. APPENDIX B - REFERENCE ARCHITECTURE FOR THE INTEGRATION OF AN AUTHENTIC SOURCE

Work Package 7 in DC4EU will implement a reference issuer system where an authentic source is integrated via standard Application Programming Interfaces (API). Authentic Sources in social security coordination are competent institutions qualified to issue a certain Verifiable Credential (VC) type. There could be two possible options for implementation of the issuer system ((Q)EAA provider).

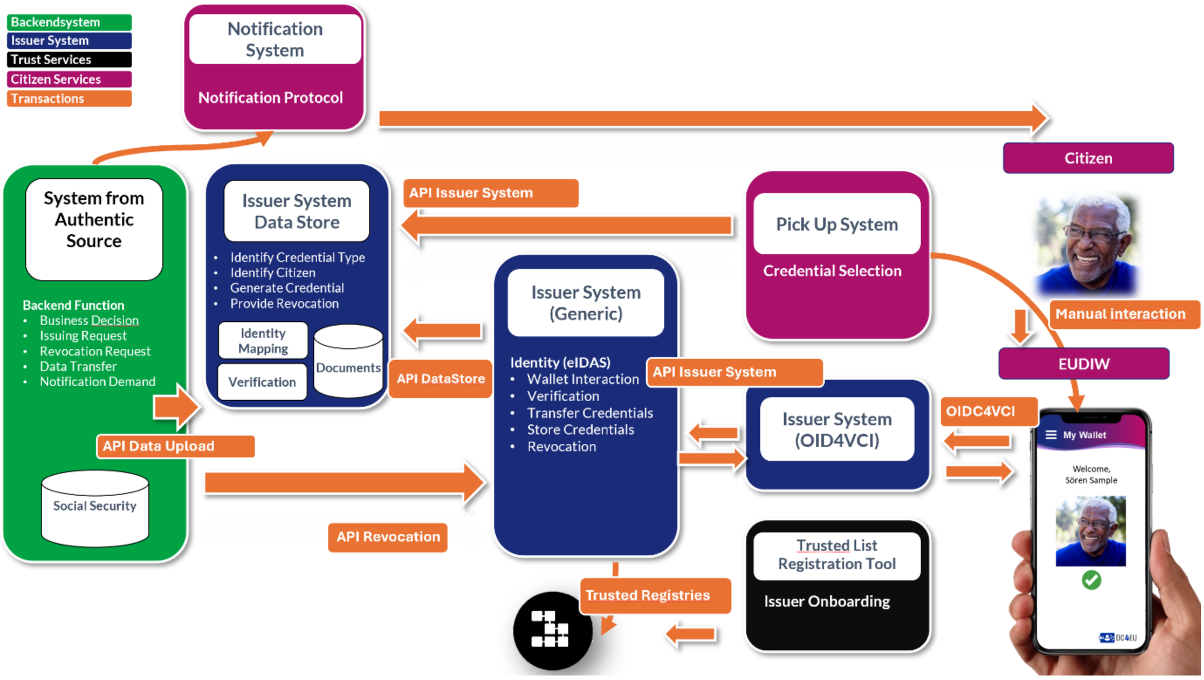


FIGURE 37: TECHNICAL INTEGRATION OF AUTHENTIC SOURCE BACKEND SYSTEM (REFERENCE IMPLEMENTATION). ISSUER OF VERIFIABLE CREDENTIALS ACTS ON BEHALF OF ONE OR MORE AUTHENTIC SOURCES.

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

OpenID for Verifiable Credentials (OID4VCs) is a product of the OpenID Connect Working Group. It is a standard interface used between the EUDI wallet and the Issuer System.

OID4VC consists of three specifications:

- **OpenID for Verifiable Credential Issuance (OID4VCI):** Defines an API and corresponding OAuth-based authorisation mechanisms for issuance of VCs.
- **OpenID for Verifiable Presentations (OID4VPs):** Defines a mechanism on top of OAuth 2.0 to allow presentation of claims in the form of VCs as part of the protocol flow.
- **Self-Issued OpenID Provider v2 (SIOPv2):** Enables End-Users to use OpenID Providers (OPs) that they control.
- OID4VC empowers End-Users to directly present identity information to Verifiers. It is being adopted in various projects and standards, such as the European Digital Identity Architecture and Reference Framework, the European Commission EBSI project, and draft ISO standards.

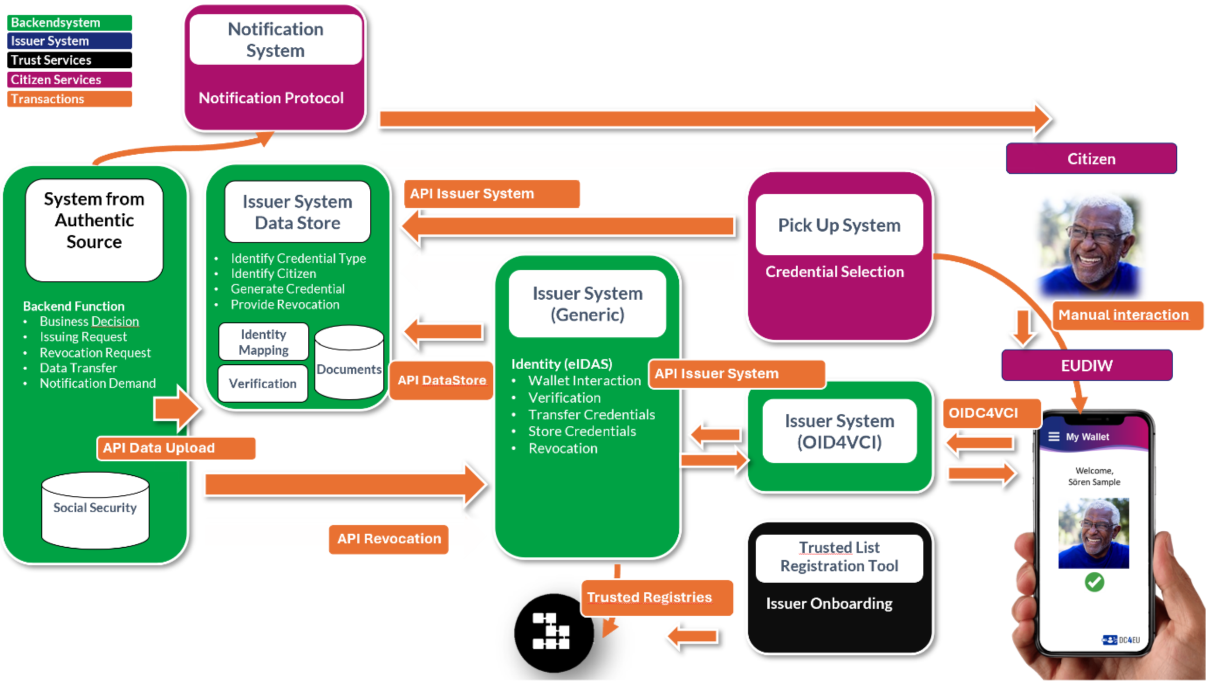


FIGURE 38: TECHNICAL INTEGRATION OF AUTHENTIC SOURCE BACKEND SYSTEM. THE AUTHENTIC SOURCE IS ALSO THE ISSUER OF VERIFIABLE CREDENTIALS

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