EBSI-VECTOR
Education and work reloaded

D5.1: Document describing the business blueprint, the high-level business processes, the use case interactions, and the onboarding for issuers

Project title:	**EBSI-VECTOR** - EBSI enabled Verifiable Credentials & Trusted Organisations Registries
Grant Agreement No.	101102512 - DIGITAL-2022-DEPLOY-02-EBSI-SERVICES
Deliverable Title	D5.1: Document describing the business blueprint, the high-level business processes, the use case interactions, and the onboarding for issuers
Version:	1.0
Date:	31st of January 2024
Responsible Partner:	INAIL
Authors:	Carlo Lentini (INAIL)
Contributing Partners:	INAIL, ENG, Walt.ID, DVSV, DRV-Bund, NASK, Smals
Reviewers:	Vincenzo Savarino (ENG) Maria Garcia Flores (FNMT) Fernando Mata (FNMT)
Dissemination Level:	PU – Public

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Document Change History

Version	Date	Author (organisation)	Description
v0.0	01/11/2023	Carlo Lentini (INAIL)	Final table of contents, distribution of responsibilities
v0.1	19/12/2023	Carlo Lentini (INAIL)	First draft
v0.2	12/01/2024	Carlo Lentini (INAIL)	Second draft
v0.3	23/01/2024	Carlo Lentini (INAIL)	Third draft
v0.4	29/01/2024	Vincenzo Savarino (ENG) Maria Garcia Flores (FNMT) Fernando Mata (FNMT)	Peer review
v1.0	31/01/2024	Carlo Lentini (INAIL)	Final version

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Table of Contents

1 EXECUTIVE SUMMARY 13

2 INTRODUCTION 14

2.1 CONTEXT, RELEVANCE AND PURPOSE: EBSI-VECTOR WP5 14

EBSI-VECTOR 14

EBSI-VECTOR and its role in Social Security 15

WP5 16

2.1.1 Core EU Principles on Social Security Coordination 17

2.1.2 Scope of Deliverable 5.1. 17

2.1.3 Methodology 18

2.1.4 Structure 19

3 ANALYSIS OF THE CURRENT STATUS OF EHIC 20

3.1 THE EHIC – GENERAL OVERVIEW 20

3.1.1 Challenges with the EHIC 21

3.1.2 Current Legal Framework 22

3.1.3 Characteristics of the EHIC 23

3.1.4 The Provisional Replacement Certificate (PRC) 23

3.2 ISSUANCE 24

3.2.1 Requesting of the EHIC & PRC – As/Is Procedure 25

3.2.2 Summary of Current Process Workflows 29

3.2.3 Central Repository for the Issuers of the EHIC – As/Is Analysis 31

3.3 VERIFICATION 31

3.3.1 The Verification Process of the EHIC/PRC – As/Is Analysis 31

3.3.2 Central Repository for the Verifiers of the EHIC – As/Is Analysis 33

3.3.3 Documentation Process for the EHIC – AS/IS Analysis 33

3.4 THE ONBOARDING PROCESSES FOR ISSUER AND AUTHORIZED VERIFIERS FOR THE EHIC – AS/IS ANALYSIS 34

3.4.1 The Onboarding of Issuers for EHIC - As/Is Analysis 34

3.4.2 The Onboarding of Authorized Verifiers for EHIC - As/Is Analysis 35

3.5 CONCLUSION 35

4 ANALYSIS OF THE CURRENT STATUS OF PD A1 37

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

4.1 THE PD A1 - GENERAL 37
4.1.1 PD A1 Current Legal Framework 38
4.1.2 Characteristics of the PD A1 39
4.1.3 Central Repository for the PD A1 – As/Is Analysis 39
4.2 ISSUANCE 40
4.2.1 The Issuance of the PD A1 – As/Is Analysis 40
4.3 VERIFICATION 41
4.3.1 The Verification Process of PD A1 – As/Is Analysis 41
4.3.2 Documentation Process for the PD A1 – AS/IS Analysis 42
4.3.3 Central Repository for the Verifiers of the PD A1– As/Is Analysis 43
4.4 THE ONBOARDING OF ISSUERS AND VERIFIERS FOR PD A1 – AS/IS ANALYSIS 43
4.4.1 The Onboarding of Issuers for PD A1 - As/Is Analysis 43
4.4.2 The Onboarding of Authorized Verifiers for PD A1 - As/Is Analysis 44
4.5 CONCLUSION 45

5 SYSTEM ARCHITECTURE 46

5.1 THE ACTORS 46
5.2 THE ARCHITECTURE 47
5.3 SOCIAL SECURITY ISSUER DIAGRAMS 49
5.4 VERIFIER ARCHITECTURE 51
5.5 CONCLUSION 52

6 DEFINITION OF THE BUSINESS PROCESSES OF EHIC AND PD A1 CREDENTIALS 53

6.1 PREREQUISITES FOR EXECUTING USER JOURNEYS 53
6.2 CORE USE CASE INTERACTIONS 54
6.2.1 Issuing of Credentials 54
6.2.2 Revocation of Credentials 55
6.2.3 Verification of Credentials 55
6.3 NON-CORE USE CASE INTERACTIONS 56
6.3.1 Delegation of a Credential 56
6.3.2 Self-verification of Credentials 56
6.3.3 Proof of Verification 57
6.4 USE CASE 1: ISSUANCE OF A PERSONAL VERIFIABLE CREDENTIAL IN SOCIAL SECURITY 57
6.4.1 The Process 58

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

6.5 USE CASE 2: REVOCATION OF A CREDENTIAL 61
6.5.1 The Process 63
6.6 USE CASE 3: VERIFICATION 65
6.6.1 The Process – Verification 65
6.6.2 User Journey 67
6.6.3 Verification by Unregistered Verifiers (Sharing of Credentials) 68

7 DATA MODEL FOR EHIC AND PD A1 CREDENTIALS 70

7.1 DATA MODEL FOR EHIC CREDENTIALS 70
7.2 DATA MODEL FOR PD A1 CREDENTIALS 71

8 DEFINITION OF ONBOARDING BUSINESS PROCESS FOR INSTITUTIONS IN THE EHIC AND PD A1 USE CASES 73

8.1 DEFINING A TRUST FRAMEWORK 73
8.1.1 EESSI Institution Repository – a Trust Framework for Social Security 73
8.1.2 EIDAS 2.0 Trust Framework 75
8.1.3 EBSI Trust Framework 77
8.2 IMPLEMENTATION OF THE TRUST FRAMEWORK: ISSUER REGISTRY AND ONBOARDING SERVICE 85
8.3 CHALLENGES 85
8.4 CONCLUSION 86

9 CONCLUSIONS 87

10 ANNEX - DEFINITION OF BACK-OFFICE INTERFACES FOR EHIC AND PD A1 ISSUERS & VERIFIERS (INCLUDING ANALYSIS OF REUSABLE BACK-OFFICES) 88

10.1 INTRODUCTION 88
10.2 ALIGNMENT WITH THE DC4EU FRAMEWORK 88
10.3 CACHE API 89
10.3.1 Data Upload 89
10.3.2 Get portal data 90
10.3.3 Get Document by Collection Code 90
10.3.4 Additional endpoints 91
10.4 ENTERPRISE WALLET APIS 92
10.4.1 Revocation 92
10.5 LIST OF REST APIS 93

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

10.6 CONCLUSION 100

11 REFERENCES 101

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

List of Figures

FIGURE 1 - AUTOMATIC ISSUANCE FLOW OF THE EHIC (SOURCE: DC4EU) 26
FIGURE 2 - ISSUANCE UPON REQUEST FLOW OF THE EHIC (SOURCE: DC4EU) 27
FIGURE 3 -ISSUANCE FLOW OF THE PRC (SOURCE: DC4EU) 28
FIGURE 4 - VERIFICATION FLOW OF THE EHIC/PRC (SOURCE: DC4EU) 32
FIGURE 5 - ISSUANCE FLOW OF PD A1 (SOURCE: DC4EU) 41
FIGURE 6 - VERIFICATION FLOW OF THE PD A1 (SOURCE: DC4EU) 42
FIGURE 7 - CURRENT EBSI ECOSYSTEM [11] 48
FIGURE 8 - ISSUER FLOW DIAGRAM USING CACHE COMPONENT 49
FIGURE 9 - VERIFIER ARCHITECTURE WITH INTERFACE TO VERIFIER ORGANISATION 51
FIGURE 10 - ISSUANCE WORKFLOW 58
FIGURE 11 - VERIFICATION FLOW 66
FIGURE 12 - UNQUALIFIED VERIFICATION FLOW 69
FIGURE 13 - THE EESSI INSTITUTION REPOSITORY [12] 74
FIGURE 14 - THE EESSI INSTITUTION REPOSITORY – PUBLIC ACCESS INTERFACE FOR SVS – ISSUER OF PORTABLE DOCUMENTS. [12] 75
FIGURE 15 - EBSI TRUST FRAMEWORK [14] 77
FIGURE 16 - LEGAL ENTITY ONBOARDING 79
FIGURE 17 - HIGHER LEVEL LEGAL ENTITY ACCREDITATION 81
FIGURE 18 - SUB-LEVEL LEGAL ENTITY ACCREDITATION 82
FIGURE 19 - ISSUER ACCREDITATION PROCESS 84

List of Tables

TABLE 1 – CURRENT EHIC PROCESS WORKFLOWS 29

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

List of Terms and Abbreviations

Term or Abbreviation	Definition
(Q)TSP	**(Qualified) Trusted Service Provider**: a natural or a legal person who provides one or more trust services as a qualified trust service provider, and adheres to the strict requirements that ensure the validity and security of the certificates, keys and signatures
(Qualified) Electronic Attestation of Attributes ((Q)EAA)	A proof in electronic form that allows the authentication of attributes. In its "qualified" form, issued by a (qualified) trust service provider ((Q)TSP)
Attestation Provider	Any provider that is able to issue an attestation, including PID Provider EAA and QEAA provider
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 the primary source of that information or recognized as authentic under national law
Basic Regulation	Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems
Cache system	A component of the Enterprise Wallet able to temporarily store all relevant business and functional data, while operational logs and data (non-privacy disclosing) can be stored (semi)permanently to comply with national legislations/requirements
Competent Institution	The Member State in which the institution with which the person concerned is insured or from which the person is entitled to benefits is situated. In eIDAS terms, the competent institution refers to the Authentic Source entitled to issue credentials

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Deeplink	A type of link that sends users directly to an app instead of a website or a store
DID	**Decentralized Identifier:** type of identifier that enables verifiable, decentralized digital identity. A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID
Download Service	Public or private services that allow the delivery of digital information
EBSI Trusted Issuers Registry	EBSI-based registry that uses distributed ledger technology that allows for the secure storage and management of accreditation status information
EBSI-Wallet	An end-user wallet conformant to EBSI infrastructure and specifications. In the context of the EBSI-VECTOR project, EBSI-conformant wallets will be defined inside WP3
EESSI	**Electronic Exchange of Social Security Information**: A decentralised IT system that helps social security institutions across the EU exchange information more rapidly and securely
EESSI IR	**Electronic Exchange of Social Security Information Institution Repository**: a repository for trusted actors which contains important information like official Institution IDs, validity statuses, and (in-)direct rules regarding authorisations to issue certain documents
EHIC	**European Health Insurance Card**: a free card that grants citizens access to necessary government-provided healthcare when temporarily staying in EU countries, Iceland, Liechtenstein, Norway, and Switzerland, under the same conditions and costs as local residents
EHIC PIN	The unique personal identification number (PIN) associated with the European Health Insurance Card (EHIC)

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

eIDAS Regulation	The European Regulation on electronic identification and trust services for electronic transactions in the internal market
Enterprise Wallet	Within the scope of the Social Security use cases of the EBSI-VECTOR project, an Enterprise Wallet is a software capable of managing the credentials lifecycle. It serves as an Issuer and Verifier System
EUDI Wallet	A product and service that allows the user to store identity data, credentials and attributes linked to its 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 of the eIDAS Regulation, and to create qualified electronic signatures and seals
IR-SPOC (EESSI)	**Institution Repository – Single Point of Contact**: the competent national body responsible for maintaining and updating the EESSI Institution Repository
Issuer (Trusted)	Any subject (legal person or not) capable of issuing credentials. In the context of social security, a trusted issuers of PD A1 or EHIC. Within the eIDAS 2.0 framework this could be an Authentic Source, see above
Legal entities	Private or public organizations entitled to issue, verify, hold and share digital certificates
Mapping Plugin	A software component that aids in the process of “mapping” one user identity to another system
NAB	**National Accreditation Bodies**: under Regulation (EC) No. 765/2008 are the bodies in Member States that perform accreditation with authority derived from the State
National Social Security Institution (SSI) Portal	The website of a national social security institution where a citizen can have access to various online services

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

PD A1	**Portable Document A1**: a document that confirms which social security legislation applies to a worker not affiliated with the country of work
PID	Personal Identifier
PIN	**Personal Identification Number**: used in Social Security Institutions to identify citizens
Private Keys	A cryptographic key that is used with an asymmetric (public key) cryptographic algorithm
Public Keys	A cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key)
Relying Party	In the context of trust framework, it is a natural or legal person that relies upon an electronic identification or a Trust Service for verification purposes
REST - API	**Representational State Transfer – Application Programming Interface**: application programming interface (API or web API) that conforms to the constraints of REST architectural style and allows for interaction with RESTful web services
Supervisory Bodies	Bodies entitled to supervise QTSPs and act, if necessary, in relation to non-qualified Trust Service Providers. Notified to the EU Commission by the Member States
Trust Framework	A common set of rules based on best practice standards that ensure compliance with the minimum requirements for security, privacy, identification management and interoperability of the Social Security environment
Verifiable Credential	A tamper-evident credential that has authorship that can be cryptographically verified. Verifiable Credentials can be used to build Verifiable Presentations, which can also be

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

	cryptographically verified. Must comply with (Q)EAA requirements
Verifiable Presentation	Tamper-evident presentation encoded in such a way that authorship of the data can be trusted after a process of cryptographic verification. Certain types of Verifiable Presentations might contain data that is synthesized from, but do not contain, the original Verifiable Credentials (for example, zero-knowledge proofs)
Verifier	A role an entity performs by receiving one or more Verifiable Credentials, optionally inside a Verifiable Presentation for processing. Other specifications might refer to this concept as a relying party
Verifier (unregistered)	A verifier (see above) that has not been onboarded on a Trusted Verifier Registry. It is possible for an unregistered verifier to receive Verifiable Credentials and Presentations, possibly with limitations imposed by the holder
VID	Verifiable Identity Data

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

1 Executive Summary

This deliverable establishes the foundational elements for the implementation of social security use cases in a cross-border scenario, through the leverage of the EBSI infrastructure capabilities and the use of Verifiable Credentials. Social security is a highly regulated sector, and therefore requires particular attention motivated by the careful management of sensitive personal data linked to the accessibility of primary public services and the founding pillars of the EU, such as the freedom of movement.

This business blueprint produced by WP5 has been structured starting from an analysis of the status quo of the selected social security use cases, namely the Portable Document A1 (PD A1), a document that confirms which social security legislation applies to a worker not affiliated with the country of work, useful to prove entitlement to public services in a State different from the one of residence, and the European Health Insurance Card (EHIC), a free card that grants citizens access to necessary government-provided healthcare when temporarily staying in a different Member State under the same conditions and costs as local residents. Legislative requirements, specifications, and peculiarities of the current interactions served as a baseline to build future digital interactions, with a clear focus on the need to streamline the process of issuance, revocation, and verification in order to avoid frauds and errors and enhance usability.

The analysis of the status quo of the use cases has then been contextualized in the proposal for a System Architecture able to fulfil the requirements of usability, interoperability and privacy as well as avoiding the need for difficult implementations for the already established social security institutions' systems. The main outcome is linked to the implementation of the Enterprise Wallet, which has been envisioned as a set of plug-in capabilities able to serve as Issuer and Verifier.

The architecture is instrumental to the realization of the selected business processes. In this regard, this business blueprint identified three core processes: issuance, revocation, and verification of a Verifiable Credential. Moreover, three secondary use cases have been selected, in order to propose further advancements to the digitalization of the sector. The processes entail the need for improvements to the EBSI infrastructure and capabilities, in order to build secure, transparent, and traceable interactions between the actors involved. Those actors are identified in the final chapter, within the analysis of the onboarding process. Here, the need for compliance with existing social security frameworks, such as the EESSI and the eIDAS Regulation, is stated as a necessary requirement to guarantee an interoperable and widely recognized solution in the coordination of social security in Europe.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

2 Introduction

Work Package 5 of the EBSI-VECTOR project has been entrusted with the task of developing this deliverable, which provides a comprehensive business blueprint of the Social Security use cases. It delves deeply into the sophisticated business processes at a high level, explores the dynamic interactions across a range of use cases, and offers a guideline for the onboarding of issuers, specifically designed for the social security context.

The primary objective of this document is to lay down a robust and clear framework, offering practical and actionable guidelines for the effective implementation and seamless integration of the EBSI-VECTOR within the social security domain. It establishes a solid foundation for Deliverable 5.2, which is dedicated to the practical realization of these use case interactions and the strategic onboarding of issuers. This foundational document not only steers the direction for the execution of Deliverable 5.2 but also acts as an indispensable tool in providing feedback and validation for the implementation activities of the piloting phase.

By establishing these expectations, the document ensures that all implementation efforts are perfectly aligned with the overarching goals of EBSI-VECTOR. This alignment is crucial for enhancing the operational efficiency of social security coordination by contributing to the broader objective of advancing digital transformation in Europe.

As the culmination of dedicated efforts and extensive activities carried out in Task 5.1, this document stands as a marker of progress and a reservoir of insights gained in this field, symbolizing a major stride forward toward the digitalization of Verifiable Credentials in Europe.

2.1 Context, Relevance and Purpose: EBSI-VECTOR WP5

EBSI-VECTOR

EBSI-VECTOR has a multifaceted objective encompassing the enhancement of capabilities in social security, educational credentials, and eSSIF use cases. The project seeks to expand the scope of self-sovereignty principles, decentralized Verifiable Credentials, and decentralized trusted registries within each of these use cases, all with the aim of delivering tangible benefits to European citizens.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

To achieve this, EBSI-VECTOR leverages the European Blockchain Service Infrastructure (EBSI) as a foundational trusted framework with DLT or Private Blockchain technologies, such as BESU. It is committed to implementing these improvements across various countries and facilitating seamless cross-border interactions to ensure that the benefits of these advancements are accessible to a broad spectrum of end-users throughout Europe.

EBSI-VECTOR and its role in Social Security

Within the context of social security, EBSI-VECTOR's objective is to establish an EBSI-compliant infrastructure for issuing and verifying entitlement documents related to social security benefits. This infrastructure will rely on "Electronic Identification, Authentication, and Trust Services" (eIDAS) and the "European Blockchain Services Infrastructure" (EBSI) as its foundation for cross-border operations.

Two specific business cases have been identified: PD A1 and EHIC:

1) PD A1 - The provision of a statement of applicable legislation is useful for individuals who work in multiple EU countries or are posted workers, as it helps demonstrate their payment of social contributions in another EU nation.
2) EHIC - The European Health Insurance Card, a free card that grants citizens access to necessary government-provided healthcare when temporarily staying in EU countries, Iceland, Liechtenstein, Norway, and Switzerland, under the same conditions and costs as local residents.

These use cases encompass various cross-border social security activities. Coupled with the EESSI capabilities, which connect competent institutions involved in cross-border activities, the implementation of EBSI and eIDAS technologies aims to streamline processes and reduce instances of fraud and errors.

The project also recognizes the need to address the identity of legal entities or organizations within the decentralized ecosystem, a component that was initially overlooked in the ESSIF specification and capabilities. To fill this gap, the EBSI-VECTOR initiative will collaborate with business registries and related projects. The goal is to explore, define, develop, pilot, and implement this new capability, which will facilitate consistent and controlled interactions between organizations across various business domains and processes. This enhancement is expected to benefit a range of use cases beyond education and social security.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

WP5

As Europe strides towards an era of digital transformation, Work Package 5 (WP5) of the EBSI-VECTOR project emerges as an important component in the field of social security coordination. This initiative is strategically aligned with the broader objectives outlined in the European Commission's digitalization efforts, particularly in enhancing the efficiency and interoperability of cross-border social security systems.

WP5's primary focus will be on the deployment of social security use cases and conducting a Proof of Concept (PoC) with key stakeholders (Deliverable 5.2). This PoC is designed to demonstrate and validate the functionality of Verifiable Credentials within an EBSI-compliant infrastructure, a foundational element introduced by the European Blockchain Service Infrastructure (EBSI) project.

EBSI-VECTOR WP5 is set to tackle a spectrum of challenges, including addressing security and trust concerns, ensuring interoperability, and maintaining compliance with evolving regulations. By incorporating digital and decentralized concepts, WP5 aims to modernize the way legal documents are provided and verified, thus enhancing the overall efficacy and reliability of social security processes. Collaboration is a cornerstone of this endeavour, with WP5 working closely with WP3 to construct and refine interactions related to specific business cases such as the PD A1 and the European Healthcare Insurance Card (EHIC).

In this concerted effort, WP5 will not only identify and implement necessary interactions for the PD A1 and EHIC use cases but will also streamline the onboarding procedures for issuers. This comprehensive approach ensures a robust feedback mechanism and validation process across various implementation activities. By sharing its outcomes and insights, WP5 contributes significantly to the overarching goals of the EBSI-VECTOR project, ultimately aiming to deliver a final report that encapsulates the successes and learnings of this ambitious journey towards a more integrated and digitally advanced European social security landscape.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

2.1.1 Core EU Principles on Social Security Coordination

The fundamental principle underlying the Community rules on social security coordination is the so-called principle of uniqueness of the applicable legislation: persons are subject to the legislation of only one Member State. If the person carries out a work activity, they are subject to the legislation of the State where the activity is carried out (*lex loci laboris*).

In some specific situations, however, different criteria are applied. Such situations are related specifically to:

- Employees working for an employer who normally carries out its activities in one Member State and who are posted by that employer to another Member State to carry out work on its behalf (Article 12(1) of the Basic Regulation) – "POSTING OF AN EMPLOYED PERSON";
- Persons normally pursuing an activity as a self-employed worker in one Member State pursuing a similar activity in another Member State (Article 12(2) of the basic Regulation) – "SELF-EMPLOYED POSTING";
- Persons pursuing an activity as an employed/self-employed person in two or more Member States (Article 13 of the Basic Regulation). [1]

2.1.2 Scope of Deliverable 5.1.

The scope of Deliverable 5.1 is focused on creating a detailed business blueprint, which thoroughly addresses high-level business processes, the dynamics of different use case interactions, and the methodologies for onboarding issuers. This Deliverable is crucial for laying down a solid foundation necessary for effectively implementing these use case interactions and integrating issuer onboarding procedures. Its aim is to provide a clear and well-organized blueprint, guiding the execution and integration of these processes through a Proof of Concept (PoC) outlined in Deliverable 5.2.

In achieving this, Deliverable 5.1 plays a vital role in supporting the EBSI-VECTOR project's objectives and contributes to the European Commission's initiatives in digitizing social security coordination, ensuring a more streamlined and effective approach.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

2.1.3 Methodology

In order to meet EBSI-VECTOR's goals, WP5 will begin by identifying and articulating the existing business requirements for issuing PD A1 and EHIC, translating them into high-level business processes, and adapting them to EBSI-VECTOR goals and technical capabilities before identifying use case interactions for PD A1 and EHIC. In addition, it will establish the onboarding process for issuers in multiple releases to ensure continuous delivery and minimize the time required to initiate the test piloting phase (Task 5.1).

Subsequently, these interactions will be implemented within an EBSI-compliant infrastructure for the specified use cases. This includes executing issuer onboarding, testing its functionality in the project's second phase, and building and integrating functions to manage back-office information. Throughout these tasks, feedback will be provided on the EBSI reference architecture, related projects, and policy actions (Task 5.2).

Lastly, WP5 will conduct a pilot phase to gather feedback on implementing the use cases within the EBSI infrastructure and subsequently contribute to the EBSI-VECTOR project's final report (Task 5.3).

The methodology utilized in the preparation of Deliverable 5.1 is grounded in the development of a conceptual model that draws extensively from the initiatives and frameworks established by the European Commission, including key projects like the digitalization of the EHIC [2] and ESSPass [3] as well as other related efforts. Additionally, this methodology incorporates insights and foundational elements from consortia such as DC4EU [4]. This integration is particularly pertinent given the commonalities in the foundational principles and objectives shared between DC4EU and EBSI-VECTOR, both of which are dedicated to fostering a unified solution for social security coordination across Europe. This approach ensures that Deliverable 5.1 is not only informed by leading-edge practices but also harmonizes with broader strategic visions for social security in the European context.

A critical aspect of this methodology was the thorough definition of business requirements for the digitalization of social security credentials. This process involved a comprehensive delineation of current and imagined future business processes, onboarding procedures, data models, and back-office interfaces which together comprise the "business layer" of the project. This layer forms the backbone of the WP5's goals, ensuring a structured and coherent approach to their execution.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Moreover, the content of Deliverable 5.1 is the culmination of extensive collaborations and discussions with partners involved in WP5. These partners, who are experts in the fields of social security and the digitalization of credentials, provided invaluable insights and perspectives. Their contributions were instrumental in refining the deliverable, ensuring that it not only builds upon established works but also resonates with current trends and requirements in the fields of social security and digital credentials. This collaborative approach has been pivotal in shaping a deliverable that is both comprehensive and attuned to the nuances of social security coordination in a digitally evolving Europe.

2.1.4 Structure

Deliverable 5.1 is organized into ten chapters, encompassing an Executive Summary and an Annex dedicated to back-office interfaces. The document begins with an introduction that sets the stage for its relevance and scope. It then progresses into chapters 3 and 4, which are focused on describing the European Health Insurance Card (EHIC) and the Portable Document A1 (PD A1), respectively. Chapter 5 addresses the development of a potential system architecture, aiming to align with existing infrastructures of public organizations. Chapter 6 offers an in-depth analysis of the business processes associated with EHIC and PD A1 credentials, distinguishing between core and secondary use cases. The following chapter, Chapter 7, presents a detailed view of the data models for both EHIC and PD A1 credentials, highlighting their stages of development and crucial data components. Finally, Chapter 8 explores the onboarding business processes for institutions related to EHIC and PD A1 which aims to lay out a comprehensive framework for the onboarding procedure, emphasizing the creation of a solid trust framework critical for the effective application of Verifiable Credentials (VCs).

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

3 Analysis of the Current Status of EHIC

This chapter offers a detailed exploration of the European Health Insurance Card (EHIC), leveraging extensive data sourced from the DC4EU Consortium's comprehensive questionnaires, and insights from the Technical Commission's ad-hoc Working Group dedicated to the digitalization of the EHIC. Our aim is to present an all-encompassing analysis of the EHIC, focusing on its core attributes, the challenges it faces, and the operational mechanisms underpinning its function.

Central to our inquiry is the legal framework governing the EHIC, its physical characteristics, and the consequent effects these have within the larger scope of European healthcare systems. We delve into the card's distribution patterns, its utilization trends, and the diverse methodologies employed by different Member States in its issuance and validation. Furthermore, we examine its operational dynamics within the collaborative healthcare network of the EU, highlighting the nuances and implications of cross-border medical care facilitation.

Through this review, we strive to shed light on the multifaceted nature of the EHIC, considering its current status and potential evolutionary paths in the context of an increasingly digital landscape.

3.1 The EHIC – General Overview

The EHIC (European Health Insurance Card) is a free card that grants citizens access to necessary government-provided healthcare when temporarily staying in EU countries, Iceland, Liechtenstein, Norway, and Switzerland, under the same conditions and costs as local residents.

WP5 will identify use case interactions for EHIC and establish the onboarding process for issuers in multiple releases to ensure continuous delivery and minimize the time required to initiate the test piloting phase.

As of now, approximately 240 million European Health Insurance Cards (EHIC) are in circulation, representing about half of the total population of the European Union (Source: DC4EU). However, the prevalence of EHIC ownership varies significantly among EU Member States, largely due to the absence of unified standards governing the application, issuance, and validity periods of the cards, resulting in some Member States automatically issuing the card to the entirety of

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

the population, whereas others only issue upon request to a limited portion of it. Additionally, the EHIC may exist as a standalone card or be integrated with a national health insurance card.

A key feature of the EHIC is its role in the 'reimbursement' process as defined by EU coordination rules. Essentially, healthcare costs incurred in a Member State where an individual is visiting are reimbursed by the individual's home Member State (the competent Member State), based on the rates applicable in the visited Member State. This reimbursement typically occurs directly between the Member States involved, which is the case in about 90% of instances. Alternatively, reimbursement may be processed between the competent Member State and the insured individual.

3.1.1 Challenges with the EHIC

The EHIC is an undoubtedly widespread method of ensuring access to unplanned necessary healthcare. However, current regulations can pose challenges in certain Member States when it comes to application, issuance, validity, and reimbursement settlement processes.

- First of all, when the EHIC is refused by healthcare providers, it is mostly due to a lack of understanding regarding its workings and how it operates.
- Secondly, there is no clear and universally accepted interpretation of the terms "unplanned" and "necessary" healthcare.
- Lastly, approximately 2% of the reimbursements are rejected by the competent institutions, primarily due to an invalid EHIC or treatment dates preceding EHIC issuance**,** with (creditor institution) possibly severe repercussions on budgetary matters of the Member State of stay.

Downsides are not limited to those mentioned above. Among others, issuing a physical card with different validity period between Member States (sometimes even one year-long), has considerable impact in terms of cost and environment.

The digitalization of the European Health Insurance Card (EHIC) could therefore resolve several challenges linked to the physical format of the card, such as the irrevocability of the card once issued, and the lack of a specified activation date.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

3.1.2 Current Legal Framework

The relevant regulations regarding the procedures, scope, and entitlement to the EHIC are set by Article 19 of Regulation (EC) No. 883/2004 (also, Basic Regulation) and by Article 25 of Regulation (EC) No. 987/2009, which follow:

1) Article 19 of Regulation (EC) No 883/2004 [1]:

An insured person and the members of their family staying in a Member State other than the competent Member State shall be entitled to the benefits in kind which become necessary on medical grounds during their stay, considering the nature of the benefits and the expected length of the stay.

These benefits shall be provided on behalf of the competent institution by the institution of the place of stay, in accordance with the provisions of the legislation it applies, as though the persons concerned were insured under the said legislation.

2) Article 25 of Regulation (EC) No 987/2009 [5]:

For the purposes of the application of Article 19 of the basic Regulation, the insured person shall present to the health care provider in the Member State of stay a document issued by the competent institution indicating their entitlement to benefits in kind. If the insured person does not have such a document, the institution of the place of stay, upon request or if otherwise necessary, shall contact the competent institution in order to obtain one (Art. 25.1).

That document shall indicate that the insured person is entitled to benefits in kind under the conditions laid down in Article 19 of the Basic Regulation on the same terms as those applicable to persons insured under the legislation of the Member State of stay (Art. 25.2).

The benefits in kind referred to in Article 19(1) of the basic Regulation shall refer to the benefits in kind which are provided in the Member State of stay, in accordance with its legislation, and which become necessary on medical grounds with a view to preventing an insured person from being forced to return, before the end of the planned duration of stay, to the competent Member State to obtain the necessary treatment (Art. 25.3) [1] [5].

According to the current legal framework (Decision S1 and S2 of 12 June 2009, Decision S11 of 9 December 2020), the technical specifications require the EHIC to be a physical card providing a set of data required for the identification of the insured person [6] [7] [8]:

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- Surname and forename of the card holder;
- Personal identification number of the card holder;
- Date of birth of the card holder;
- Validity period of the card;
- ISO 3166-1 numeric code of the Member State issuing the card;
- Identification number and acronym of the competent institution issuing the card;
- Logical number of the card according to EN 1867 of 1997.

3.1.3 Characteristics of the EHIC

In terms of their characteristics, most countries issue the European Health Insurance Card (EHIC) as a plastic card. However, in some European countries it can also be provided in digital form as a PDF. Among these, eight countries issue standalone EHIC cards (Denmark, France, Ireland, Latvia, Poland, Portugal, Spain, Sweden). On the other hand, Austria, Czechia, Germany, Italy and Switzerland include the EHIC as part of their national health cards. Finland and the Netherlands offer a combination, providing both standalone EHIC cards and incorporating EHIC into their national health cards.

The duration of validity for an EHIC is contingent upon the regulations stipulated in national law, the policies of the issuing institution, and the particular category of individuals for whom it is issued (e.g., pensioners, children, etc.). Notably, discrepancies in the validity period may also exist when compared to the national health card. In most member states, alterations in the individual's category (e.g., transitioning to adulthood or entering retirement) do not impact the EHIC's expiration date.

3.1.4 The Provisional Replacement Certificate (PRC)

The PRC serves as a substitute for the EHIC when the EHIC is lost or not accessible. The requirements for obtaining the PRC are essentially identical to those for the EHIC, except in Austria, where an insurance period is not required. The main distinctions between the PRC and EHIC are as follows:

- The PRC is intended for temporary use, unlike the EHIC (except for Austria and Portugal);
- PRC requests are handled manually;
- The PRC is issued in a paper format or as PDF rather than as a plastic card.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

3.2 Issuance

In the issuance process, there are no distinctions among institutions; differences are solely at the country-specific level.

EHIC issuance methods are categorized into initial and subsequent issuance:

1) **Initial Issuance**:

- Automatic Issuance: triggered by birth or new citizen registration, with EHICs sent via mail after issuance.
- Issuance upon Request: insured individuals can apply through various channels, and in-person applications result in direct or mailed issuance.

2) **Re-Issuance**:

- Automatic re-Issuance: occurs in countries with EHIC as part of the national card, and some countries with EHIC as a standalone card. EHICs are sent via mail after re-issuance.
- Re-Issuance upon Application: available for reasons such as loss/theft, data changes, insurance changes, and expiration. Applications can be made through phone, email, platforms, or in-person, with in-person resulting in direct or mailed issuance.

Revocation or deactivation of EHICs is a process confined to national registries and databases. It is important to note that a centralized revocation is not possible, meaning that cards that have already been distributed cannot be declared as “invalid” on a centralized level. The authority for deactivation lies within individual national systems rather than being centrally coordinated.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

3.2.1 Requesting of the EHIC & PRC – As/Is Procedure

Currently, EHICs can be requested in two ways[1]:

1) **Automatic request** (i.e., at birth)

EHIC eligibility is contingent on social security institution verification, ensuring that only eligible citizens receive the credential. If eligible, citizens will receive an EHIC either as a standalone card or as part of a national card.

In cases of fraud, a replacement single EHIC will be issued and sent to the rightful holder.

[1] In certain cases, you may encounter both request scenarios since EHICs can be revoked and subsequently re-requested.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

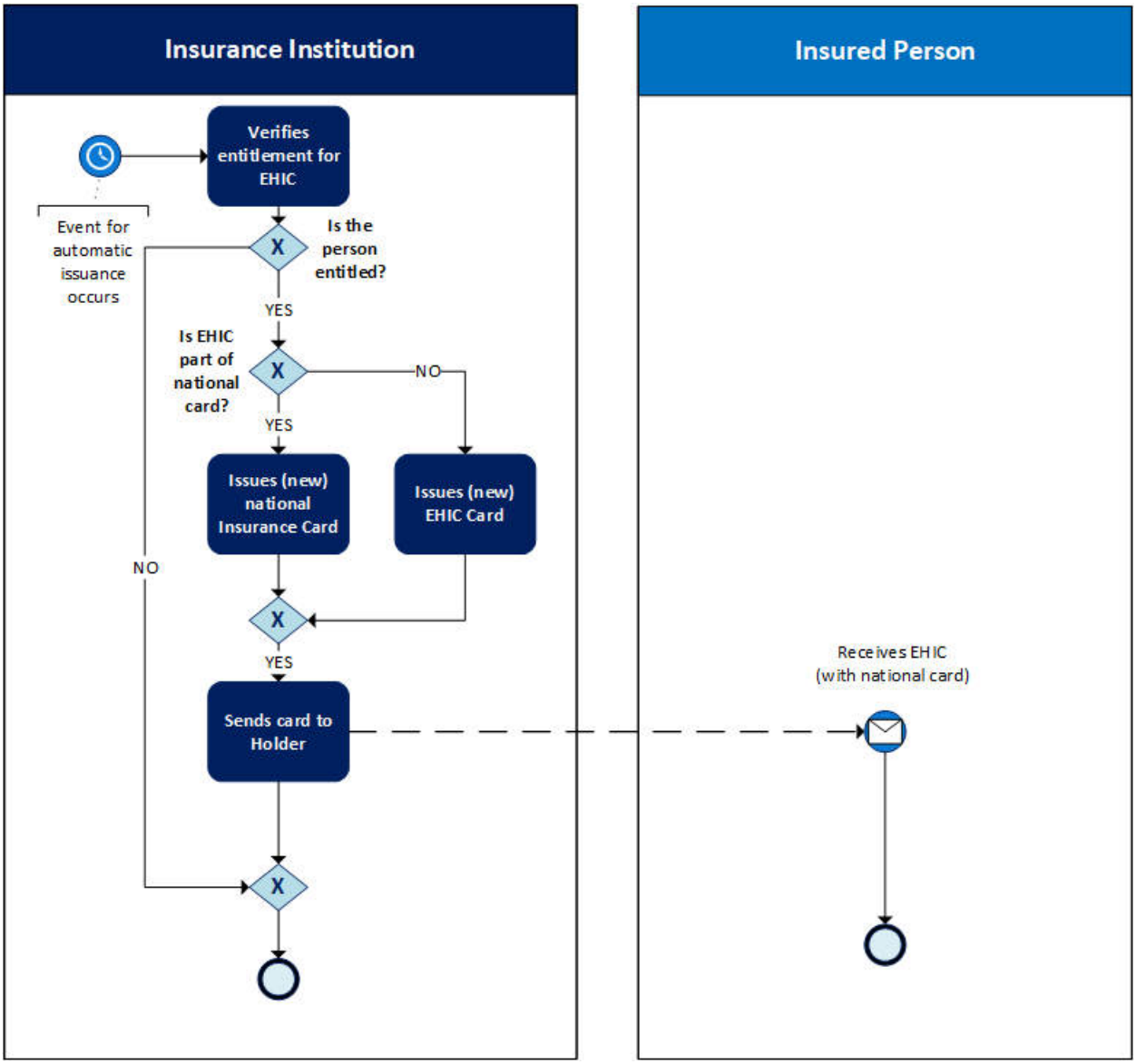


Figure 1 - Automatic issuance flow of the EHIC (Source: DC4EU)

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

2) **Upon request** (i.e., to obtain an EHIC, an individual must formally request it from the competent institution)

Requests can be made through various channels, including public authorities' platforms, email, phone, or in-person visits to the insurance office.
Once the insurance institution receives the request and verifies the entitlement, it will either deny the request or issue and deliver the EHIC to the eligible holder.

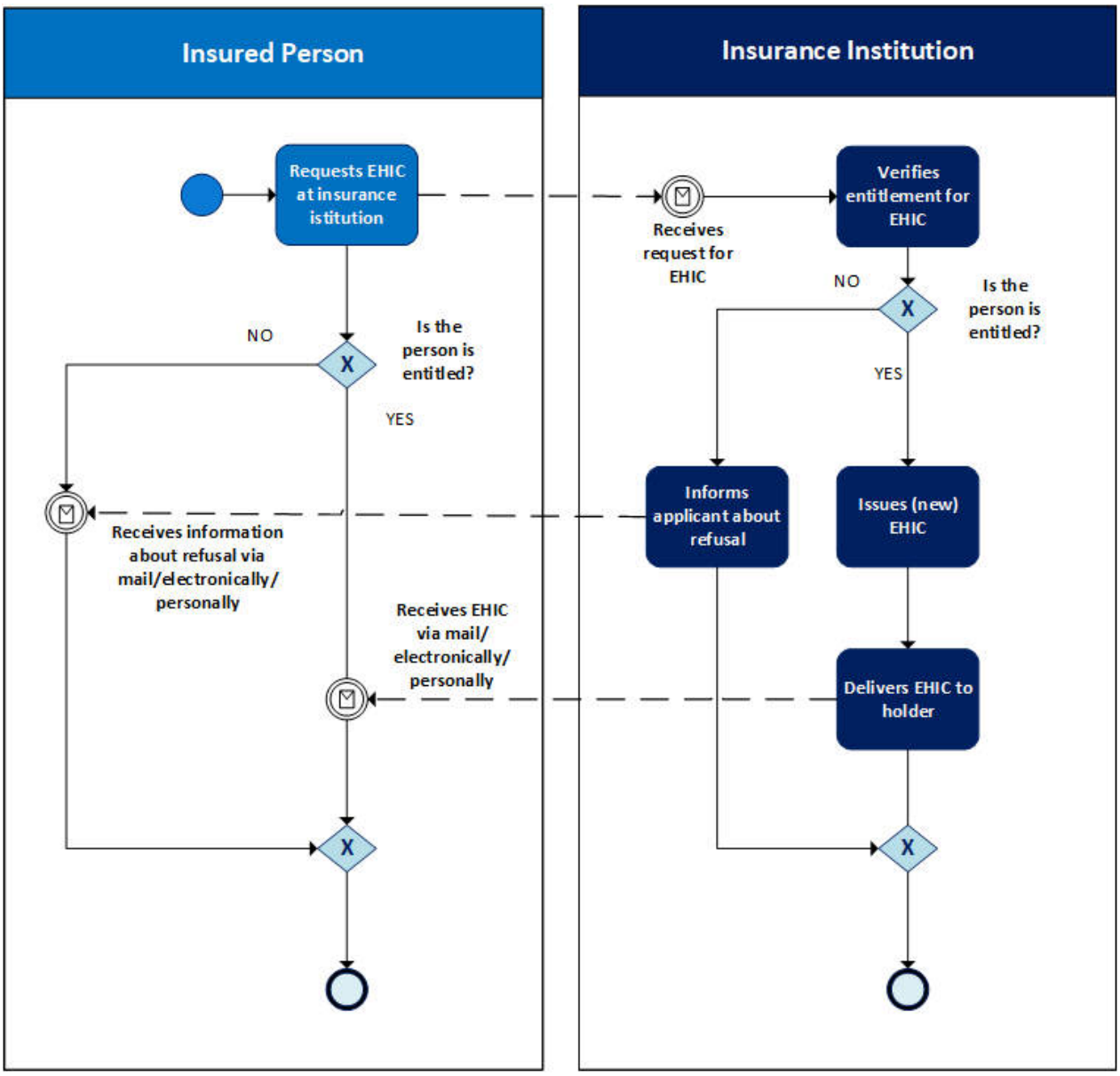


Figure 2 - Issuance upon request flow of the EHIC (Source: DC4EU)

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

PRCs are typically issued before stays abroad, although some Member States may not issue them in advance. These requests can be made through various channels, such as online, phone, email, or in-person, and the certificate is issued only for the duration of the stay, with the stay dates specified during the application. PRCs are always provided in paper format, although they may be sent digitally in PDF form when urgency is a factor, for instance, when waiting for an EHIC to arrive.

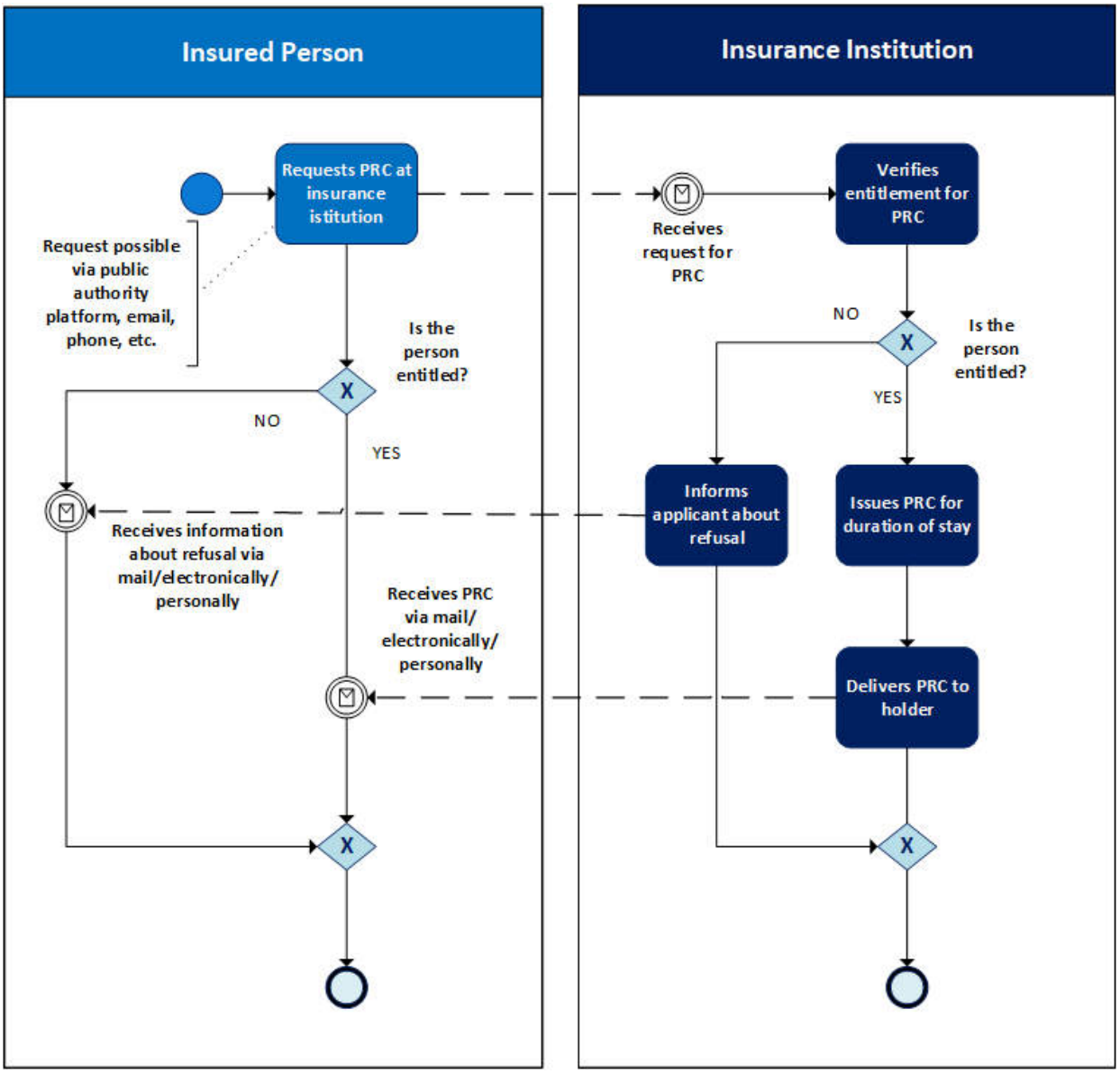


Figure 3 -Issuance flow of the PRC (Source: DC4EU)

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

We believe, that with the introduction of the digital EHIC, the PRC in its current form will become obsolete. In fact, the loss or inaccessibility of the digital EHIC credential would entail, at most, a re-issuance of the credential itself, and therefore eliminating the need for a Provisional Replacement Certificate in digital form.

3.2.2 Summary of Current Process Workflows

Currently, the EHIC process workflows can be summarized as follows:

Table 1 – Current EHIC process workflows

Activity	Description	Actor
Issues the physical card	Issuance of the card differs between Member States according to internal norms. The EHIC can be either issued automatically after its expiry date or must be requested via application by the citizen.	Competent institution of the Member State
Stores the physical card and presents it in case of need	If the citizen requires urgent and necessary medical treatment while travelling in a different Member State, they show the EHIC in order to receive such treatment on the same terms as those applicable to persons insured under the legislation of the Member State of stay. Many countries also require providing an identification document together with the EHIC.	Citizen

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Checks the validity of the card, fills out the form and sends the refund claim	After checking the validity of the card, the healthcare provider fills out the claim for refund of benefits provided on the basis of the EHIC. The healthcare provider is also **obliged to keep a copy of the EHIC** in order to claim the refund. It later sends the claim to the competent institution of the Member State of residence (of the citizen).	Healthcare provider of the Member State of stay
Accepts/rejects the refund claim	The competent institution cannot reject the refund on the grounds that the citizen has ceased to be insured in the Member State of residence. It can, however, reject the refund if the information is incomplete or incorrectly filled out, or if the medical treatment has not been given within the validity period of the EHIC.	Competent institution of the Member State of residence

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

3.2.3 Central Repository for the Issuers of the EHIC – As/Is Analysis

The Electronic Exchange of Social Security Information (EESSI) is a system funded by the Connecting Europe Facility (CEF) deploying cross-border digital services that allows the exchange of social security information between relevant EU institutions. The EESSI Institutional Repository is thus a crucial database for social security competencies. This repository can serve as a reference model for establishing a trust framework for issuers and verifiers, indicating a notable consistency across countries. [9]

While this component is EESSI-specific, it may not be suitable for populating qualifications into an ecosystem like EBSI using EBSI's unique services and capabilities.

The EHIC contains a personal identification number (PIN) that is displayed on the physical EHIC card. In most member States the EHIC PIN is the same as the PIN on the national health care card. Regarding the storage of this PINs, most EU Member States maintain a centralized national database to store and manage PIN information, Germany is the exception. For countries where the EHIC PIN differs from the PIN on the national health insurance card, dedicated databases are used to store this PIN information. These countries include Switzerland, France, Netherlands, and Portugal. Four countries (Denmark, Ireland, Netherlands, and Sweden) do not have dedicated databases for the PINs indicated on the EHIC.

3.3 Verification

3.3.1 The Verification Process of the EHIC/PRC – As/Is Analysis

When an individual presents their EHIC or PRC to a verifier during a visual inspection, the verifier also verifies the person's identity in order to confirm that the person presenting the EHIC/PRC is indeed the rightful holder of the card.

Therefore, the verification process starts when the insured person presents their EHIC/PRC to the verifier, which may, for example, be a healthcare provider. Upon receipt, the health care provider verifies the identity of the person (ID), and then verifies the validity of the EHIC/PRC presented. If the verification of the EHIC/PRC and of the ID are successful, it proceeds with the visual inspection.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

After the visual inspection, the healthcare provider copies the EHIC/PRC. It sends 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. If either the EHIC/PRC or the ID verification is unsuccessful, the health care provider informs the person about the negative verification. Once the health insurance institution receives the EHIC/PRC copy and the invoice, it initiates the reimbursement process.

This process includes the recognition of the health care services, the calculation of costs, and the reimbursement to the health care provider.

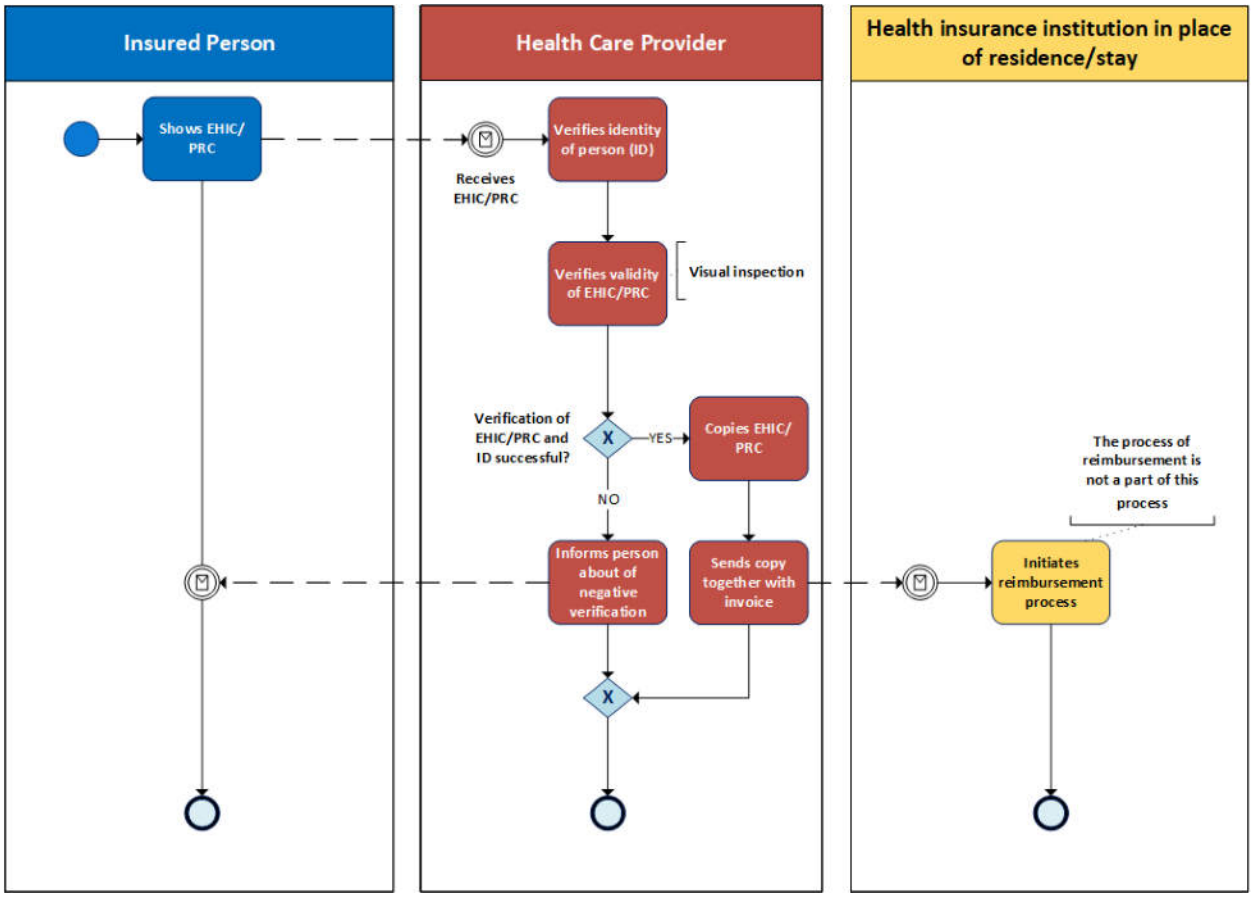


Figure 4 - Verification flow of the EHIC/PRC (Source: DC4EU)

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

3.3.2 Central Repository for the Verifiers of the EHIC – As/Is Analysis

To understand the workings of a trust model, it is important to enquire about the procedures for onboarding verifiers within these ecosystems. In Austria, for instance, healthcare providers require a legal authorisation, often leading an entry in a national registry. This raises questions about establishing registries for verifiers, aligning with eIDAS regulations, and trust service principles. Understanding how these registries evolve, handle events like mergers or deactivation, and maintain institutional records will provide insights into the workings of a trust model.

Across the surveyed countries, it is notable that the majority, specifically eleven nations (Austria, Switzerland, Czechia, Germany, Denmark, France, Ireland, Latvia, Netherlands, Poland, Portugal, Sweden), have confirmed a central national repository for healthcare providers. This repository serves as a centralized database where essential information about healthcare providers is maintained.

3.3.3 Documentation Process for the EHIC – AS/IS Analysis

Identity Documentation:

In the context of identity verification for EHIC issuance, six countries (Austria, Germany, France, Latvia, Poland, Sweden) mandate identity verification, while five countries (Czechia, Denmark, Ireland, Netherlands, Portugal) adopt an optional approach. Notably, none of the surveyed countries indicated a lack of necessity for identity verification. Among them, five countries (Austria, Czechia, France, Latvia, Sweden) document the identity verification process, while three countries (Germany, Ireland, Netherlands) specified that they do not maintain documentation. It’s noteworthy that the remaining countries did not provide a response to the question mentioned.

Verification Process Documentation:

Regarding the documentation of the EHIC verification process, twelve countries (Austria, Switzerland, Czechia, Germany, Denmark, Finland, France, Ireland, Latvia, Netherlands, Poland, Sweden) follow a practice of documentation, whereas Spain and Portugal do not adhere to this practice. Typically, a copy of the EHIC serves as evidence, and in many instances, this

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

documentation is stored and made available upon request. The retention period for these records varies across countries, with the prevailing approach being to preserve them until the completion of the cost settlement period.

3.4 The Onboarding Processes for Issuer and Authorized Verifiers for the EHIC – As/Is Analysis

3.4.1 The Onboarding of Issuers for EHIC - As/Is Analysis

In most Member States, there is **no formal onboarding process for issuers** since new issuers are not anticipated, and they are legally mandated entities. This differs significantly from the education use case, where there may be more flexibility. Typically, the number of issuers remains low or remains stable. Authorization for issuers is generally governed by national law. In some cases, private companies, such as those in the Netherlands, also issue EHICs and are mandated by law. Extensions of authorization are usually not required, as they are typically unlimited in duration.

In the event of **issuer mergers**, these must adhere to Decision E2 regulations, which are legally binding and subject to supervision. If changes occur in user data or the responsible competent institution changes, the EHIC must be invalidated, and a new EHIC must be issued. The old EHICs remain valid until the exchange is completed.

Regarding the **deactivation of an issuer**, this process must also align with Decision E2 regulations. Deactivation is managed in national registries and within the Institutional Repository (IR). The necessary information flow is coordinated through EESSI. A successor must be designated, and insured individuals are responsible for cancelling or changing their insurance. New EHICs must be issued by the new insurance institution, and transitional arrangements can be made for the insured during this period.

Maintaining the institutional repository is a crucial aspect, serving as a reference model for the trust framework. A supervisory authority communicates with the IR SPOC (Single Point of Contact), which is responsible for maintaining and updating the institutional repository, and ensures immediate changes are implemented. These processes include registering institutions, and in the context of EBSI, a TAO (Trusted Authority Organization) will take on this role.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

3.4.2 The Onboarding of Authorized Verifiers for EHIC - As/Is Analysis

Authorized Verifiers in the EHIC system typically refer to healthcare providers. The **onboarding process for verifiers** involves their registration in national registries and the establishment of contracts with insurance institutions. Legal frameworks govern healthcare providers' authorization, and in most Member States, there is no defined process for extending this authorization since it is usually unlimited. If a contract expires, it must be renewed.

When **changes occur in verifier data**, national registries must be promptly updated. In some cases, changes may require approval from a supervisory authority, and existing contracts need to be modified accordingly. In the event of verifier mergers, registries must also reflect these changes, possibly requiring supervisory approval, and existing contracts should be updated to align with the new entity.

For the **deactivation of a verifier**, their license is revoked, and they are removed from healthcare provider records in national registries. Contracts must be formally terminated.

The **maintenance of the national repository** varies among Member States. For example, in Germany, the responsibility for updating the registry falls upon each federal state.

3.5 Conclusion

This chapter has provided an in-depth analysis of the European Health Insurance Card (EHIC), elucidating its significance, challenges, and operational mechanisms. The investigation delved into various aspects of the EHIC, including its legal basis, characteristics, issuance, and the intricacies of cross-border healthcare facilitation. Notably, the chapter highlighted the disparities in EHIC issuance and validity across different EU Member States, underscoring the need for standardized practices.

Key challenges identified include issues related to the application, issuance, validity, reimbursement processes, and the occasional refusal of the EHIC by healthcare providers due to misunderstandings. These challenges are compounded by the varying interpretations of "unplanned" and "necessary" healthcare, as well as discrepancies in the card's validity period.

The potential for digitalization of the EHIC is a significant theme, offering solutions to several of these challenges, especially those associated with the physical format of the card. The chapter also explored the role and functioning of the Provisional Replacement Certificate (PRC) as a

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

temporary solution in the absence of EHIC which would be rendered futile with the digitalization of the EHIC.

The analysis delved into the processes of EHIC issuance, including the automatic and request-based issuance methods, and the procedures for EHIC verification.

In summary, the chapter presents a nuanced understanding of the EHIC, recognizing its critical role in facilitating healthcare access across the EU while also acknowledging the need for further improvements, particularly in terms of standardization, digitalization, and education about its usage.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

4 Analysis of the Current Status of PD A1

This chapter aims to present a thorough analysis of the Portable Document A1 (PD A1), a key instrument in the European social security framework. The insights and findings within this chapter are underpinned by extensive data acquired from the DC4EU Consortium's questionnaires, alongside the empirical insights derived from the ESSPass pilot project focusing on the PD A1. The objective of this analysis is to examine the functional attributes, legal and operational contexts, and the challenges associated with the PD A1. This chapter seeks to provide a comprehensive and critical examination of the PD A1, offering insights into its application within the landscape of European social security coordination. Through this analytical approach, we endeavour to shed light on the dimensions of the PD A1, thereby contributing to a deeper understanding of its role and significance within the broader framework of social security coordination across Europe.

4.1 The PD A1 - General

The Portable Document A1 (PD A1) is a document that confirms which social security legislation applies to a worker not affiliated with the country of work. It is useful for individuals who work in multiple European countries or are posted workers, as it helps demonstrate their payment of social contributions in another European nation.

It is issued by the social security institution in the EU, Iceland, Liechtenstein, Norway, Switzerland, or the UK, where the worker pays contributions. It is a required document for posted workers who temporarily work in another country.

WP5 will identify use case interactions for PD A1 and establish the onboarding process for issuers in multiple releases to ensure continuous delivery and minimize the time required to initiate the test piloting phase.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

4.1.1 PD A1 Current Legal Framework

While carrying the PD A1 is not mandatory for workers moving within the European Union, it is highly recommended. The PD A1 can expedite processes in the event of work-related accidents or occupational diseases. This document certifies the social security status of the individual in various scenarios, ensuring that the social security laws of the issuing Member State are applied. It also confirms that the individual is exempt from paying social security contributions in other Member States.

Under Regulation 987/2009, employers or concerned individuals are required to notify the competent authorities about their activities in another Member State, preferably before commencing such activities. After verifying the specific conditions outlined in the EU regulations for different cases (like self-employed, posted employees, or those working in multiple states), the competent institution issues the PD A1. [5]

In cases of employee postings, the A1 certificate is issued by the competent institution and communicated to the institution in the other relevant member state through the EESSI system. Relevant posting details must be conveyed to the institution of the destination state.

Additionally, EU citizens, that exercise their right for free movement in the Single European Market can transfer specific healthcare and pension benefits from their home country to their new country of residence.

Given the rising number of posted workers and the risks of fraudulent use and falsification of the PD A1, it's crucial to implement a document traceability system to ensure its authenticity.

Regarding the A1 certificate issued for workers, pursuing work in a Member State other than the one in which they are insured, the information that must be reported for each worker is the following:

- Personal Details of the holder (identification data);
- Member State legislation which applies (with starting date and ending date);
- Status of the holder. It must be indicated whether the person is an employed or self-employed posted person etc;
- Details of Employer/Self-Employment (home state);
- Details of Employer/Self-Employment (host state);
- Institution completing the form.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

4.1.2 Characteristics of the PD A1

Based on a questionnaire prepared by the DC4EU Consortium the following outcomes were shared with EBSI-VECTOR. Concerning the form of PD A1, 11 respondents confirmed digital formats, predominantly in PDF form (Austria, Belgium, Czechia, Denmark, Finland, Germany, Ireland, Poland, Portugal, Slovakia, Sweden). Seven respondents mentioned paper formats (Austria, France, Lithuania, Latvia, Netherlands, Portugal, Switzerland). It's noteworthy that some member states allow flexibility in the form of PD A1, permitting a combination of paper and digital (PDF) formats.

Member States have varying validity periods in accordance with their national rules and regulations. In most countries:

- Limited/temporary PD A1 credentials: default type issued in Europe.
- Provisional temporary PD A1 credentials are issued in all respondent countries (except Austria, Belgium, Switzerland, Czechia, Netherlands, and Poland).
- Unlimited PD A1 credentials are typically not issued (with exceptions in Spain and Portugal), these PD A1s retain validity indefinitely, subject to maintaining eligibility criteria.
- Provisional unlimited PD A1 credentials are generally not issued (except in Portugal).

These variations in validity periods across Member States are significant considerations for our modelling approach.

4.1.3 Central Repository for the PD A1 – As/Is Analysis

In many countries, PD A1 storage is typically centralized, and access to the central database of all valid PD A1s is subject to the legal authority of an institution. This necessitates the existence of (separate) repositories for both issued and received PD A1s, each serving as a valuable tool for cross-verification in the back office. It is important to note that the repository for incoming PD A1s is valuable for verification purposes in the country where the activity is pursued.

Based on the aforementioned DC4EU questionnaire, all 18 respondent countries have affirmed the utilization of a centralized database for maintaining valid PD A1 documents.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

For incoming PD A1 documents (Host Member State storing PD A1s issued in another Member State), centralized storage is implemented in Belgium and Germany (two countries).
Concerning outgoing PD A1 documents (Member State storing their own issued PD A1s), centralized storage practices are observed in the Czechia, Ireland, Poland, Slovakia, Spain, and Sweden (six countries).
In 10 countries, namely Austria, Switzerland, Denmark, Finland, France, Italy, Latvia, Lithuania, Netherlands, and Portugal, both incoming and outgoing PD A1 documents are centrally stored.

For instance, when an inspector requests credentials from a citizen, these databases are employed to cross-reference information and identify any potential fraud or misuse. This is a significant consideration because certain processes can potentially be replaced by efficient solutions involving digital wallets and registries. When referring to the legal competencies of institutions, we address the question of who is authorized to perform verifications, a crucial aspect of identifying qualified verifiers.

4.2 Issuance

4.2.1 The Issuance of the PD A1 – As/Is Analysis

Employers or self-employed individuals can initiate the issuance of the PD A1 by submitting requests through various means, including public authority platforms, emails, payroll accounting, or in-person interactions.

The application process outlined here is not a part of the ecosystem's user journeys but acts as a catalyst for credential issuance. Once approved by the Competent Institution the paper/PDF PD A1 is issued and delivered to the applicant, whether they are an employee or a self-employed individual. It is essential to note that while this process occurs outside of our ecosystems, it plays a vital role in initiating the issuance of the PD A1 credential.

Note: The issuance of the PD A1 is contingent on the institution's competence and its utilization for specific employment groups. The criteria for PD A1 issuance regarding particular categories of individuals are detailed in the Regulations on applicable legislation. Depending on the individual's circumstances, different conditions may apply under these regulations.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

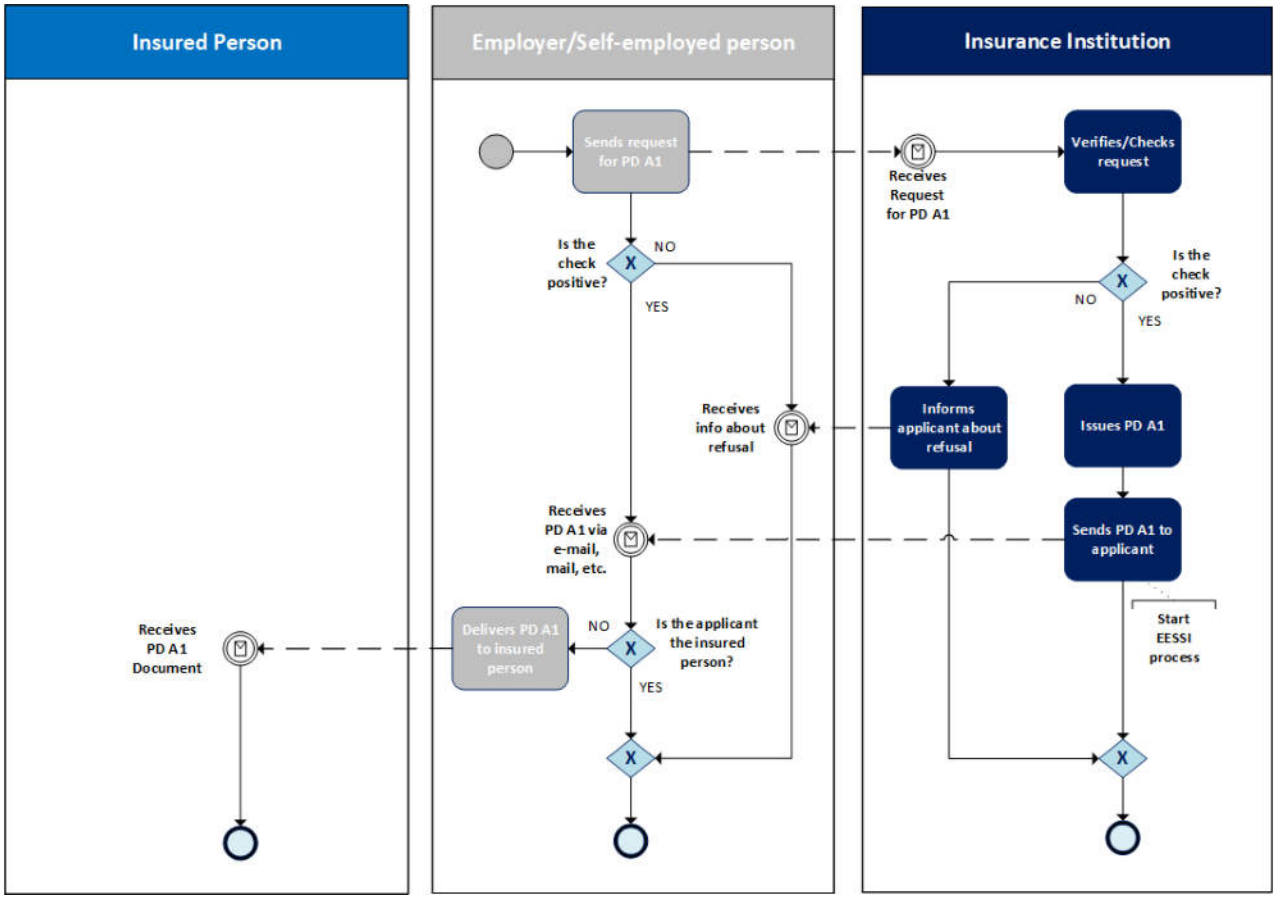


Figure 5 - Issuance flow of PD A1 (Source: DC4EU)

4.3 Verification

4.3.1 The Verification Process of PD A1 – As/Is Analysis

When an individual presents their PD A1 to a verifier during a visual inspection, the verifier also verifies the person's identity. Subsequently, a back-office process is initiated to cross-reference the presented PD A1 with a database to detect potential fraud or errors. This necessitates the transfer of information to the back-office system, as previously mentioned, and becomes an integral part of the business process.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

In some countries, the verification of identity is documented. Similarly, 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.

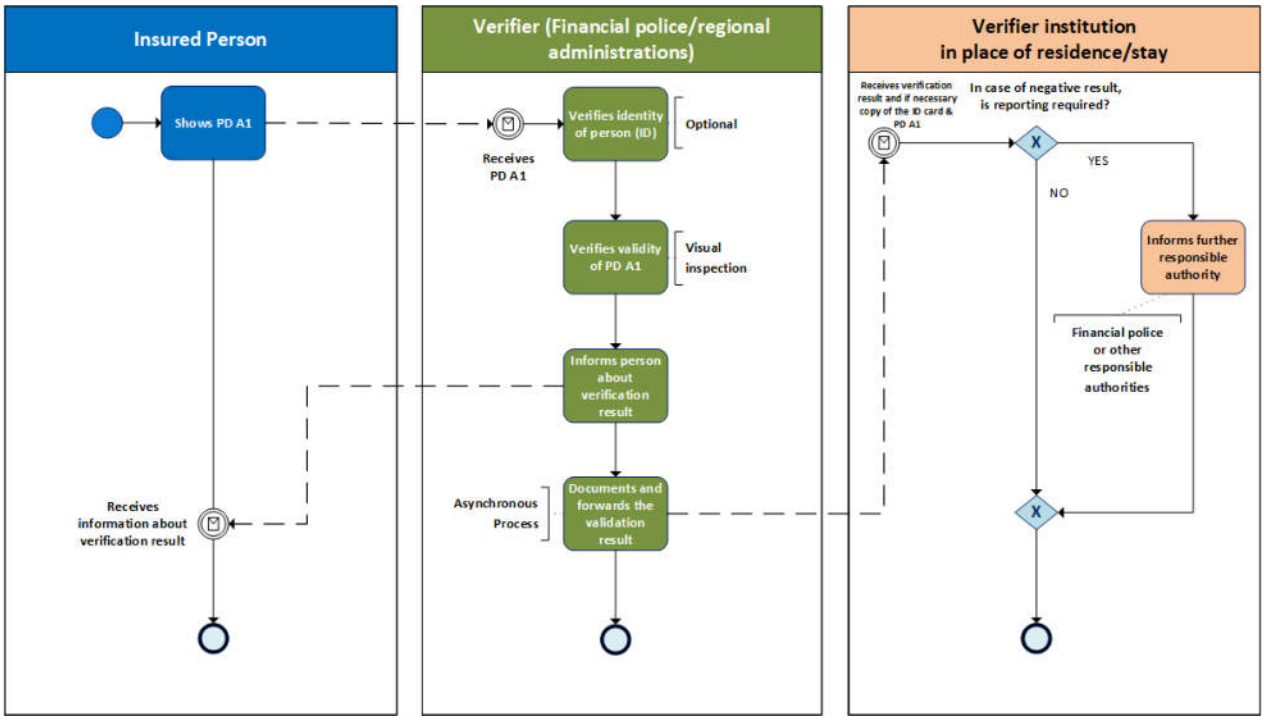


Figure 6 - Verification flow of the PD A1 (Source: DC4EU)

4.3.2 Documentation Process for the PD A1 – AS/IS Analysis

Documentation Identity:

The majority of respondent countries acknowledge the necessity or the option of identity verification, with none reporting the absence of such verification. Among these, four countries (Switzerland, Czechia, Germany, Italy) specified that they document the identity verification process, while four countries (Austria, Belgium, Portugal, Slovakia) mentioned that they do not maintain documentation for identity verification. Five countries did not provide any response.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Verification Process Documentation PD A1:

All respondent countries confirmed the practice of documenting the verification of PD A1. Six countries did not provide any response. The documentation processes for PD A1 verification vary among countries, with records stored in diverse 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 contingent upon national regulations.

4.3.3 Central Repository for the Verifiers of the PD A1– As/Is Analysis

Regarding the central registration practices, five countries (Belgium, France, Italy, Portugal, Switzerland) have confirmed having a central database for verifiers. On the other side, ten countries (Austria, Czechia, Finland, Ireland, Latvia, Netherlands, Poland, Slovakia, Spain, Sweden) mentioned they do not have a database for verifiers. Notably, three countries did not answer this question. What stands out is that, in general, most European countries do not use a central repository for verifiers of a PD A1. This means that how countries organize and manage verifier-related activities can differ quite a bit.

4.4 The Onboarding of Issuers and Verifiers for PD A1 – As/Is Analysis

4.4.1 The Onboarding of Issuers for PD A1 - As/Is Analysis

In most Member States, there currently exists no formal onboarding process for new issuers, primarily because PD A1 issuers are mandated by law, much like EHIC issuers. This is especially true for PD A1 since there are typically no private issuers (with social security institutions being the primary issuers in most cases), resulting in a relatively low and stable number of issuers. Authorization for an issuer is typically governed by national legislation, with authorization often being unlimited in duration.

Changes in issuer data are carried out following Decision E2 and are regulated by administrative commission decisions [7]. These changes are made in national registries and the Institutional Repository (IR), with an essential information flow through EESSI. Issued PD A1s remain valid during these changes.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

In line with Decision E2, a merger of issuers involves data migration to the newly competent institution and issued PD A1s remain valid throughout this process.

The deactivation of an issuer aligns with Decision E2, with deactivation procedures executed in national registries and the Institutional Repository. This process requires the appointment of a successor.

Institutional Repository maintenance is initiated when a supervisory authority or ministry notifies the IR SPOC (Single Point of Contact), who promptly updates the IR.

Note: In contrast to the EHIC, changes in issuer information do not necessarily invalidate PD A1 credentials. This distinction will have implications for our revocation model.

4.4.2 The Onboarding of Authorized Verifiers for PD A1 - As/Is Analysis

Authorized Verifiers are primarily public authorities, such as financial police, the Ministry of Labour or social security institutions, depending on national regulations, and as they are mandated by law, there is typically no registration process in place for them.

In most Member States, there currently exists no formal onboarding process for new verifiers, as the expectation is that no new verifiers will be added. Verifier authorization is predominantly governed by legal regulations, with most verifiers having unlimited authorization.

As there is no anticipation of changes, there is generally no established process for modifying verifier data. However, national registries must be updated to manage access changes, particularly in cases like Germany where access management for the PD A1 database requires updates.

Similar to other scenarios, there is typically no existing process for handling verifier mergers, as these situations are not expected. When necessary, national registries must be updated to accommodate access management changes, often involving a legal decision.

In cases where a verifier needs to be deactivated, national registries must be updated to manage access changes, with the removal of verifier access contingent on a legal decision. This process, as seen in Germany, may also require updates to access management for the PD A1 database.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

National repositories for verifiers are not widely established in Member States. In some instances where verifiers are listed in the Institutional Repository, updates may be required, specifically if the verifiers are considered competent institutions.

4.5 Conclusion

This chapter has analyzed the Portable Document A1 (PD A1), a component in the European social security framework, by integrating extensive data from the DC4EU Consortium's questionnaires and insights from the ESSPass pilot project. The PD A1, instrumental for workers across European nations, especially those engaged in cross-border employment, serves as a confirmation of the applicable social security legislation, and helps in the administration of social security contributions and benefits.

The chapter comprehensively addressed the legal framework, operational context, and challenges linked with PD A1. The issuance process of PD A1, as outlined, involves various application methods and is critical in triggering the PD A1 credential issuance. In the realm of verification, the chapter described procedures involving identity checks and cross-referencing with databases to identify fraud. Documentation practices and storage durations for these verifications vary across countries, reflecting different national regulations. Furthermore, we delved into the centralized registration practices for verifiers, noting significant variations among Member States. The lack of a central repository for verifiers in most countries indicates diverse approaches to managing verifier-related activities.

In terms of issuer and verifier onboarding, we have found that, typically, no formal onboarding process exists in most Member States, given that issuers and verifiers are often legally mandated entities. The authorization and data management processes are governed by national legislation and administrative decisions, with necessary updates managed through national registries and the Institutional Repository.

In conclusion, this chapter provided a thorough examination of PD A1, highlighting its role in the European social security system.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

5 System Architecture

This chapter delves into the task of defining a system architecture, an endeavour guided by the imperative to harmonize with the pre-existing infrastructures of public entities. Such a design demands consideration to avoid disruption to these established systems. Central to this effort is the facilitation of interoperability, ensuring that the architectural framework is not only compatible across national boundaries but also seamlessly integrated. This model, conceptualized as the Enterprise Wallet in EBSI-VECTOR, is envisioned to streamline the issuance and management of credentials. By doing so, it sets the stage for a more interconnected and efficient digital ecosystem for the issuance and management of credentials. The ensuing discourse in this chapter is not just a technical exposition but also a strategic blueprint, laying the groundwork for a system that is robust, adaptable, and forward-thinking, addressing the current and future needs of the EBSI-VECTOR project.

5.1 The Actors

Actors are subjects that play roles within the framework of digital certifications lifecycle.

There are two types of actors in this lifecycle: legal entities (which can be private organizations or public bodies) and citizens:

1) Legal Entities: these can be private or public organizations that issue, verify, hold, share digital certificates;
2) Citizens: these can be workers, retirees, students, etc., who request, hold, share, and verify digital certificates.

These actors play four possible roles in the Verifiable Credentials' ecosystem for social security coordination:

- A (Trusted) Issuers of credentials, could be any subject (legal person or not) capable of issuing credentials. When the issuer is identified as "trusted", it would be legally recognized as a competent institution, e.g., in the context of social security, a trusted issuer of PD A1 or EHIC which acts on behalf of an Authentic Source (as defined in the eIDAS Regulation, see below) based on the onboarding process described in Chapter 8 of this document;

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- An Authentic Source[1] is 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 recognized as authentic in national law;
- The holder of credentials is a citizen who stores their credentials into their EBSI-eIDAS 2.0 compliant wallet;
- The Verifier validates the credential.

The authentic source may act as issuer itself (when trusted) or could delegate this service to another issuer, which handles tasks such as credential creation and allows users to download these credentials into their wallets. It is important to distinguish between these roles, with the authentic source being a significant component specified in the eIDAS regulation. It is worth noting that the concept of an issuer differs between public services and qualified issuers in the private sector, as a distinction is now incorporated into the new version of the eIDAS regulation (eIDAS 2.0). This may affect the trust model and technical details e.g., for signing, while having no effect on the System Architecture as described in the following.

5.2 The Architecture

Figure 7 shows the general issuance process as envisioned by EBSI. The two main Use Cases “Issuance of Verifiable Credentials” as well as “Presentation of Verifiable Presentation” are shown. The differentiation of Verifiable Credential (VC) and Verifiable Presentation (VP) is an important concept in the ecosystem.

For the sake of this project, a VC must comply with the definition of (qualified) electronic attestation of attributes ((Q)EAA) given by the eIDAS Regulation, issued by an Issuer on behalf of an Authentic Source [10]. Again, this may be the same institution. Besides the Business Data, references to relevant EBSI-Registries are included. These Registries are about the Issuers accepted Data-Schemas. Through these Registries trust is established in the ecosystem. As there also could be the need of ensuring trust on some verifiers there could be a Verifier Registry, too limited to authorized verifiers. The presence of a Verifier Registry will not, however, limit the right of citizens to send their VC/VP to other “unregistered” verifiers, in compliance with Article 6a of the proposed eIDAS 2.0 Regulation, which states “that all natural and legal persons in the

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Union have secure, reliable, trusted and seamless access to cross-border public and private services, while having full control over their data" [10].

With the help of the EBSI-Registries every VC can be trusted and verified on its own, without any interaction with the Issuer.

Finally, the Verifiable Credential is cryptographically signed by the issuer and can afterwards be downloaded by the citizen using the OID4VCI Protocol. The VCs are stored in the EBSI-compliant wallet. For the Holder-Verifier interaction the OID4VP Protocol is used to establish mutual trust. After trust is ensured, the holder may share a Verifiable Presentation (VP) with the Verifier.

A VP is derived from one or more VCs, encapsulated by Presentation Data including the signature of the Holder(-Wallet). As an example, multiple VCs can be bound and presented alongside with a separate Identity-Credential (e.g., VID, PID) to prove identity.

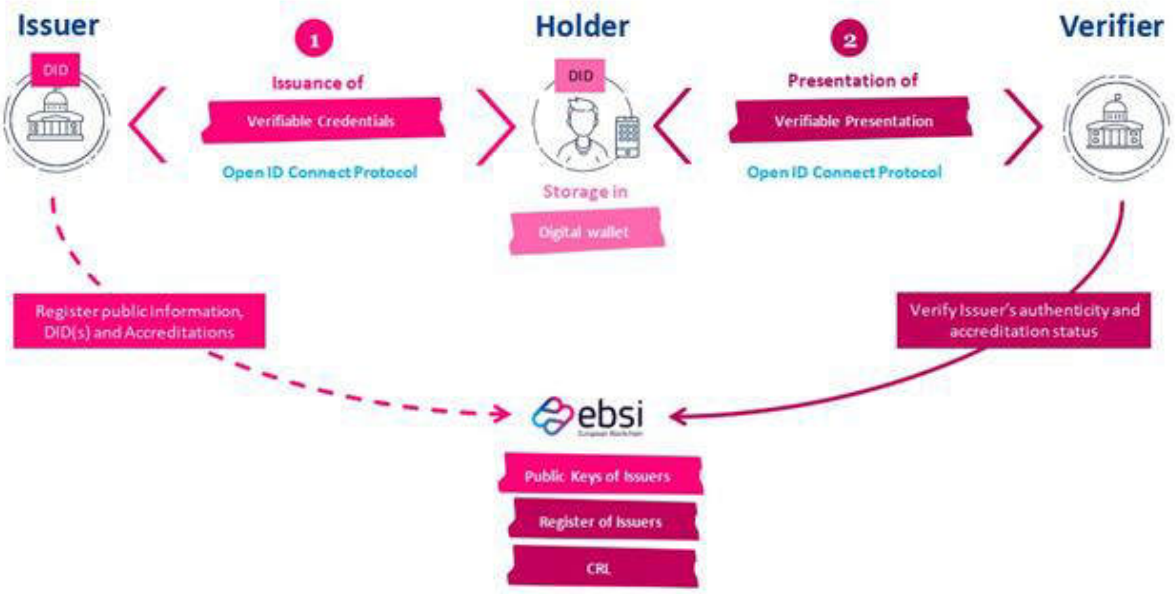


Figure 7 - Current EBSI ecosystem [11]

For Issuers and Verifiers to interact with the Citizen and Registries a specific IT System needs to be in place. This System is referenced here as Enterprise Wallet and will have capabilities to cover the various needs for different Use Cases. In the following sections, the required capabilities for social security will be covered.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

5.3 Social Security Issuer diagrams

There are different possible setups for the Issuer in the context of social security. These depend on whether an Issuer is responsible for multiple authentic sources and the security of the current system of the Issuer organisation. The Enterprise Wallet is expected to be an autonomous, ready to deploy component that can be used by Issuers with little configuration. It will be responsible for creating and delivering the Credentials including key management and other required capabilities.

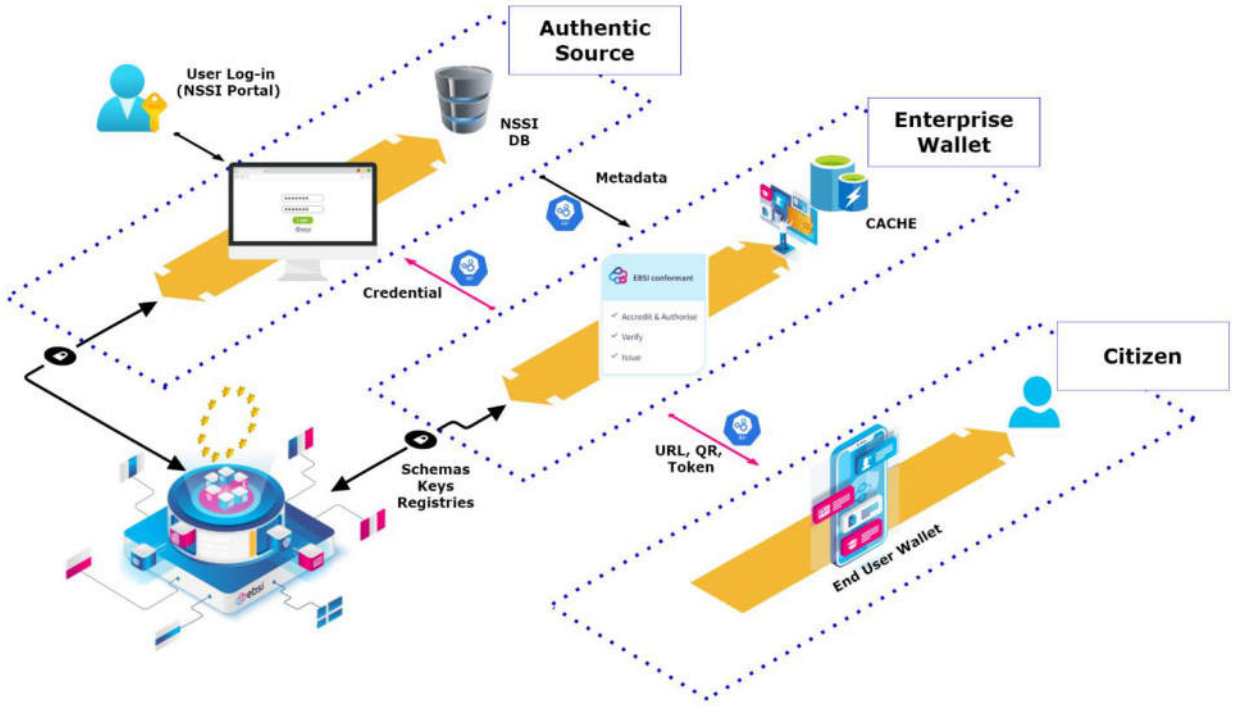


Figure 8 - Issuer flow diagram using Cache Component

This Issuer component of the Enterprise Wallet aims to be stateless and therefore will not store any privacy-related information. For this purpose, a Cache component is envisioned to temporarily store all relevant business and functional data, while operational logs and data (non-privacy disclosing) can be stored (semi)permanently to comply with national legislations/requirements. Institutions can deploy this component or develop their own component inside their core systems. This component includes a mapping plugin to match an approaching wallet-identity to available documents for this identity. Functionalities like identity mapping are further described in the Annex “Backoffice Interfaces”.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

One or multiple Authentic Sources provide the business data to the Issuer (the Issuer may be an Authentic Source itself) alongside a request to issue a VC. The data gets processed in the Issuer Core System and afterwards pushed into the Cache System. The Cache System then creates the Deeplink and QR-Code for download. Afterwards the National SSI Portal can display the attestations available in the Cache to the Citizen, based on a REST-API. Then the EBSI-Wallet approaches the Enterprise Wallet to download a specific credential. General checks, including the mapping of the identity data, will be done in the Enterprise Wallet. When successful the Wallet-Identity of the Citizen can be checked against the identification data of the attestation. Finally, the attestation business data is sent to the Enterprise Wallet and the VC is created.

This setup is expected to be used for piloting by DC4EU which may also be suitable for the EBSI-VECTOR approach. It is easy to deploy and doesn't need many customizations for Issuers. It also adds security since the Enterprise Wallet doesn't call into the Core Databases of the Issuer.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

5.4 Verifier Architecture

For the Verifier Architecture the Enterprise Wallet needs to have a suitable component available to create Proof Requests (including Verifier Identity) and verify the Verifiable Presentation in the response of the Citizen Wallet. However, we expect that the verification request can also come from the citizen side.

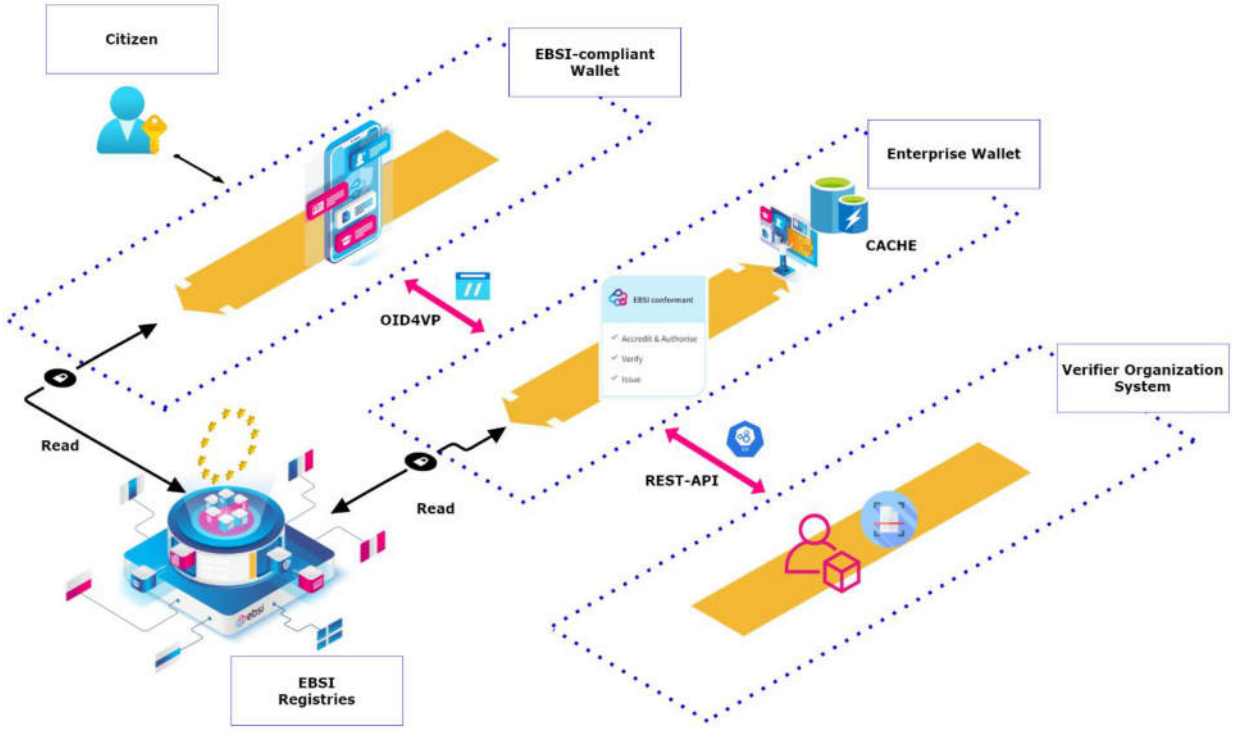


Figure 9 - Verifier Architecture with interface to Verifier Organisation

In addition to using the OID4VP Protocol several transmission protocols need to be supported for both sending and receiving interaction. This protocol shall support different interaction mechanisms, such as QR-Code, NFC, Bluetooth, and Endpoint. A detailed explanation of the mentioned interactions will be provided in the following chapters.

To establish mutual trust the Enterprise Wallet needs to send a Verifiable Identity with a Proof Request. The EBSI-compliant wallet may verify this identity against EBSI-Registries whenever the request is coming from an authorized verifier. After successfully checking the verifier and its authorization to demand presentation of specific credential types, the holder can respond with the chosen transmission method between the presented available ones. The Enterprise wallet at

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Verifier side will then perform the validation and check against the registries on their part. In conclusion, interfaces to the EBSI-Registries are required in both wallets.

The result of the verification process is then processed and sent to the backend system of the Verifier organization by the Enterprise Wallet in order to allow for further processes, e.g., reimbursement processes between Member States in the EHIC use case or documentation of violations in the PD A1 use case.

5.5 Conclusion

This chapter on System Architecture offers a comprehensive view of the structural design proposed for the implementation and integration of the Enterprise Wallet within the EBSI-VECTOR project in the realm of social security. This chapter underscores the importance of harmonizing with existing public entity infrastructures, focusing on interoperability to ensure seamless integration across national boundaries. The envisioned Enterprise Wallet model aims to facilitate the streamlined issuance and management of credentials, contributing significantly to a more interconnected and efficient digital credential ecosystem.

The chapter outlined the roles of various actors in the digital certification lifecycle, including legal entities and citizens, each playing distinct roles in the Verifiable Credential ecosystem. It emphasizes the importance of the Authentic Source and its relationship with Trusted Issuers. The role of the EBSI-Registries in establishing trust and the autonomous functionality of the Enterprise Wallet are key highlights of the chapter. The proposed system architecture, including the Issuer and Verifier setups, is aimed at facilitating secure and efficient interactions between citizens, legal entities, and EBSI.

Through various diagrams and detailed descriptions, the chapter lays out a proposed strategic and technical blueprint for a robust, adaptable, and forward-thinking system. It sets a solid foundation for addressing both current and future needs of the EBSI-VECTOR project, paving the way for a more streamlined and digital interaction landscape in European social security.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

6 Definition of the Business Processes of EHIC and PD A1 Credentials

In this chapter we delve into a comprehensive examination of the business processes surrounding the European Health Insurance Card (EHIC) and the Portable Document A1 (PD A1) credentials. Our approach is anchored in a structured analysis of the prerequisites, core use cases and the interactions required for the effective execution of user journeys. In terms of core use cases, we explore the procedural aspects of issuing, revoking, and verifying credentials, emphasizing the importance of a coherent and functional system that aligns with the long-term vision put forth by the European Commission for the digitalization of social security credentials. Furthermore, our discussion extends to secondary use cases such as credential delegation, self-verification, and proof of verification, underlining their significance in the broader context of social security coordination. This analysis is aimed at delineating a clear and coherent framework for managing EHIC and PD A1 credentials, thereby contributing to the efficiency and efficacy of the European social security system.

6.1 Prerequisites for Executing User Journeys

To facilitate the user journey, several prerequisites are essential:

- Installation of a Digital Wallet: Citizens must install a digital wallet on their devices. For optimal compatibility, the wallet should adhere to the European Blockchain Services Infrastructure (EBSI) standards and be eIDAS-compliant;
- Onboarding Qualified Verifiers: Establish comprehensive onboarding procedures to ensure authorized verifiers are fully qualified and understand the verification process;
- Download Service Provision: The competent social security institution must provide a reliable download service for citizens to access necessary digital credentials. This service will be provided by the Enterprise Wallet;
- Enterprise Wallet: Implement an issuer & verifier system that utilizes OpenID Connect for Verifiable Credentials Issuance (OpenID4VCI) protocols. This system should be maintained by the social security institution responsible for issuing credentials and by the verifying institution;

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- Reliable Internet Connectivity: Guarantee robust and reliable internet connections to facilitate uninterrupted access to required services.

By improving the clarity and precision of each prerequisite, stakeholders will gain a deeper comprehension of the necessary requirements and infrastructure for the effective implementation of digital credentials. The involvement of stakeholders in the engineering of business requirements is enhanced through collaboration with DC4EU.

It is crucial to note that while these elements are vital for pilot implementations, apart from the integration of the Authentic Source, their detailed architecture definition and technical implementation falls within the scope of other work packages, such as WP3, rather than WP5. Nevertheless, they represent essential prerequisites for the successful execution of the envisioned user journeys.

6.2 Core Use Case Interactions

The success of WP5's social security pilot is anchored in a suite of critical components, collectively identified as our core use cases. These vital elements – encompassing the issuance, revocation, and verification of credentials – form the cornerstone of the pilot's structural integrity.

6.2.1 Issuing of Credentials

This use case scenario pertains to the issuance of Verifiable Credentials in the context of social security being a public service with extensive involvement of e-government platforms. Therefore, the issuance process is closely linked to national e-government practices. Our objective is to establish a generic approach that can be applied in any country in combination with a competent institution for social security coordination. In the context of credential issuance, the user journey commences with a request from the authentic source to the Enterprise Wallet for the issuing of digital credentials, serving as the triggering event for the journey. This journey encompasses various stages, including notifying the citizen to download specific items, with a significant emphasis on the role of identity verification concerning the credential. Consequently, our primary focus is on the user journey associated with credential issuance, representing the initial phase and a potential candidate for the first pilot or feasibility study.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

6.2.2 Revocation of Credentials

This use case scenario pertains to credential revocation, a crucial element for both EHIC and PD A1 use cases. EBSI has been exploring revocation over the past few months, partly due to the influence of social security considerations (DC4EU, EHIC digitalization) and our workstream in VECTOR. A promising reference model for how revocation could function effectively has been previewed by some of our WP5 partners. Our next steps involve a comprehensive examination of this user journey, including defining revocation requirements, exploring the technical aspects, and integrating it into the EBSI framework.

6.2.3 Verification of Credentials

A crucial use case scenario revolves around the verification of credentials, specifically addressing the methods for credential verification. This encompasses several user journeys, including verification conducted by qualified/authorized verifiers (following the eIDAS regulation's verifier qualification standards).

When the verification is triggered by a digital request, trust in the requesting party is essential, and the requester's identity and entitlement must be verifiable. However, there are scenarios where unqualified verifiers are encountered, particularly in cases where onboarding all verifiers could be impractical or whenever the verification is triggered by holder.

For instance, in the context of PD A1, there are two distinct use cases for registered verifiers. One case involves registered verifiers such as financial police, the Ministry of Labour, depending on national regulations, who can request credential sharing from holder. In contrast, another scenario features single entities like construction site owners, responsible for ensuring the legality of activities on their sites. They may only need to verify the validity of a PD A1 without requiring additional personal information. Due to the possible impracticality of qualifying all construction site owners in Europe, we introduced "unregistered" verifiers as actors in the process.

User journeys are defined for the "unregistered" category, and this is closely related to a minimal dataset that can be shared with unregistered verifiers, excluding personal data but triggering the disclosure of specific information. For example, the disclosure of a valid PD A1 for a limited period is sufficient for assessing credential validity.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

6.3 Non-core Use Case Interactions

While they may not be critical for the initial release of the social security pilot, there exists a set of use cases that we've classified as non-core. These components, though not immediately vital, harbour considerable value for the pilot's progressive evolution. Strategically integrating these elements in future iterations will be key to expanding the pilot's ambit and enriching its functional capabilities, thereby propelling it beyond its initial scope and laying the groundwork for a more comprehensive application.

6.3.1 Delegation of a Credential

In the context of credential delegation from holder to a third party, e.g., between wallets, there are various potential requirements and methods to consider, and the most practical approach must be assessed. There are two primary scenarios. For instance, in the EHIC context, a parent may wish to transfer their child's EHIC to their wallet. This transfer can be achieved through a request-based issuing process thus triggering a "delegation" process from holder. These scenarios offer multiple transfer methods, necessitating careful examination. It's particularly crucial in the eIDAS context where a strong link to the ID or wallet exists, as transferring to another device could invalidate the credential. This challenge revolves around managing the identity aspect and the credential aspect separately, but it is vital to address given the significance of transfer use cases. Additional scenarios require consideration of revocation of transferred credentials, or time limited transfer. An illustrative example could be a child who wants to join a travel group or a friend's family on a vacation. In such a case it could be necessary to transfer the EHIC to the wallet of a supervisor only for the time of vacation.

6.3.2 Self-verification of Credentials

This use case scenario for citizens revolves around wallet capabilities that enable them to check the status of their credentials within their wallets or the status of credentials when being transferred into the wallet from the issuer. An essential aspect here is the self-verification of these credentials, constituting a key component of the wallet user journey. This self-verification addresses the question of how citizens can confirm the validity of their credentials within the wallet system. Moreover, self-verification and self-presentation of data are closely intertwined with the verification of credentials, which represents a previously described use case scenario. In any case, this self-verification will take place upon receiving a VC to check validity before saving a VC in the wallet.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

6.3.3 Proof of Verification

A verification proof mechanism that can be forwarded to a back office, serving as evidence of the verification process, is a critical aspect for both EHIC and PD A1 use cases. Until now, the need for documenting the verification process hasn't been addressed, particularly in the case of EHIC. Healthcare providers need to document their verification of EHIC, which they use to determine the kind of information required for service reimbursement to citizens. This documentation then falls under the jurisdiction of the Creditor State, which sends it to the Debtor State and is closely tied to the reimbursement process. Similarly, in PD A1, qualified verifiers require information in their back offices to investigate potential frauds and errors, possibly involving checks on the citizen's employer. Therefore, there's a need for a mechanism to transfer verification proofs from enterprise wallet to backend systems. The challenge lies in defining an exchange protocol between enterprise wallet and verifier backend that specifies the dataset required to be included into the proof of verification as this dataset will vary depending on the verifier institution legal requirements.

6.4 Use case 1: Issuance of a Personal Verifiable Credential in Social Security

In the issuing process, there are two key roles: the issuer and the citizen. The process begins (see Figure 10 – Issuance workflow) when the Enterprise Wallet receives a request from an Authentic Source that includes the attributes required for the creation of a credential based on the applicable schema, as well as holder identification reference (DID). The Enterprise Wallet, operated by the Authentic source or by a (Q)TSP acting on its behalf, creates a legally binding Verifiable Credential (EEA) encapsulating within it the attributes alongside an eIDAS compliant e-seal.[2]

[2] "Authentic source" refers to entities providing the necessary data. They may be the same as the issuer or distinct roles. For example, in social security, some service providers issue credentials on behalf of multiple authentic sources. However, the authentic source can also be the issuer themselves.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

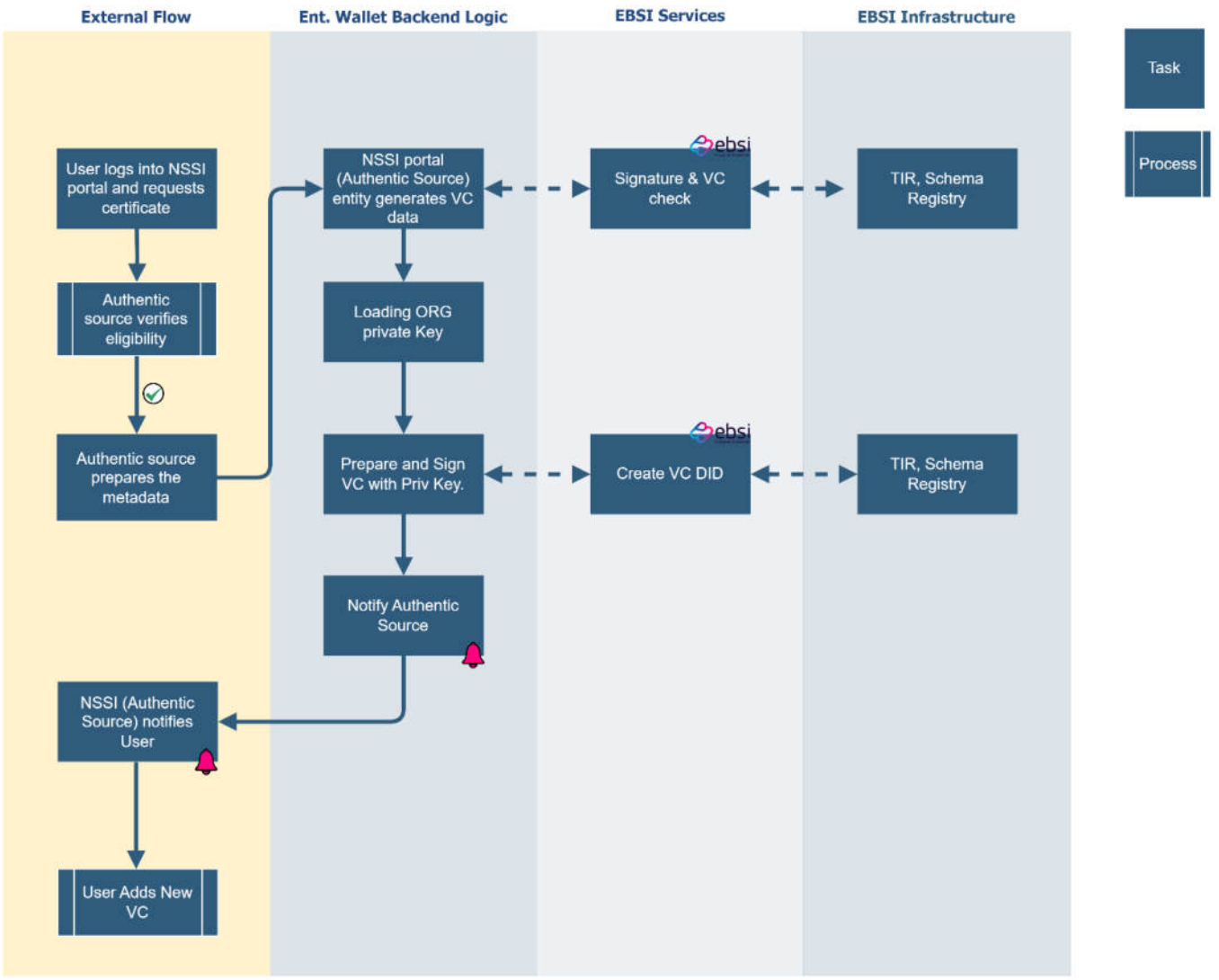


Figure 10 - Issuance workflow

6.4.1 The Process

6.4.1.1 (Issuer side) Request Reception

National processes for credential requests vary, therefore, to be able to define a generally applicable process, the workflow we envision starts when requests/applications are successfully

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

processed, triggered by a positive response from the relevant institution. This initiation icon into the flow in Figure 10, marks the beginning of the user journey.

1) The Enterprise Wallet receives a request, containing all attributes required by the applicable schema, from the Authentic Source's backend, triggering the process of generating a credential for an individual, specifying the necessary attributes for identity mapping. Currently, the use of the related EBSI DID is envisioned, but in the future any other relevant method of secure authentication could be implemented, particularly the possibility of leveraging the PID for regulatory compliance;
2) The Enterprise Wallet processes this request, generating a Verifiable Attestation/Credential, where:
    a. the Credential Type is linked to the applicable schema type and its unique identifier present into the EBSI Trust Registry;
    b. the Credential Subject is linked to the holder's necessary identity attributes, and data are retained for future issuance;
    c. The Credential Issuer is linked to the DID of the Authentic Source;
    d. The Claim related to this credential includes all the Attributes defined by the Authentic Source;
    e. The Validity Period is set as per received request.

The Proof is based on the Authentic Source's Private Key. Subsequently, the Enterprise Wallet initiates a notification protocol to inform the citizen regarding the successful preparation of the credential (the notification method detail is not in scope of this document). The responsibility for notifying citizens falls on national authorities[3] as this is the entity the holder or its representative relates to initiate the request. Bases on this assumption, the notification system currently envisioned by WP5 unfolds through the Authentic Source, following the triggering of the notification protocol by the Enterprise Wallet. The Enterprise Wallet will need to provide a specific and wallet-compliant process that allows only the holder to securely download the credential (e.g., requesting the holder to proof the ownership of the private key corresponding to the one referenced into the Credential Subject through the DID).

[3] In public services, a close collaboration between issuers and authentic sources is common. Many social security institutions have their notification systems or platforms. Different methods and structures are in place, but they all rely on communication between the authentic source and the issuer to activate notification systems.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

A suitable alternative to this notification process could be influenced by the future capabilities of the Enterprise Wallet to directly notify the citizen, a topic still under discussion within Work Package 3 of the EBSI-VECTOR project.

Regarding revocation, for security purposes and as not all Member States define the same process, it would be required, for the authentic source to provide, together with other data, the DID/DIDs of the entity authorized to revoke or more generically change the state of the issued credential. If the Authentic Source is the only allowed to perform this task (as in many member states), the DID provided will be its own DID. This list can be maintained within Enterprise Wallet's log or otherwise stored securely into EBSI Trust Layer (e.g., encrypting each entry with the public key of the Authentic Source). Independently from this list, judicial authorities will always be able to perform such change.

6.4.1.2 (Citizen side) Notification Receival

- The citizen enters the process when they receive a notification from a known notification service, informing them that requested credential is available for download.
- This notification may take the form of an informative message that includes a direct link to the download service. Alternatively, in some solutions, the notification seamlessly integrates with the download service itself.
- Upon receiving the notification, the citizen proceeds to select the provided link, which activates the EBSI compliant wallet and directs it to the designated download service, initiating the process of credential retrieval.

6.4.1.3 Credential Provision, Download and Holder Identification

- Upon successful processing, the Enterprise Wallet offers a secure link for the user to conveniently download their credential.
- The download is triggered by the holder's wallet based on the received notification to download the Verifiable Credential from the Enterprise Wallet.
- To be able to securely prove that the requesting wallet is in control of the holder, proof of ownership of the private key related to the Credential Subject DID will be required to gain access to the download service for that specific credential.

It's worth noting that in the new incoming eIDAS 2.0 European regulation, the authentication level is set at a high assurance level, where the authentication will be guaranteed through the PID [10]. While some platforms may opt for a substantial assurance level, the specific choice often

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

depends on national considerations. One of the main topics discussed and analysed inside this Work Package is the chance to additionally rely on lower (substantial) level of assurance, an option made available using the EBSI infrastructure or to link the new EU PID to an EBSI-compliant DID.

It is essential to note that the EBSI-compliant wallet through DID (Decentralized Identifier) management enables the binding of the credential to the individual's identity. The appropriate verification of both the identity and its associated DID is a task that must be performed by the Authentic source prior of enabling the entire request flow described in paragraph 6.4.1.1. A proper and secure identity verification from the Authentic source is a fundamental business requirement within this process.

6.4.1.4 (Citizen side) Credential Storage Process

- The EBSI-compliant Wallet, after successful authentication and download, examines the received credential, conducting verification tests, to ensure for example, issuer trust, schema compliance, and the satisfaction of all associated constraints.
- Once the Wallet successfully completes these credential's tests, the citizen is presented with the option to accept or not the storage of the credential within his EBSI-compliant Wallet.
- Upon citizen consent, the credential is securely stored within the EBSI-compliant Wallet storage area, allowing therefore its use for future and verification.

6.5 Use Case 2: Revocation of a Credential

The process for revoking digital credentials is a crucial functionality. This transition to a digitalized system represents a significant leap forward from traditional paper-based processes.

Given the diverse national requirements across Member States, this subsection proposes two adaptable revocation processes. These processes are designed to be flexible, allowing for either independent use or a combined "hybrid" approach at the discretion of each Member State. While this flexibility may introduce complexities in standardizing the revocation process at the European level, it is essential to weigh the benefits and drawbacks of each option.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

In this section, we will detail the general functional and non-functional requirements for the revocation process aiming to provide a baseline framework. This approach is intended to facilitate the harmonious integration of these processes across different national systems. We anticipate that this section will catalyse discussion and exploration among various stakeholders, including relevant Work Packages, the EBSI team, and other parties involved. The objective is to encourage the consideration of innovative approaches and solutions to effectively manage and refine the revocation mechanism, addressing its complexities and ensuring its efficacy in the long-term.

The revocation process we are aiming for must adhere to GDPR, prevent holder traceability, respect holder privacy, and avoid storing or processing personal data on the EBSI blockchain, while also preventing issuers or third parties from linking revocation checks with the holders.

Option 1: Current EBSI revocation process

When an issuer creates a new VC, its status – whether it is valid, suspended, or revoked – is included. This status is shared with the citizen and any verifying organizations. It is also linked to a "Credential Status" VC that reports the VC's validity, which the issuer updates. EBSI serves as an intermediary between the verifier and the issuer who hosts the Credential Status VC. The contact details of the organization that issued the VC and possesses its status information are publicly accessible through EBSI's Trusted Issuers Registry.

The issuers, which are frequently public legal entities, have information that may be disclosed publicly, and their VCs are exempt from GDPR regulations. As a result, the status of an issuer's VC can be maintained and managed within the Trusted Issuers Registry on EBSI's ledger.

The EBSI solution offers two approaches for managing accreditation status information. The first approach involves storing this information directly in the EBSI Trusted Issuers Registry. In this scenario, a verifying organization can directly access the accreditation status from the Registry, which acts as a mediator between the issuer and verifier. This method relieves the Issuer from the responsibility of storing and managing the accreditation status information. The second approach, instead, allows the issuer of the VC to retain control over the accreditation status information. Here, the issuer hosts this information and makes it accessible via the EBSI Trusted Issuers Registry. This method is beneficial for issuers who have pre-existing systems for managing accreditation status and want to integrate them with the EBSI platform.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

However, legal implications of these registries in certain national context, such as Italy, warrant careful consideration. In such jurisdictions, these registries could be perceived akin to "public blacklists", raising privacy concerns. This perception stems from the potential to easily identify owners of credentials and the specific status of revoked credentials. Such transparency, while beneficial, might clash with national privacy laws around data confidentiality and individual privacy rights.

This scenario highlights the delicate balance between the need for transparency and accountability, and the need to protect personal and sensitive information – especially in regions with stringent privacy regulations and expectations.

Option 2: Revocation managed by the Enterprise Wallet

In this scenario, the issuer modifies the credential's status because of a business decision, leading to its revocation. To enact this, the issuer sends a revocation request to the Enterprise Wallet. Upon receiving this request, the Enterprise Wallet takes action to invalidate the credential. It then communicates with the holder's Wallet, notifying it of the revocation rights and subsequently restricting the sharing of this credential.

However, this process presents certain challenges, primarily due to the need for specific functionalities in the holder's wallet, which are beyond our control. This limitation becomes particularly pertinent when considering the transfer of credentials between wallets, such as moving a credential from one personal wallet to another. A key question arises: how do we ensure effective communication between different wallets to acknowledge and reflect the revocation of a credential? Addressing this issue requires a standardized protocol or mechanism across various wallet platforms, ensuring that all wallets recognize and respect the revocation status initiated by the issuer – which falls beyond the scope of our tasks in WP5 and of EBSI-VECTOR.

6.5.1 The Process

6.5.1.1 (Issuer side) Demand Reception

- The Enterprise Wallet receives a request, complete with necessary attributes, such as the DID of the credential and the holder, from the authentic source. This request indicates the need to revoke a previously issued credential to an individual.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- Upon receipt of this request, the Enterprise Wallet confirms that the requesting authentic source's DID matches the list of entities authorized for revocations. This verification may utilize the EBSI Trust layer, as outlined in the issuing process.
- There are then two potential courses of action following this verification:
    - Option 1: The Enterprise Wallet processes the revocation request through the current revocation process established by EBSI.
    - Option 2: The Enterprise Wallet issues a "Revocation Verifiable Credential", specifying the "Credential Type" accordingly.
- After deciding on the course of action, the Enterprise Wallet then engages a notification protocol, similar to the one used during the issuing process, to complete the revocation procedure.

6.5.1.2 (Citizen side) Notification Handling

The citizen's involvement in the process begins when they receive a notification from the notification service. This notification can take two forms:

- Option A: The notification explicitly informs the user about the revocation, including the details of the revocation event. In this scenario, an EBSI-compliant wallet can process these details, enabling the user to view the specifics of the revocation directly within their wallet.
- Option B: The notification acts as a prompt for the EBSI-compliant wallet, triggering it to respond as it would to any incoming Verifiable Credential. This means the wallet will automatically update to reflect the revocation, without necessarily providing the detailed context of the revocation to the user.

6.5.1.3 (Citizen side) Self verification & revocation (valid for Option 2)

The final step in this process is for the citizen's EBSI-compliant wallet to self-verify the revocation request. When the wallet receives a notification about the change, it examines the details of the VC. It checks whether the DID of the issuing entity matches one of the authorized revocation DIDs associated with the VC.

If the revocation conditions are verified successfully, the EBSI-compliant wallet will then restrict the holder's ability to share, present, or manage the revoked credential. Since a credential can be revoked effective from a specific date but remain valid for processes conducted prior to that date, this method ensures the anonymity of the revocation process, safeguarding the holder's privacy rights without the need for public disclosure in an external registry or list.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

In situations where verification is required, the revocation status of a credential is crucial. Verifiers can check the credential's current status to confirm its validity and ensure it has not been revoked.

The process includes a mechanism for the authentic source to send a notification to the citizen, informing them of changes to their credential. While the national authorities[4] are responsible for notifying citizens of such changes, the Enterprise Wallet itself does not bear this responsibility. It is the authentic source that is prompted by the system to deliver these notifications to the citizens.

6.6 Use Case 3: Verification

6.6.1 The Process – Verification

6.6.1.1 (Citizen side) Using Verifiable Presentation

A citizen, holder of an EBSI-compliant wallet, when required to share a Verifiable Credential due to a verifier's request or by their own choice, can perform several actions:

- Minimize the set of data shared with a verifier. This is possible only if the credential is appropriately structured to allow such minimization;
- Generate a multi-credential presentation that combines different VCs into a single, secure certification. This could be useful, for example, when an authorized verifier asks for multiple documents, and the Wallet automatically compiles the requested VCs in response to the request;
- Create a singular proof from an entire VC. For example, they can create a Verifiable Presentation that confirms the possession of a valid certificate (EHIC/PD A1) without revealing specific details of the certificate;
- Develop a Verifiable Presentation that offers additional protection for the user. This includes creating presentations that a verifier can use or verify only once within a specified time frame.

[4] In public services, a close collaboration between issuers and authentic sources is common. Many social security institutions have their notification systems or platforms. Different methods and structures are in place, but they all rely on communication between the authentic source and the issuer to activate notification systems.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

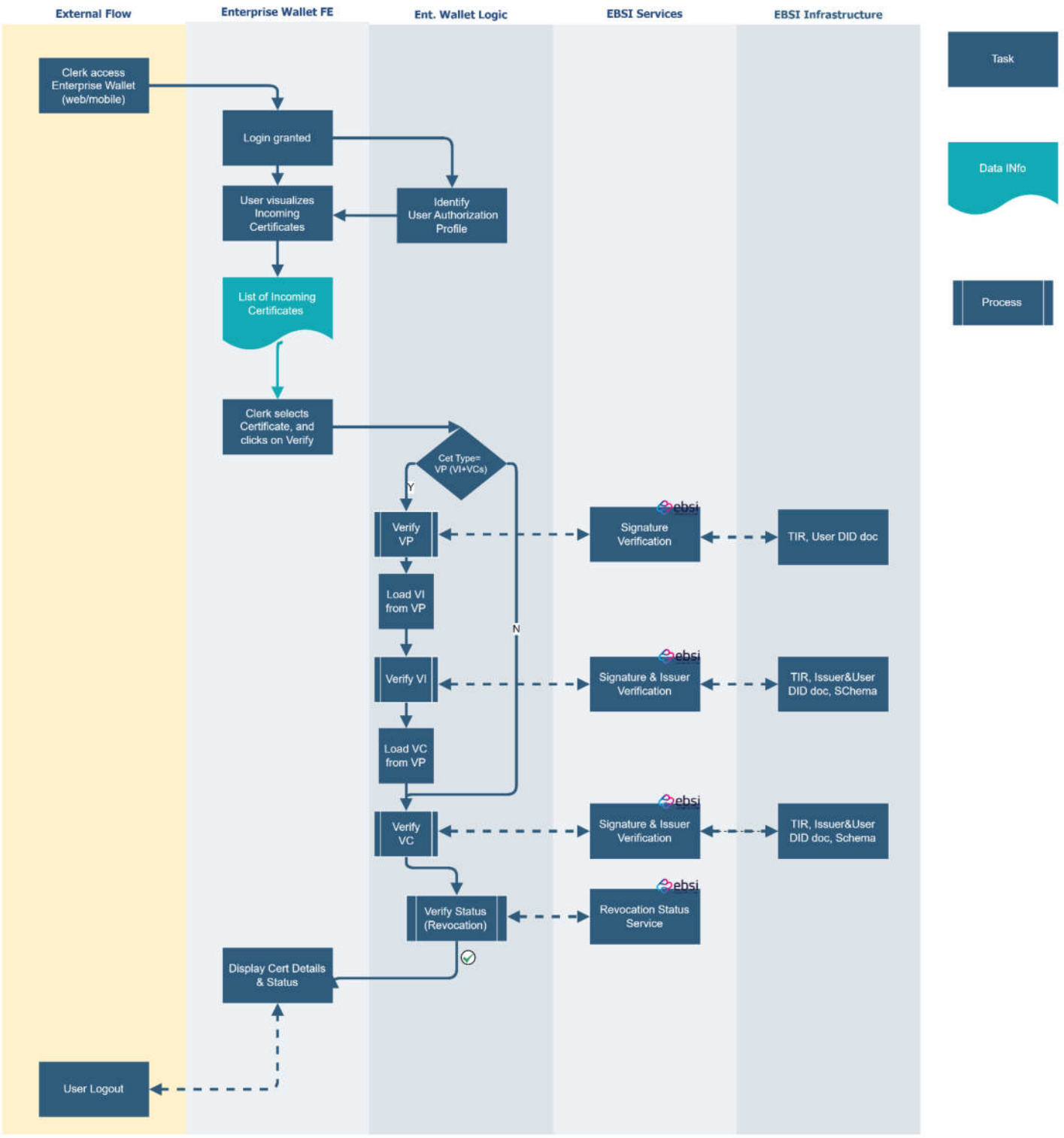


Figure 11 - Verification flow

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

6.6.2 User Journey

6.6.2.1 (Citizen side) The citizen meets a verifier

- The citizen is temporarily staying (or pursuing work) outside the competent Member State.
- The citizen is required to provide an attestation of social security attributes.
- The citizen needs to establish their status as the legitimate holder of this attestation (identity proof).

6.6.2.2 (Verifier side) The verifier requests information

- The verifier initiates contact with the citizen and launches its organization's verification application;
- The Enterprise Wallet, based on such request, issues a request to the holder's wallet, identifying within the request the Verifier, through its DID;
- In the case of the EHIC, the authorized entity may be a hospital or healthcare provider, whereas for the PD A1 scenario, it could be an inspection officer.

6.6.2.3 (Citizen side) The citizen receives the request

- The citizen receives a request to provide their social security attestation;
- The citizen's EBSI-compliant Wallet assesses the verifier's credentials and eligibility to handle the social security attestation.

6.6.2.4 (Citizen side) The citizen gives consent

- The citizen's EBSI-compliant wallet, providing all above details, requests consent for the requested actions.
- The citizen accepts the requests made by the verifier.
- The citizen's EBSI-compliant wallet then presents the required credential as requested.
    - When dealing with an Authorized Verifier, the citizen must supply all necessary information, and their wallet will automatically restrict the data shared to this specific subset.
    - If the verifier is not an Authorized Verifier, the citizen has the discretion to select which data to disclose. To simplify this process, there could be three predefined

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

profiles, such as offering maximum data minimization, moderate minimization, or no minimization.

- Concurrently, the EBSI-compliant wallet logs and documents all activities.

6.6.2.5 (Verifier side) The verifier checks the information

- The Enterprise Wallet of the verifier retrieves the Verifiable Presentation (VP) from the user's EBSI-compliant wallet and transfers the data to the verifier's backend system.
- The verifier's backend system examines the presentation received from the EBSI-compliant wallet.

In instances where manual verification initiates the process, the verifier's app will show the results of the identity verification from the Verifiable Presentation

6.6.3 Verification by Unregistered Verifiers (Sharing of Credentials)

Verifiable Credentials and Verifiable Attestations can be either shared or presented to a third party, or they can be "encapsulated" within a Verifiable Presentation. A Verifiable Presentation can consolidate data from multiple Verifiable Credentials (such as linking a Verifiable Identity with a Verifiable Credential) and may contain additional arbitrary data (for example, usage limitation constraints).

Verifiable Presentations are also very useful in the context of data minimization, following the principle of Selective Disclosure or Zero Knowledge Proofs. Zero-knowledge proofs are cryptographic methods which enable a user to prove knowledge of a value without disclosing the actual value. Furthermore, when creating a Verifiable Presentation, a new DID is generated, minimizing the possibility of tracking a specific Verifiable Credential when reused.

A possible workflow describing this process is depicted in the figure below:

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

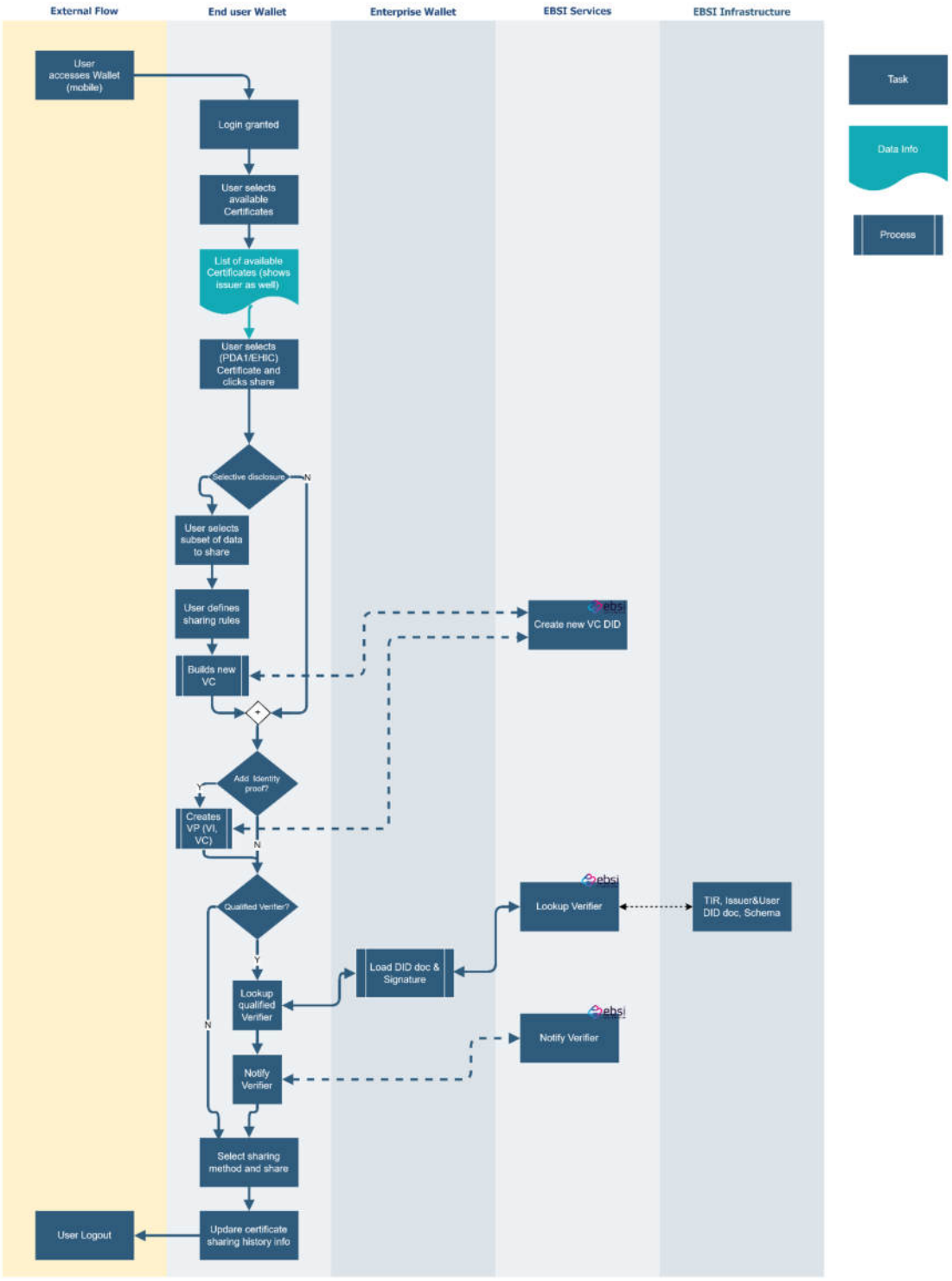


Figure 12 - Unqualified verification flow

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

7 Data Model for EHIC and PD A1 credentials

This chapter provides an overview of the data models for both the European Health Insurance Card (EHIC) and the Portable Document A1 (PD A1) credentials, detailing their current development stages and key data elements. These models are being crafted with a strong emphasis on privacy, data minimization, and authenticity verification. The chapter is divided into two sections.

The first focuses on the EHIC credentials, outlining the mandatory and optional data fields that align with the existing legal frameworks and technical specifications of the physical EHIC card. With this exercise, we expect that the digital version of the EHIC accurately reflect the legal and technical necessities of its tangible counterpart.

The second part of the chapter delves into the PD A1 credential, highlighting the essential personal, business, employer, and issuer data required. This section emphases the development of a user-centric framework that adheres to the principles of data minimization, privacy, and self-sovereignty. By providing a detailed explanation of these data models, this chapter aims to elucidate the intricacies involved in developing digital credentials that are both secure and compliant with regulatory standards.

7.1 Data Model for EHIC credentials

The data model for EHIC that is currently being developed is in an iterative phase. Upon its completion, the design will be grounded in the principles of data minimization and privacy. Moreover, it will incorporate personal data in a manner that enhances the verification process to ensure the authenticity of the holder's association. For now, it is clear that the essential data to be included in the EHIC Verifiable Credential will align with the existing legal framework, which sets out the technical specifications for the physical EHIC card. This approach ensures that the digital credential mirrors the legal and technical requirements of its physical counterpart.

Therefore, for the EHIC, the maximum set of data to be inserted into the Verifiable Credentials are the following (for each data field it is indicated if it is mandatory or optional):

- **Personal Data**
  - Surname and forename of the card holder *(mandatory)*

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- Personal identification number of the card holder *(mandatory)*
- Date of birth of the card holder *(mandatory)*

- **Business data**
  - Valid from (date) *(mandatory)*
  - Valid to (date) *(mandatory)*

- **Data of the Issuer**
  - ISO 3166-1 numeric code of the member state issuing the card *(mandatory)*
  - Identification number of the competent institution issuing the card *(mandatory)*
  - Logical number of the card according to EN 1867 of 1997 *(optional)*

7.2 Data Model for PD A1 credentials

The PD A1 data model, which is under active development, is currently in a progressive stage of refinement. When finalized, it will be firmly rooted in the principles of data minimization, privacy, and self-sovereignty to ensure a robust and user-centric framework. Moreover, it will incorporate personal data in a manner that enhances the verification process to ensure the authenticity of the holder's association.

Based on the PD A1 form, the **maximum set of data** to insert into the Verifiable Credentials are the following (for each data field it is indicated if it is mandatory or optional):

- **Personal Data**
  - Personal details of the holder - worker's identification data including first name, surname, PIN, and date of birth *(mandatory)*

- **Business Data**
  - Member State whose legislation applies (mandatory)
  - Information about the duration of the activity (mandatory)

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- Start date of the decision *(mandatory)*
- End date of the decision *(optional)*
- The status confirmation of the worker's position *(mandatory)*

- **Employer Data**
  - Employer/self-employment details including Name, ID and Country *(mandatory)*
  - Employer/self-employment details where an activity is pursued including Name, ID and Country *(optional)*

- **Data of the Issuer**
  - Country and ID of the institution issuing the form *(mandatory)*

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

8 Definition of Onboarding Business Process for Institutions in the EHIC and PD A1 Use Cases

This chapter delves into the onboarding business process for institutions in the context of the European Health Insurance Card (EHIC) and the Portable Document A1 (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 Verifiable Credentials (VCs). It navigates through the complexities of integrating existing structures such as the EESSI Institution Repository (EESSI IR), the eIDAS 2.0 trust framework, and the EBSI trust framework 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 EBSI-VECTOR project.

8.1 Defining a Trust Framework

As a reliable basis for an appropriate use of Verifiable Credentials a “trust framework” needs to be designed and implemented. This 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, three main inputs are relevant: the EESSI Institution Repository, the eIDAS 2.0 trust framework, and the EBSI trust framework. They will be descripted in further detail below.

8.1.1 EESSI Institution Repository – a Trust Framework for Social Security

Social security is a highly regulated domain with clear responsibilities defined through normative mandates. For the “EESSI” system a repository for trusted actors has already been established – the **EESSI Institution Repository (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

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

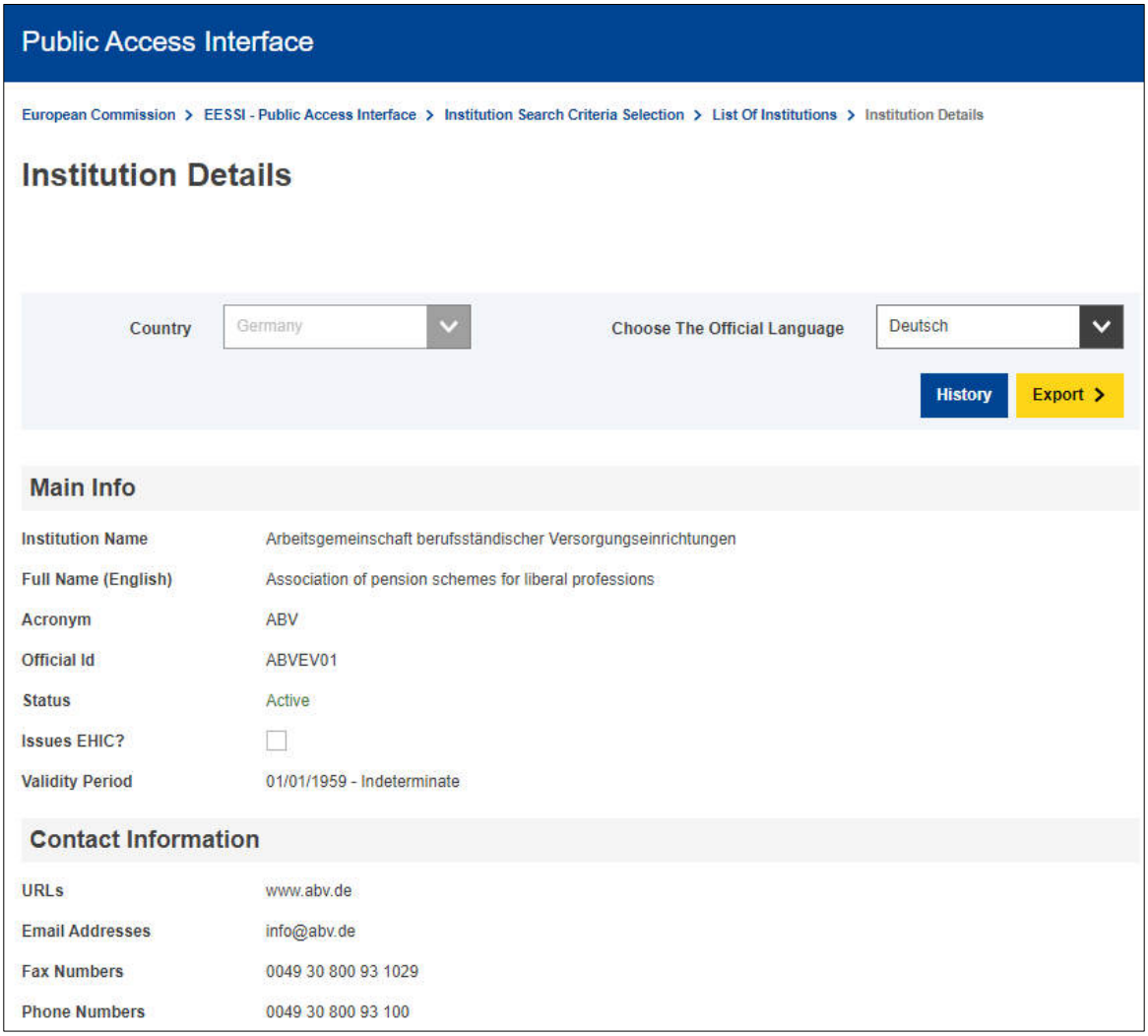


Figure 13 - The EESSI Institution Repository [12]

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 authorized 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.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Type Of Benefits	Functions	Portable Documents	Category Of Social Security	General Comments

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 14 - The EESSI Institution Repository – Public Access Interface for SVS – Issuer of Portable Documents. [12]

In the event of a merger involving two or more institutions, it is mandatory to inform the European Commission about the significant change one month prior to the merger. Subsequently, this merger must be recorded in the IR.

Along with notifying the European Commission about the closure, it is also required to designate a successor institution that will assume the responsibilities of the institution being closed.

All updates and changes in the IR are handled by the IR-SPOC.

The Institution Repository needs to be integrated/mapped/transferred into the new ecosystem developed by EBSI-VECTOR. Achieving the project objectives requires this integration to take into account two key factors:

- Firstly, adherence to the eIDAS 2.0 regulation, as compliance is essential;
- Secondly, alignment with the EBSI trust framework.

8.1.2 EIDAS 2.0 Trust Framework

The ecosystem and trust framework of the European Digital Identity Wallet (based on eIDAS 2.0 and ARF) consists of the following roles on the credential issuer side (see ARF definitions):

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- **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 EUDI Wallet there may be multiple providers for PID and (Q)EAA";
- **Attestation Provider**: "It means any provider that is able to issue an attestation, it includes PID Provider EAA and QEAA provider";
- **National Accreditation Bodies (NAB)**: "National Accreditation Bodies (NAB) under Regulation (EC) No 765/2008 are the bodies in Member States that perform accreditation with authority derived from the State".
- **Supervisory Bodies**: "The supervisory bodies are notified to the Commission by the Member States, which supervise QTSPs and act, if necessary, in relation to non-qualified Trust Service Providers". [10]

All in all, Attestation Providers, also referred to as Issuers, issue attestations on behalf of authentic sources based on their authorisation by National Accreditation Bodies (thus creating a "Trust Chain"). All those actors are overseen by Supervisory Bodies. Attestation Providers/Issuers and Authentic Sources could be the same entity.

Those roles interact with other actors in the trust ecosystem which are not in focus here – like Trusted List Providers, PID Providers and Wallet Providers. Besides that, it is important to mention that in the credential issuing process the issuing institution is also a Relying Party (also known as "Verifier") – 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". [13]

The extent to which this impacts a distinct or a unified approach for Issuers and Verifiers Trusted Lists needs to be examined.

In any case, the Credential Issuers 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 issuer. This authorisation should not only cover the fact that an institution is allowed to issue a credential – it should also state that

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

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" (Art. 45da). [10]

The different eIDAS roles, levels, authorisations, and the relations towards each other must be covered by an EBSI-VECTOR solution.

8.1.3 EBSI Trust Framework

In its current state, EBSI offers a trust framework which contains roles like Trusted Issuers (TI) and Trusted Accreditation Organisations (TAO), based on a decentralised Trusted Issuer Registry (TIR):

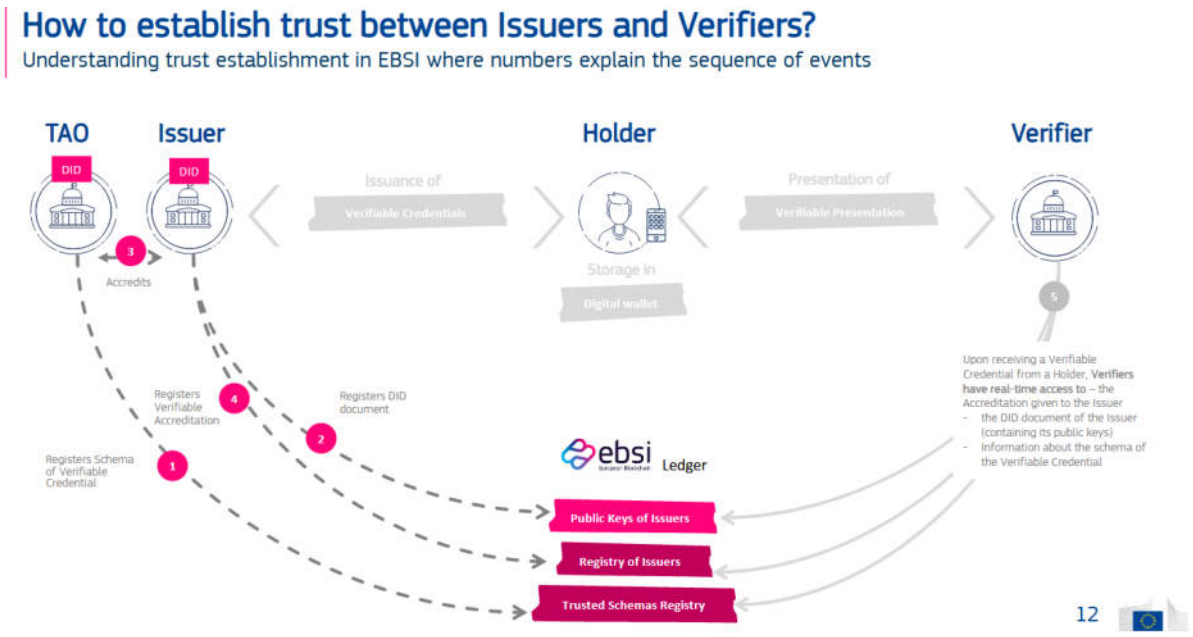


Figure 15 - EBSI Trust Framework [14]

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

In order for the Issuer to support the core business processes highlighted in this document[5], a fundamental requirement is for the Trusted Issuer to be officially recognized within the Trusted Issuers Registry. This registration ensures the legitimacy and trustworthiness of the Issuer within the EBSI ecosystem.

8.1.3.1 Registering Trusted Issuers onto EBSI

EBSI establishes a framework for two primary types of Decentralized Identifiers (DIDs) to accommodate the main participants in the system:

- **Legal Entities (Issuer, Verifier)**:
    - These DIDs are composed of the prefix 'did:ebsi' followed by a sequence of 16 randomly generated bytes.
    - The DIDs for Legal Entities are catalogued within EBSI's records and linked to a corresponding DID-Document, a critical component for ensuring secure and authenticated transactions within the EBSI ecosystem.

- **Natural Person (Wallet users):**
    - DIDs for individual users are structured with the 'did:key' prefix and a public key. This public key is generated using the Elliptic Curve NIST P256 algorithm and is encoded as a base58 string.
    - These user-specific DIDs are not recorded in EBSI's registers. They offer flexibility as they can be replaced with a new DID, generated in the same manner, to meet the evolving needs or preferences of the user.

This two-tiered DID approach within EBSI ensures that both legal entities and individual users have secure, yet adaptable, identifiers suitable for their distinct roles and interactions within the blockchain infrastructure.

[5] The Issuer must possess capabilities including:
- Retrieving EBSI schema using a unique identifier;
- Digitally signing Verifiable Credentials (VCs);
- Revoking issued VCs when necessary;
- Providing information on the revocation status of any VC.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

8.1.3.2 Legal Entity Onboarding

The process of incorporating both legal entities and individuals into the EBSI system presents distinct differences:

1) **DID Method and Identifier Specification:**

One key variation lies in the EBSI DID Method which outlines the prerequisites for the registration of Trusted Issuers on EBSI. This requirement is essential for legal entities as it establishes their credibility and trustworthiness within the EBSI framework.

2) **DID and DID Document Registration**:

Legal entities are required to register their specific DID and the accompanying DID Document within the EBSI's DID registry. This process is crucial whether the entity functions as an Issuer or a Verifier.

The onboarding of a Legal Entity is methodical and involves specific steps to ensure accurate registration and proper integration into the EBSI ecosystem. A comprehensive diagram depicting this onboarding process provides an overarching view of the necessary steps and considerations involved.

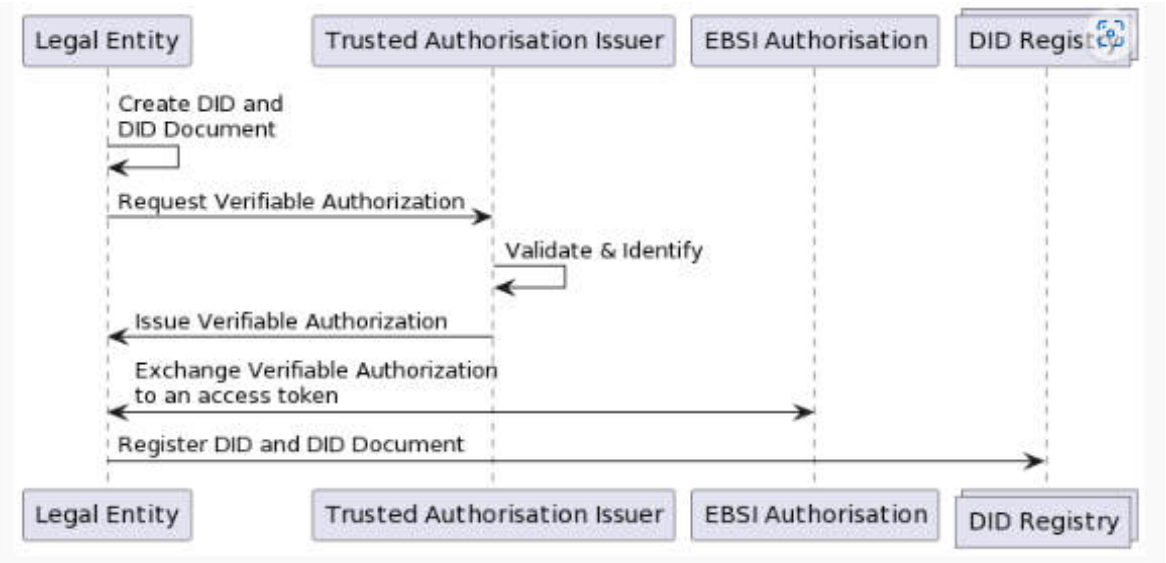


Figure 16 - Legal Entity Onboarding

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

The initial onboarding is a critical and obligatory step that must precede any other activity within the system. This foundational phase culminates in the registration of a Decentralized Identifier (DID) and the acquisition of a verifiable, non-transferable authorization. This initial step ensures that all subsequent interactions and transactions within the system are grounded in a verified and secure framework, establishing a solid foundation for reliable and trusted operations.

8.1.3.3 Accrediting Legal Entity

Legal Entities within the system are categorized into two distinct types, higher-level legal entities or sub-level legal entities. For example, in the Italian context a high-level legal entity could be considered as the Ministry of Health for the EHIC or the Ministry of Labor for the PD A1. A sub-level legal entity, in the same context, could be the INPS (The Italian National Institute for Social Security), that is mandated by law to issue Verifiable Credentials.

1) Higher-Level Legal Entity

As a Trusted Entity, specifically a Reliable Accreditation Issuer, this category operates distinctively due to its elevated status.
It is self-declared, meaning that after registration in the Trusted Issuers Registry (TIR), the entity autonomously declares itself as a Trusted Accreditation Issuer for the attributes specified in its Verifiable Authorization.
The process culminates in the registration within the TIR and the acquisition of a disposable Verifiable Accreditation.
Post-registration, the necessity for the Verifiable Accreditation diminishes as its details are securely stored in the TIR, ensuring a streamlined process for higher level legal entities.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

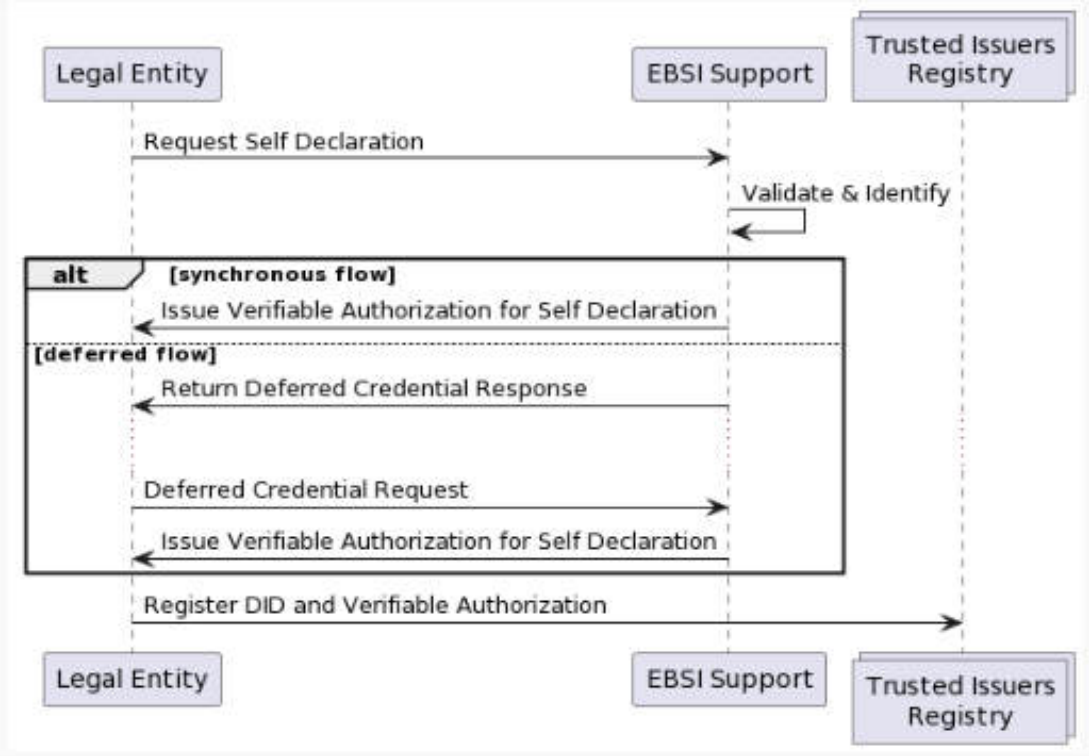


Figure 17 - Higher level Legal Entity Accreditation

2) Sub-Level Legal Entities

These entities can possess a range of accreditations, either from the same or different higher-level legal entities.

Following their registration in the Trusted Issuers Registry (TIR), each new accreditation aligns with the types outlined in the previously provided accreditation documentation.

The process leads to a streamlined TIR registration, accompanied by the acquisition of a disposable Verifiable Accreditation.

Once the registration is complete, the need for retaining the original Verifiable Accreditation is negated, as its information is securely maintained within the TIR. This ensures an efficient and organized approach for sub-level legal entities managing multiple accreditations.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

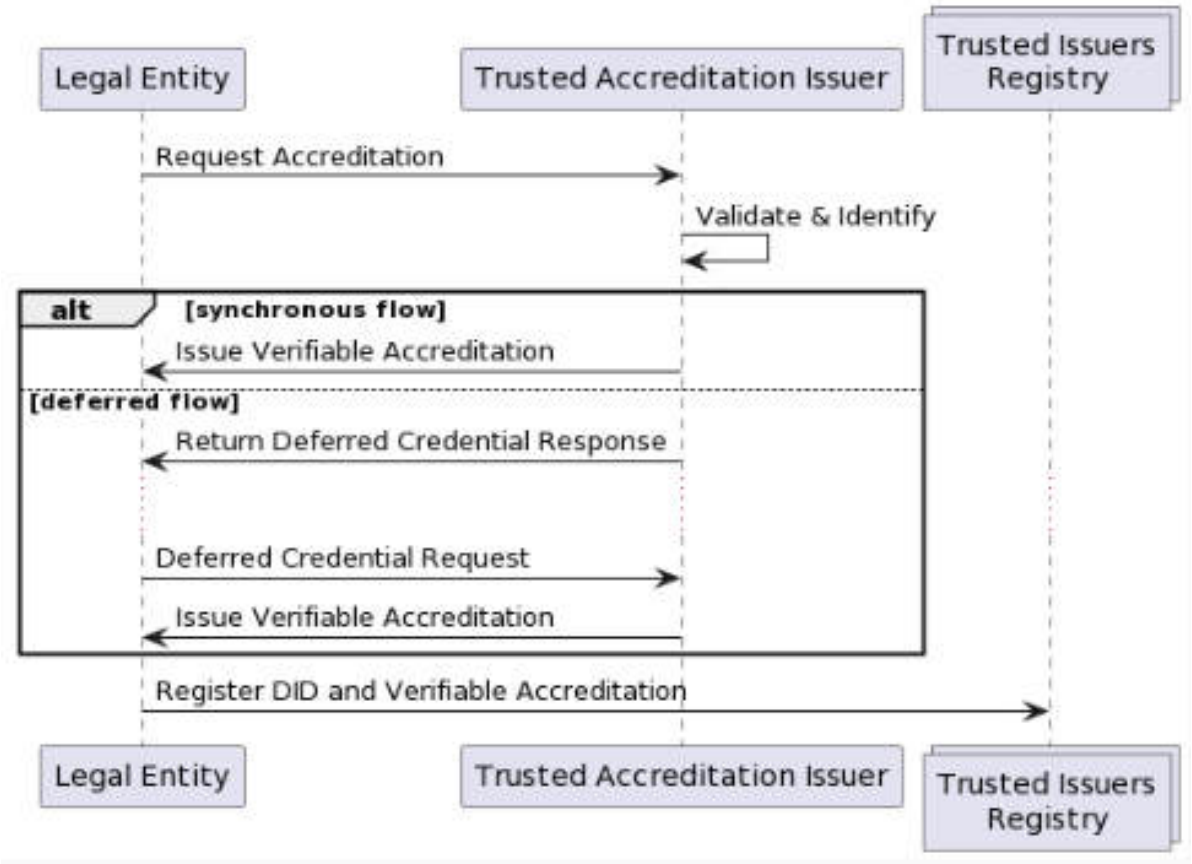


Figure 18 - Sub-level Legal Entity Accreditation

8.1.3.4 Leveraging the EBSI-Framework for Credential Issuance and Signing

To begin issuing Verifiable Credentials, an entity must first achieve "Trusted Issuer" status by registering with EBSI. This crucial step authenticates the issuer's authority and legitimizes the signature affixed to any issued credentials.

Post-registration, issuers are required to configure their credential issuing applications. This involves setting up a secure environment on the server where a public and private key pair is stored. These keys, essential for signing Verifiable Credentials (VCs), are securely housed in a cryptographic wallet, namely the Enterprise Wallet.

The application, the Enterprise Wallet in this project, utilized for issuing must be integrated with the Decentralized Identifier (DID) Protocol, version 1, specifically tailored for legal entities such

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

as issuers. A critical component of this integration is the inclusion of the DID Document, which houses essential verification details like the issuer's public keys.

Upon successful accreditation, other entities within the EBSI ecosystem can confidently validate the existence and credentials of the issuer. This ensures that the VCs issued by the accredited entity are recognized and can undergo the verification process seamlessly.

8.1.3.5 Preconditions for Credential Issuance

The Issuer is required to have systems in place for issuing Verifiable Credentials (VCs). These systems must adhere to the security protocols and guidelines specified in the eIDAS and GDPR frameworks. Furthermore, the component responsible for creating the Enterprise Wallet, used by the trusted Issuer, should be seamlessly integrated and accessible through the application designated for Issuer registration.
The platform administrator plays a critical role in managing the applications and the data associated with credential issuance. It's imperative that the administrator retains the capability to resolve them, especially in scenarios where security protocols are compromised.
For effective interaction with the EBSI, the Issuer must have access to the EU Login system. This is essential to generate the necessary access token, which enables the Issuer to utilize EBSI services effectively.

8.1.3.6 Specifications Overview

The process flow for the Issuer to execute operations within the EBSI Intake Scheme via ID and Verifiable Credential (VC) Signing is detailed as follows:

- The Issuer initiates the process by creating a Decentralized Identifier (DID) and its corresponding DID Document, adhering to the specifications laid out by EBSI.
- The Issuer then submits a request to EBSI for authorization to register this DID Document within the DID registry.
- Upon receiving authorization, the Issuer proceeds to register the DID Document on the DID registry.
- With the DID Document now registered, the Issuer's next step involves requesting authorization from EBSI to register the accreditation for issuing credentials.
- EBSI reviews this request and, if deemed appropriate, grants the Issuer authorization to register this accreditation on the registry.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

- The Issuer completes this phase by registering the accreditation for issuance in the registry. Post-registration, the Issuer is empowered to issue Verifiable Credentials and apply verifiable signatures to them, thus ensuring authenticity and integrity.

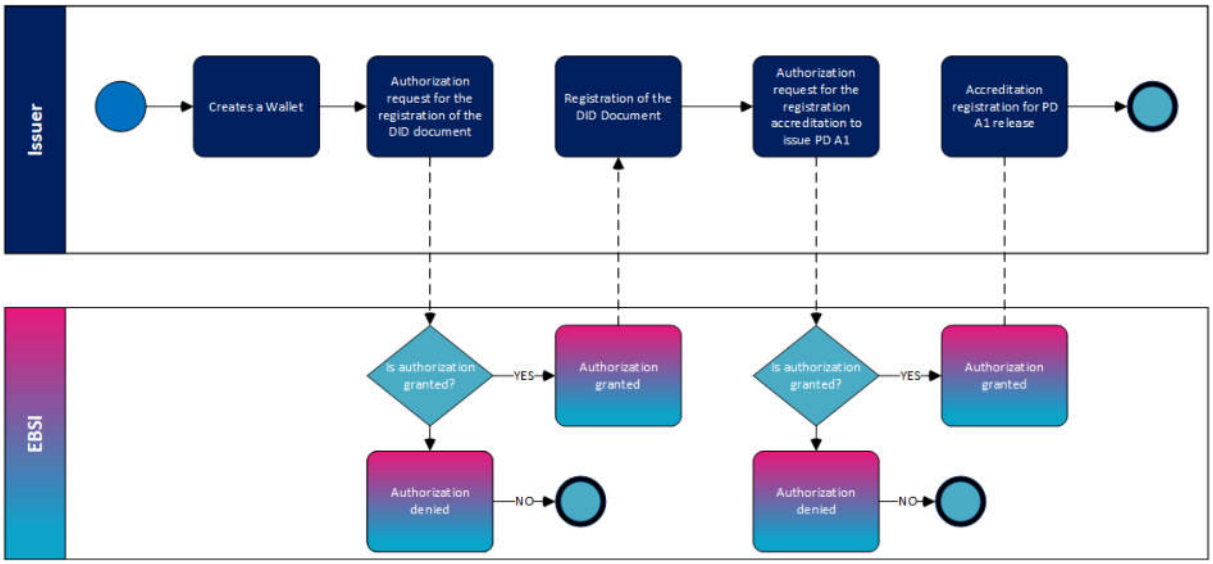


Figure 19 - Issuer Accreditation Process

8.1.3.7 Post-conditions

The Issuer gains the capability to distribute VCs accompanied by a trustworthy signature in a successful outcome, enabling other participants to verify and confirm the Issuer's accreditation for issuing these VCs and to authenticate the validity of the signatures. However, in error scenarios, there is a need for the establishment of detailed error information pages to address any failures in VC issuance. Additionally, should an error occur that hinders the Issuer's completion of registration, the Issuer must work closely with EBSI to resolve the issue.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

8.2 Implementation of the Trust Framework: Issuer Registry and Onboarding Service

Given the processes described in the previous section, two things are needed for the implementation of this trust framework:

- First, the definition and implementation of a corresponding Issuer Registry;
- Second, a capability of the Enterprise Wallet to execute onboarding procedures (via an "Onboarding Service").

The Onboarding Service has to realise the accreditation process, to create seals/private keys and to fill the Issuer Registry. The Issuer Registry needs to have a well-secured insert mechanism while being publicly readable.

The Issuer Registry must contain information on:

- Basic information about the Institution (Name, country etc., including ID/DID);
- Role in the Trust Chain (Accreditor/Accredited by etc.);
- Public key(s) for proof of signature/seal;
- Authorisation for credential types which may be issued (e.g., PD A1 and/or EHIC).

8.3 Challenges

The processes have to grant performance, usability, and security while reflecting the existing legal basis.
There needs to be an analysis whether the Issuer Registry could be used in offline verification constellations (as this was found very relevant for PD A1 and EHIC in DC4EU business discussions). eIDAS 2.0 also states that an offline use is "important in many sectors" and that a wallet should be usable – where appropriate – for offline constellations. Those are described as "an interaction between a user and a third party at a physical location using close proximity technologies, whereby the Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction." (Art. 3, 55c). [10]
Some special constellations have to be taken into account – as there could be different accreditations (by different organisations) for the same issuer (e.g., a Health Insurance Institution

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

accredited by the Ministry of Health to issue EHIC while also being accredited by the Ministry of Social Affairs to issue PD A1).
The components have to be able to execute the merging or deactivation of institutions (using the trust chain).
Authorisation for identity check is required to enhance trust and data privacy. It might be required for issuers and verifiers to prove their entitlement to receive and process identity data. At least in social security base process this will be required to ensure that VCs are issued to and owned by the right person. Additionally, identity credentials might be expanded with additional national information like sector specific identifiers or health information. Thus, it can also be expected that not all information of such credential is required for specific use cases. Parties could demand a subset of identity credentials which could be realized by asking for specific reduced versions of identity credentials, defined by schema definitions.
Lastly, the participants of EBSI-VECTOR have to onboard more institutions entitled to issue credential to fulfil the project KPIs for piloting the use cases. Currently, only two issuers (DRV-Bund for Germany and DVSV for Austria) are onboarded into the project. Nevertheless, the EBSI-VECTOR participants also involved in the DC4EU Consortium already expressed the willingness of several other participating countries to join the Vector pilot activities. A decision regarding this is expected to take place at the Vector Consortium governance level.

8.4 Conclusion

The EBSI-VECTOR Trust Framework solution must comprehensively encompass and harmonize the previously mentioned frameworks and requirements. This includes addressing the varying constellations of Authentic Sources and Issuers. A critical step in this process will involve a thorough analysis to determine the extent and manner in which the existing EBSI structures and processes need to be modified or enhanced to meet these requirements effectively.

The goal is not just to create a system that functions efficiently but also one that adheres to regulatory compliance, aligns with the EBSI trust framework, and maintains a high level of trust. This includes ensuring that credential issuers are properly registered and authorized, and that their roles in the trust ecosystem are clearly defined and understood.

The outcome of this integrative and analytical process will be a trust framework that not only meets the requirements of the EBSI-VECTOR project but also sets a precedent for future developments in digital identity and security within the realm of social security.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

9 Conclusions

In conclusion, EBSI-VECTOR's Work Package 5 has effectively developed a comprehensive business blueprint, addressing the intricate dynamics of the business processes in the domain of social security. This document, focused on the integration and implementation of EBSI within the social security realm aims to enhance the operational efficiency of social security coordination and digital transformation across Europe.

This deliverable's approach, encompassing the detailed analysis of EHIC and PD A1 credentials, the formulation of use cases, and the elaboration of data models, provides a basic framework. It aims to ensure the seamless integration and effective implementation of EBSI-VECTOR within the social security context. Furthermore, this document work lays the groundwork for the practical implementation of the use cases during Deliverable 5.2 as well as providing the baseline for the feedback and validation tool for implementation activities.

In summary, the efforts and insights condensed in this document symbolize an advancement in the digitalization of social security in Europe. The comprehensive approach adopted in this deliverable not only ensures the strategic alignment of implementation efforts with the overarching goals of EBSI-VECTOR but also contributes significantly to advancing digital transformation in the European social security landscape. Future steps will entail a detailed exchange of information on the future capabilities of the EBSI infrastructure, in order to improve the likeliness of a successful pilot phase involving as many countries as possible.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

10 Annex - Definition of Back-office Interfaces for EHIC and PD A1 Issuers & Verifiers (including analysis of reusable back-offices)

10.1 Introduction

This Annex serves to define the technical and operational aspects of back-office interfaces. It is dedicated to outlining and analyzing the infrastructure and processes required for the effective and secure issuance and verification of credentials related to the European Health Insurance Card (EHIC) and the Portable Document A1 (PD A1). It aims to establish a comprehensive understanding of the back-end systems that support the issuance and verification of these documents within the context of social security within the EU. Central to this Annex is the exploration of the interaction between Authentic Sources and the Issuer and the detailed mechanisms of this interaction, particularly focusing on the challenges and solutions related to credential issuance and identity verification.

10.2 Alignment with the DC4EU Framework

In social security it is common practice to have multiple authentic sources that serve a single issuer. When a credential is issued, the authentic source makes a request to the issuer to create a credential, also sending the relevant business data to the issuer. This data is then stored in an internal database, where it is processed and used for the issuance of the credential.

When an EBSI-compliant wallet contacts the Enterprise Wallet for the issuance of a credential, it is necessary to verify that the Wallet actually belongs to the citizen who is supposed to receive the credential. In social security, it is vital that each credential is bound to a specific individual's identity.

To ensure this, the process requires that citizens provide their PID or a similar identifier to the issuer before the credential is created and issued. The issuer then uses this information to authenticate the Wallet, confirming it belongs to the intended citizen based on the verifiable identity information. This authentication allows for the issuer to securely attach the necessary binding information to the VC. This is the current proposed method within the DC4EU framework,

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

although it is important to note that the technical foundations for this approach are still being developed and requires further exploration.

The Enterprise Wallet, responsible for issuing credentials and managing EBSI interactions, operates in a stateless manner. This implies that it doesn't store data internally, instead, it retrieves business data and stores technical credential information from internal databases during runtime (i.e., as needed during its operation). Within the DC4EU Consortium, there were concerns that the existing issuer architectures and security configurations might not be able to support such permission rights for the Enterprise Wallet, which is a generic and external component.

For this reason, DC4EU has introduced a separate Cache Component (referred to as the "Data Store" in DC4EU). This component is designed for storing relevant information and operates alongside the internal core databases. However, it is located externally of the core system. This positioning allows for easier implementation, requiring less configuration, and facilitates faster issuance of credentials. Importantly, this cache component can be substituted with an internal system component at any point in time if needed in the future.

In line with these developments, DC4EU defined several endpoints to serve the needs of the specific requirements of this system. These endpoints are outlined in general terms here.

Our goal is to ensure that our back-office solution is as compatible as possible with DC4EU interfaces, aiming to provide an interoperable and efficient solution.

10.3 Cache API

10.3.1 Data Upload

First of all, a specific endpoint must be established for uploading attestation data to the Cache. Within the DC4EU framework, this data upload includes two pieces of information: the ID of the authenticating source and the ID of the person to whom the attestation belongs. It's important to note that the Person ID is only valid within the domain of the authentic source and is therefore dependent on the Authentic Source ID. Additional data to be uploaded includes the document type, the person's identity information (such as Name and Date of Birth), and various IDs related to the document itself, including those for revocation and collection.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Once the data is successfully stored in the Cache, a "success" response is generated. This response can then act as a trigger to notify the citizen that their new attestation is now available.

For efficiency in future processes of identity matching, the identity data in the Cache is expected to the same as that within the attestation (document_data). However, for faster processing, this identity data is kept separate from the attestation object itself.

10.3.2 Get portal data

A second endpoint is designed to retrieve all attestation data (-data) stored in the Cache for a individual, identified by domain specific identifier such as a Social Security Number. The Response Data includes all document information relevant for display in the national portal including the Collection-QR-Code and Collection-Deeplink. The creation of QR-Code and Deeplink, possibly through the Enterprise Wallet, still needs to be defined.

10.3.3 Get Document by Collection Code

After the EBSI-compliant Wallet contacted the Enterprise Wallet to get a specific Credential issued, the Enterprise Wallet must fetch the information from the Cache. As input Authentic Source ID, Collect ID and the Identity Data may be sufficient as input. It can be used to match the Identity Data to the corresponding Person ID and identify the attestation. The attestation data gets returned after a single match was found, which can now be processed by the Enterprise

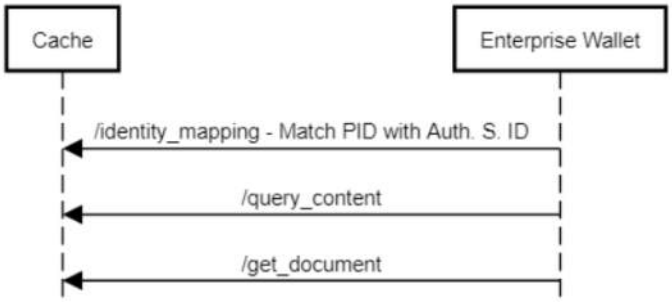
Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Wallet System for issuance. Since a collection code may be valid for single use only a check can be performed at this endpoint.

10.3.4 Additional endpoints

To allow flexibility and support testing, additional endpoints can be useful. DC4EU has defined three such endpoints. They add more transparency and can help to spot inconsistencies.



1. Identity mapping

To only map (PID-)Identity Data with the identity of the attestations an Identity Mapping endpoint may be defined.

2. Query content

Another endpoint may be used to get relevant information from all attestations that match an Authentic Source and Person ID. The response data could be used for extensive processing to increase security, stability, and quality. It may be used to secure data quality and find an unambiguous match for the collect_id (Enterprise Wallet received it from a EUDIW request).

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

3. Get document

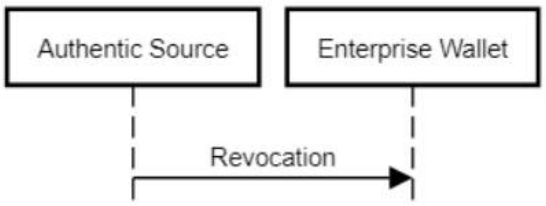
Alongside the Endpoint to get a document by collect ID a second Endpoint could serve the same purpose while using the Person ID and not the (PID-)Identity Data. Again, this can be used for testing purposes and to spot inconsistencies.

10.4 Enterprise Wallet APIs

The Enterprise Wallet will have many functionalities for different use cases and scenarios. To support social security scenarios the following Endpoints, need to be available.

10.4.1 Revocation

Revocation of a credential shall be triggered by an Authentic Source. All relevant identifying information is used as input. The Enterprise Wallet then uses this information to identify the registry entry and perform the revocation. The result gets returned to the Authentic Source for internal storage.



Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

10.5 List of REST APIs

Name	/upload	

Input	{
	“meta”: {
	“authentic_source”: “string”,
	“authentic_source_person_id”: “string”,
	
	“document_type”: “PDA1”,
	“document_id”: “string”,
	“revocation_id”: “string”,
	“collect_id”: “string”,
	
	“Identity_data”: “object”: {
	“date_of_birth”: “string”,
	“first_name”: “string”,
	“last_name”: “string”,
	},
	
	“document_data”: “object”
	}
	}
		
		ID of the authentic source
		ID of the Person (as in auth. source)
		
		ID of the uploaded document
		Type of Document “EHIC” or “PDA1”
		Optional
		Document reference ID for collection
		
		Elements of the identity object
		
		Full document payload

Output	{
	“data”: {
	“status”: “string”
	}
	}
		ResultCode
		0=OK
		<0=Error Code
		>0=Detailed Result Code

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Name	/get_portal_data	

Input	{
	“authentic_source”: “string”,
	“authentic_source_person_id”: “string”
	}
		
		ID of the Authentic Source
		ID of the Person (as in auth. source)

Output	{
	“data”: [
	{
	“document_type”: “PDA1”,
	“document_id”: “string”,
	“revocation_id”: “string”,
	“collect_id”: “string”,
	
	“attestation_data”: “object”
	“qr”: {
	“base64_image”: “string”
	},
	“deeplink”: “string”
	}
	],
	...
	
	}
		
		ID of the uploaded document
		Type of Document “EHIC” or “PDA1”
		
		Document reference ID for collection
		
		Depending on the type and includes relevant information for display
		
		Pre-formatted Collection QR-Code
		
		Collection Deeplink

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Name	/idmapping	

Input	{
	“authentic_source”: “string”,
	
	“Identity_data”: “object”: {
	“date_of_birth”: “string”,
	“first_name”: “string”,
	“last_name”: “string”
	}
	}
		ID of the authentic source
		
		Elements of the identity object

Output	{
	“data”: {
	“authentic_source_person_id”: “string”
	}
	}
		The ID of the Person (as from the Authentic Source)

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Name	/query_content	

Input	{
	“authentic_source”: “string”,
	“authentic_source_person_id”: “string”
	}
		ID of the authentic source
		ID of the Person (as in auth. source)

Output	{
	“data”: [
	{
	“document_type”: “PDA1”,
	“document_id”: “string”,
	“revocation_id”: “string”,
	“collect_id”: “string”
	}
	],
	…
	}	

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Name	/get_document	

Input	{
	“authentic_source”: “string”,
	“authentic_source_person_id”: “string”,
	“document_id”: “string”,
	}
		
		ID of the authentic source
		ID of the Person (as in auth. source)
		The Identifier of the uploaded document

Output	{
	“document_type”: “PDA1”,
	“document_id”: “string”,
	“revocation_id”: “string”,
	“collect_id”: “string”
	
	“document_data”: “object”
	}	

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Name	/document/collection_code – POST, GetDocumentByCollectCode	

Input	{
	“authentic_source”: “string”,
	“collect_id”: “string”,
	
	“Identity_data”: “object”: {
	“date_of_birth”: “string”,
	“first_name”: “string”,
	“last_name”: “string”
	}
	}
		
		ID of the authentic source
		ID of the Person (as in auth. source)
		
		Elements of the identity object

Output	{
	“document_type”: “PDA1”,
	“document_id”: “string”,
	“revocation_id”: “string”,
	“collect_id”: “string”
	
	“document_data”: “object”
	}	

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

Name	/revoke – POST	

Input	{
	“authentic_source”: “string”,
	
	“document_id”: “string”,
	“document_type”: “string”,
	
	“revocation_id”: “string”
	}
		
		ID of the authentic source
		
		ID of the uploaded document
		Type of Document “EHIC” or “PDA1”
		
		ID for revocation

Output	{
	“status”: true
	}
		Confirmation of Success

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

10.6 Conclusion

In summary, this Annex serves as a technical guide and framework for the development and implementation of back-office interfaces for EHIC and PD A1 issuers and verifiers. It emphasizes the importance of interoperability, security, and efficiency in the digital transformation of social security credentials within the EU. The chapter's insights and recommendations are geared towards ensuring a seamless, secure, and user-friendly experience for citizens and authorities dealing with EHIC and PD A1 credentials.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

11 References

[1] The European Parliament and Council, «Regulation (EC) No 883/2004 of The European Parliament and Council of 29 April 2004 on the coordination of social security systems,» EC, 2004.

[2] European Commission, «Administrative Commission for the Coordination of Social Security Systems - Summary of the minutes of the 367th meeting of the Administrative Commission,» 2021.

[3] s. a. a. i. Directorate-General for Employment, «European Social Security Pass,» EBSI, 2022. [Online]. Available: https://ec.europa.eu/social/main.jsp?catId=1545&langId=en.

[4] DC4EU, «Digital Credentials For Europe,» 2023. [Online]. Available: https://www.dc4eu.eu/.

[5] 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,» 2009.

[6] The Administrative Commission for the Coordination of Social Security Systems, «Decision No S1 of 12 June 2009 concerning the European Health Insurance Card (2019/C 106/08),» *Official Journal of the European Union,* 2010.

[7] 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 (2010/C 106/09),» *Official Journal of the European Union,* 2010.

[8] The Administrative Commission for the Coordination of Social Security Systems, «ecision No S11 of 9 December 2020 concerning refund procedures for the implementation of Articles 35 and 41 of Regulation (EC) No 883/2004,» *Official Journal of the European Union,* 2011.

[9] The European Commission, «Electronic Exchange of Social Security Information (EESSI),» Directorate-General for Employment, social affairs and inclusion, 2024. [Online]. Available: https://ec.europa.eu/social/main.jsp?catId=1544&langId=en.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.

[10] The European Parliament and the Council, «Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity,» 2021.

[11] E. B. S. I. (EBSI), «What is EBSI,» 2023.

[12] Directorate-General for Employment, social affairs and inclusion, «Public Access Interface,» 2023.

[13] The European Parliament and the Council of the European Union, «Regulation (EU) No 910/2014 of The European Parliament and the Council of the European Union of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,» 2004.

[14] European Blockchain Services Infrastructure, «EBSI Explained,» 2023.

[15] Author, «Publication Title,» p. 115, May 2023.

[16] Author2, «www.example.eu,» 22 May 2023. [Online]. Available: www.example.eu.

Co-funded by the European Union

Project co-funded by the European Union under the Digital Europe Programme under Grant Agreement n° 101102512. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HADEA). Neither the European Union nor the granting authority can be held responsible for them.