European Commission

ESSPASS

European Social Security Pass

Directorate General for Employment, Social Affairs and Inclusion

OVERVIEW
& MAIN CONCEPTS

EUROPEAN COMMISSION

Directorate-General for Employment, Social Affairs & Inclusion
E-mail: EU-ESSP@ec.europa.eu

European Commission
B-1049 Brussels

Manuscript completed in October 2022

Luxembourg: Publications Office of the European Union, 2022

EN PDF ISBN 978-92-76-58110-9 doi:10.2767/841176 KE-03-22-051-EN-N

Table of Contents

01

WHAT ESSPASS IS ABOUT

Issues ESSPASS addresses

Main objective

About the pilot project

EU rules on social security coordination[1] call on the Member States to increasingly adopt digital solutions to improve the exchange, access and processing of information across borders, as well as to offer user-friendly services. **The ultimate goal is to help people and businesses exercise their social security rights and duties when moving and working in the EU, while reducing the administrative burden on public administrations, businesses and citizens**.

In 2017, the European Commission made available the EESSI IT system, which allows social security institutions across the EU to exchange information more rapidly and securely, while gradually phasing out their paper-based processes.EESSI allows for secure and fast exchange of information between institutions (e.g. to notify a posting operation to the institution of the receiving country). However, only social security institutions have access to the EESSI system and information is not available in real-time. The ESSPASS pilot intends to complement EESSI by facilitating the interactions between mobile citizens and relevant public authorities for social security purposes (e.g. labour inspectors or health care providers), making real-time verification of social security coverage and entitlements possible, including by those actors that do not have access to the EESSI system.

What are the current issues?

Citizens who move across borders are often faced with time-consuming procedures, and they often need to request and carry several documents to certify their social security coverage. This triggers a series of administrative processes involving different public institutions and private bodies in two or more Member States. Common obstacles for mobile citizens are, for instance, the lack of awareness of their rights, the **obligation to request documents**, which are often **issued with delays** by the relevant institutions, and the **possibility to lose their document.** The fact that paper or digital proofs are still needed to verify the entitlement of the citizens to their rights might also lead to **forged documents** and loopholes in the application of the legal obligations. The **lack of timely and sufficient information** makes it more difficult for them to prevent fraud. Lengthy exchanges are sometimes needed, which can lead to refusal of the portable documents, for instance if there are doubts about their validity.

Hindered portability of social security rights and barriers to free movement

> The way social security coordination rules are implemented in each Member State are still cumbersome and paper based. This creates difficulties for citizens to move across Europe and be able to fully exercise their rights and obligations, while being compliant with National and European Regulations. As a result, the different actors involved in the execution of these rights, such as social security institutions, employers, healthcare providers and labour inspectors face difficulties to fight against fraud, to deal with different national requirements and finally to protect citizens' interests and entitlements to their social security rights.

This overall problem definition can be further broken down in more specific problems, as described below:

[1] Regulations (EC) No 883/2004 and (EC) No 987/2009

Need for Physical Evidence

Citizens currently can only prove their social security coverage by having physical evidence with them at all times (e.g., PDF or paper). This may lead to problems when it comes to the exercise of their rights (e.g., due to loss) but is also conducive to non-compliance, forgery, or fraud.

Lack of Interoperability

Several interactions are needed to obtain and verify the information. Professionals needing that information (e.g. inspectors) cannot have access to data in real-time, which makes it difficult to early detect irregular conditions, e.g. falsified documents.

Improvable Administrative Process

Member States have different levels of digital maturity. This can lead to lengthy processes and the need for citizens to be physically present at the competent institution, because digital services are not available or because their presence is needed for identification purposes.

Identification, authentication and verification

Inspectors and clerks are often faced with diversity and fragmentation of identification schemes. This makes it cumbersome or even impossible to correctly and swiftly determine the social security status of a mobile citizen, or to errors with the identification of the person.

Main Objective of ESSPASS

The main objective of ESSPASS is **to facilitate the interaction between mobile citizens and national authorities and improve the portability of social security rights across borders**. It will facilitate the **verification process** by the competent actors and institutions. Thanks to ESSPASS, the issuing institutions will be able to update in real time the validity of the document stating the social security situation of the person, for instance in cases of changes, revocation, or suspension. Furthermore, ESSPASS will reduce the need for paper or plastic certificates.

About the ESSPASS Pilot Project

The launch of the European Social Security Pass (ESSPASS) pilot was announced in the European Pillar of social rights action plan to explore the feasibility of a digital solution for the cross-border verification of social security coverage and entitlements.

The European Commission and INPS (Istituto Nazionale della Previdenza Sociale) decided to launch the first phase of the European Social Security Pass pilot **to test, in a first phase, the cross-border digital verification of the validity and authenticity of the Portable Document (PD) A1** which indicates the social security legislation applicable to the holder and is used for example when a person is temporarily posted to work in a Member State other than the one where they are insured.

Italy, with INPS, plays the role of PD A1 Issuer and other countries are actively involved in the development and testing of an application for labour inspectors to verify the PD A1 electronically. Based on the preliminary findings, the Commission would be able to decide whether to **extend the pilot to other social security coordination procedures**, which are also mainly paper-based (such as the European Health Insurance Card and other seven portable documents in the fields of sickness and unemployment benefits, accident at work and occupational diseases and pension).

02

ESSPASS SOLUTION OVERVIEW

Main areas of focus of ESSPASS

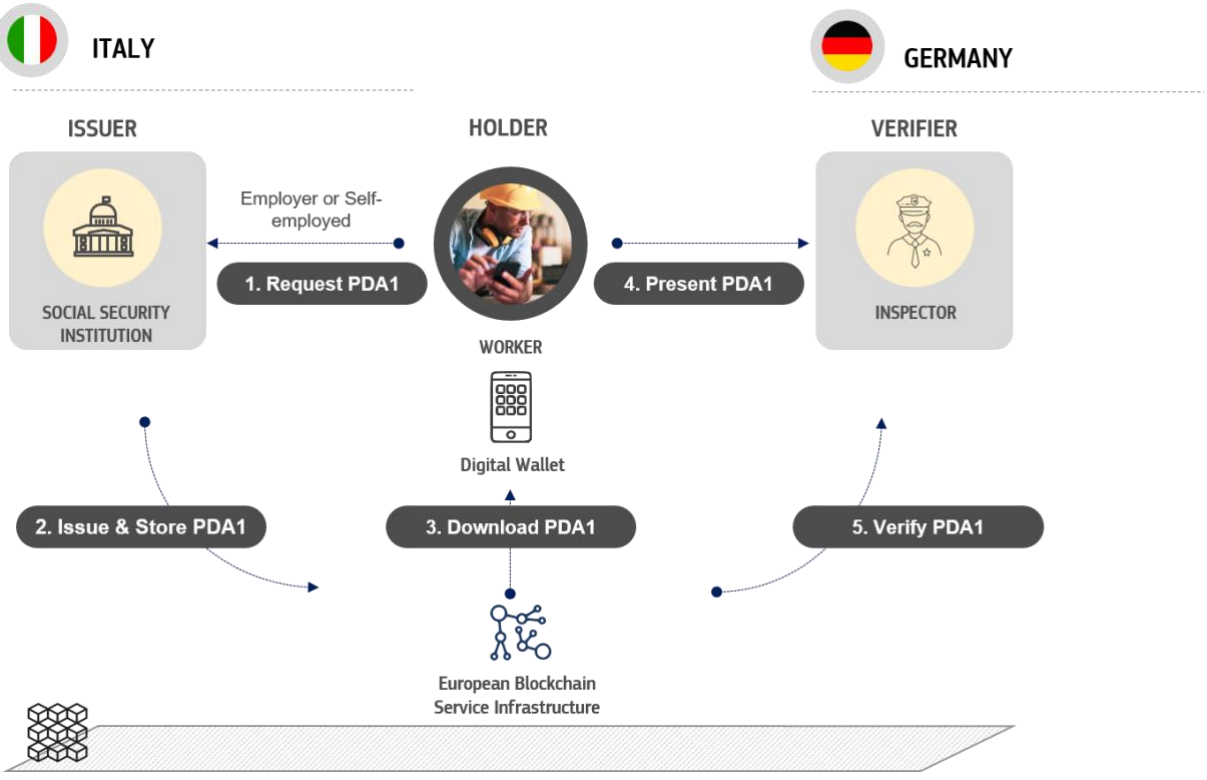
High-level flow of the PDA1 use case

Link with other initiatives

In a nutshell, the European Social Security Pass is a **blueprint for the end-to-end digitalisation of the social security coordination procedures**. It leverages on existing EU and national digital initiatives to facilitate the interactions between mobile citizens, workers, businesses and public or private social security institutions. The European Social Security Pass focuses on three main areas:

1. **Digitalising the processes for the request and issuance** of portable documents;
2. **Improving the identification of mobile citizens** and workers when performing activities or accessing public services abroad; and
3. **Introducing real-time mechanisms for the cross-border verification** of the social security entitlements of mobile citizens and workers.

The first use case of ESSPASS focuses on the verification of social security coverage of posted workers (and possibly of other relevant categories of workers like those working in at least two countries). Nevertheless, ESSPASS is designed to be able to implement in a potential second phase other social security coordination procedures, e.g. digitalisation of the European Health Insurance Card (EHIC).



The issuance and verification of the PDA1 using ESSPASS entails the following steps:

1. The employer of the sending Member State requests the verifiable attestation from the National Social Security Institution for the posted worker (in case of an employee) or by the posted worker itself (in case of a self-employed person), requesting the verifiable attestation from the National Social Security Institution.

2. The National Social Security Institution verifies the request for the verifiable attestation successfully. The attestation is made available to the posted worker.

3. The posted worker stores the verifiable attestation duly signed by a Trusted Issuer in a digital wallet, together with his/her identity.

4. The process is finalised in the hosting Member State where an inspector requests the posted worker to present the verifiable attestation.

5. The inspector then does a real-time validation of the verifiable attestation by checking the verifiable attestation and signatures of all involved parties.

European Blockchain Service Infrastructure (EBSI)

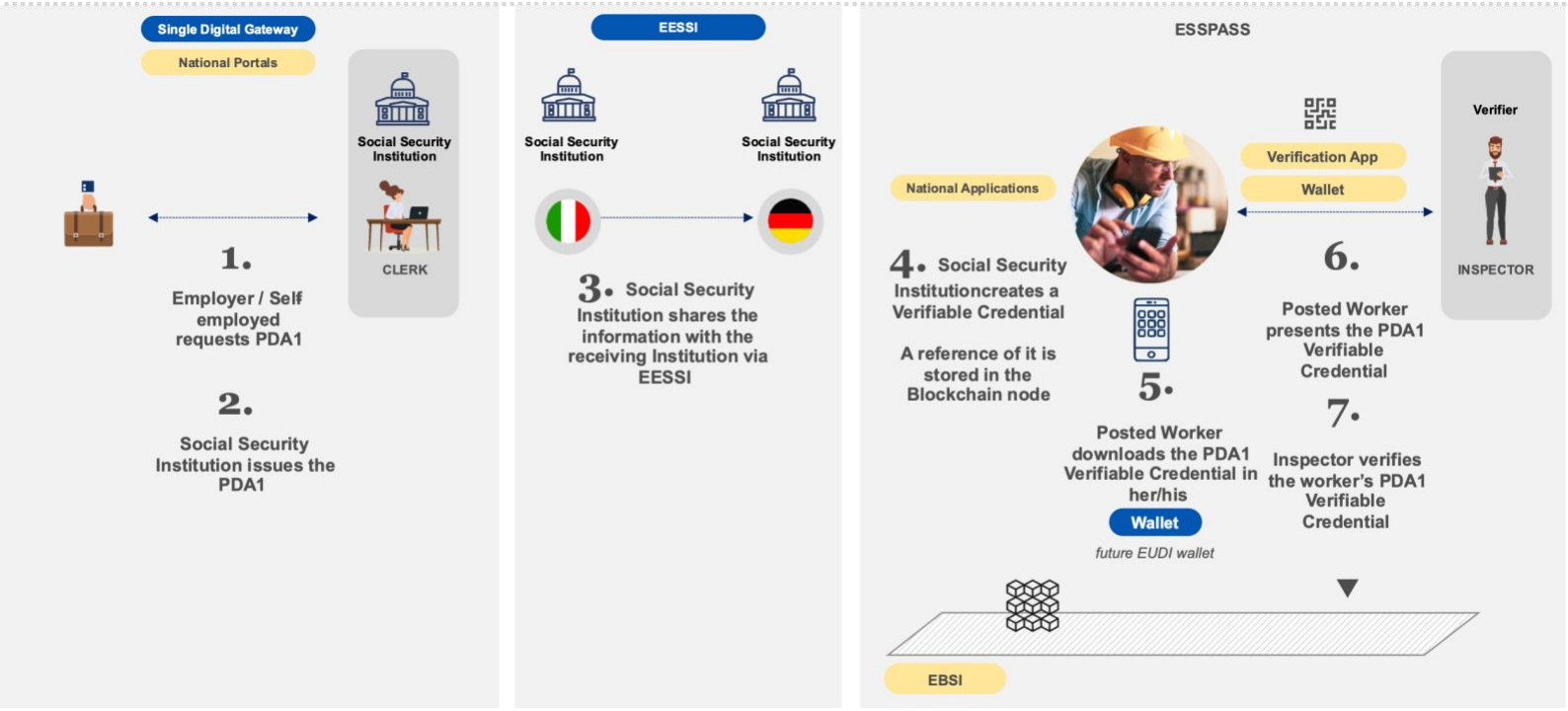
ESSPASS relies on EBSI to guarantee the trust chain for the generation of the Verifiable Credentials (e.g PDA1). Generic and standard exchange protocols are used for the user, holder and verifier. These protocols are implemented by EBSI. This issuance and verification process is fully aligned with the EU Digital Identity principles: Citizen at the centre, and the citizen has full ownership of his/her information.

More about EBSI

Link with other EU initiatives

ESSPASS is about standardising the process for the issuance, sharing and verification of digital documents between citizens and public administrations. To foster standardisation and guarantee interoperability, the ESSPASS pilot intends to build on current and future EU initiatives such as the Single Digital Gateway or the proposed EU Digital Identity Framework, among others.

The ESSPASS pilot is designed to reuse and build on other relevant digital initiatives.



Electronic Exchange of Social Security Information (EESSI)

EESSI is a message exchange system that allows for secure and fast exchange of information between institutions (e.g. to calculate the pension entitlements of someone who worked in several Member States over their career). Only social security institutions have access to the EESSI system. The ESSPASS pilot explores ways to complement EESSI by facilitating the interactions between mobile citizens and relevant public authorities and other actors for social security purposes (e.g. labour inspectors or health care providers), making real-time verification of social security coverage and entitlements possible, including by those actors that do not have access to the EESSI system.

Single Digital Gateway

The Single Digital Gateway Regulation (SDG) provides that Member States shall ensure that users can access and complete key administrative procedures fully online, and deliver the output of such

procedures electronically[2]. An automatic acknowledgement of receipt to the user will also have to be provided, once the request is submitted. Some of these procedures are under the social security coordination field, including the request for determination of applicable legislation (whose output is the PD A1) and for the issuance of the European Health Insurance Card.

While the SDG could be used, in the future, as a possible entry point for people and businesses, redirecting them to the national portals where they can, for instance, request online the issuance of the PD A1, it is not meant to cover the cross-border digital verification of its authenticity and validity, which is explored in the ongoing ESSPASS pilot.

The mobile citizen can choose to either store the PD A1 in electronic format in an electronic wallet, or still print the PD A1, augmented with a QR-code, on paper. Both mechanisms will facilitate the verification of the:

- Integrity of the PD A1,
- Validity of the PD A1,
- Authenticity of the Issuer;

The authenticity of the Holder can only be verified when the PD-A1 is shared via the electronic wallet.

European Digital Identity (EUDI) Framework

ESSPASS intends to make use of the European digital identity wallet. On 3 June 2021, the Commission published the proposal for a European Digital Identity (EUDI) framework. The initiative revises the existing cross-border legal framework for trusted digital identities: the European electronic identification and trust services (eIDAS) Regulation. ESSPASS could make use of this framework for the cross-border identification and authentication of citizens.

[2] Where possible under applicable Union and national law (Article 6 and Annex II of the SDG Regulation) from 12 December 2023

03

KEY BENEFITS OF ESSPASS

Main benefits that the digitalisation of the verification of social security coverage and entitlements brings to all actors - mobile citizens, social security institutions, verifying bodies, healthcare providers…

The envisaged benefits from the ESSPASS pilot (considering the implementation of all use cases, not only limited to the PDA1), fostering the digitalisation of the verification of social security coverage and entitlements, are the following:

Easier portability of social security rights thanks to a more efficient verification of citizen's entitlements

Facilitation of the verification process to all actors involved without the need to call upon a central entity

The early identification and prevention of fraudulent activities Reduced risk of fraud and errors, e.g. clerical errors, falsification of documents

ESSPASS would in particular bring:

1. Trusted Verification Process

Digitalisation of portable documents alone is not enough. One of the key challenges that ESSPASS addresses is digital verification of these documents in a trusted way. This is facilitated by the Verifiable Credentials standard (W3C). Verifiable credentials are essentially tamperproof and secure, allowing verification without calling upon the issuer. The holder can generate and instantly share verifiable presentations upon request of a verifier. This allows the verifier to trust the information that is shared, in a face-to-face or online interaction, i.e. that the issuer of the credential is a trusted issuer, that the credential has not been tampered with and that it belongs to the person who presents it. Furthermore, ESSPASS would also improve security of the paper version of the Portable Document, as an alternative to the digital version.

2. Interoperable Verification Tools

The institution/competent actor (such as the labour inspectorate or health care provider) in another Member State will be able to rely on interoperable verification tools to improve the identification of citizens, and to verify the authenticity, integrity and validity of Portable documents. The ESSPASS verification tools should not replace systems already established in the Member States but rather complement, or be integrated, in these. In the case of the PDA1-related procedures it provides labour inspectors additional means to verify the integrity of PD A1 documents.

3. Citizen-centric Solution

Citizens/workers will not have to carry paper documents, as they will be able to choose to download the electronic version of the portable documents, along with other documents – e.g. EHIC, in their electronic wallet. This facilitates the recognition of entitlements and avoids the citizen being in a difficult situation just by having forgotten or lost the physical evidence that proves such entitlements. Furthermore, the citizen keeps control and ownership of their data. The citizen can decide which data to share.

4. Improved checks at issuing stage

ESSPASS opens opportunities for institutions to perform additional checks before issuing a credential (e.g. improved checks of the posting conditions), which further supports them in preventing fraud and errors.

ESSPASS should thus benefit all those involved in cross border activities, starting with mobile workers/citizens and employers but also social security institutions, verifying bodies (e.g. labour inspectors) or health care providers.

04

ESSPASS IN DETAIL

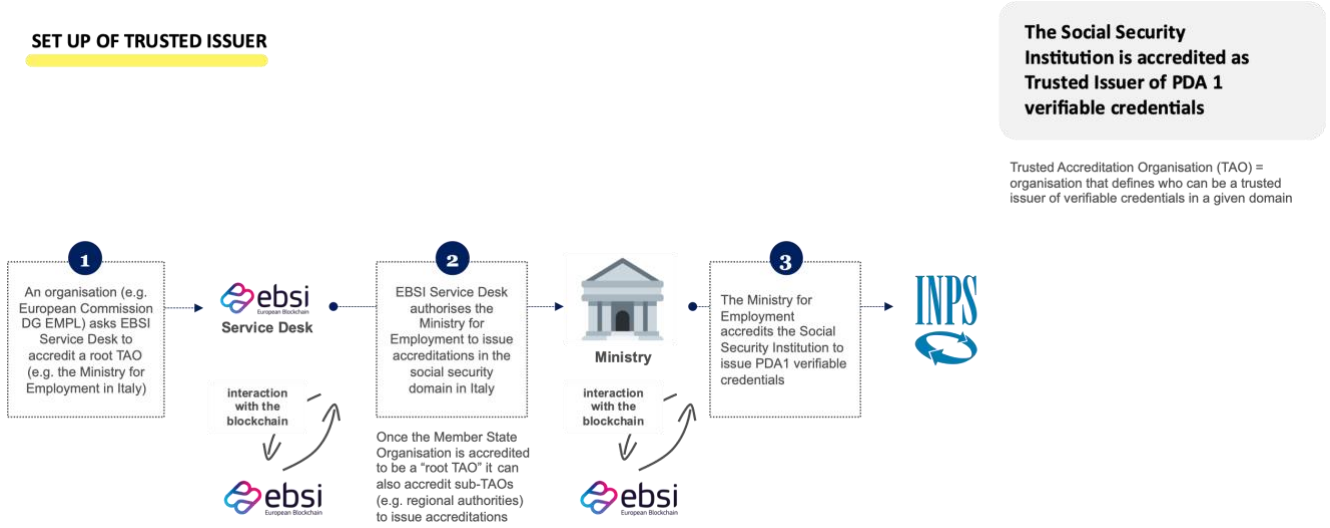
Actors and user flows
High-level Architecture
Standards
Main Concepts

Actors and User flows

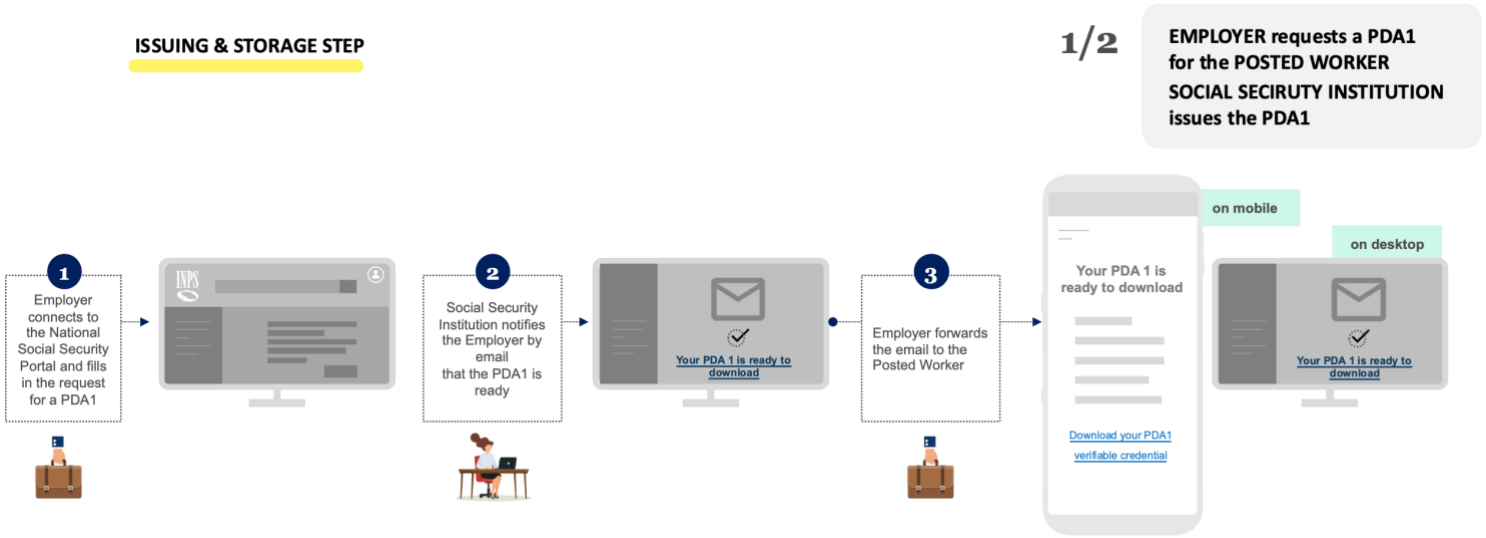
The actors and the user flows below are based on the use case for the verification of social security coverage of posted workers – the issuance of a PDA1 Verifiable Credential, the download of it in a digital wallet and its verification by an inspector on site. The user flows represent the step-by-step process from the perspective of the involved actors.

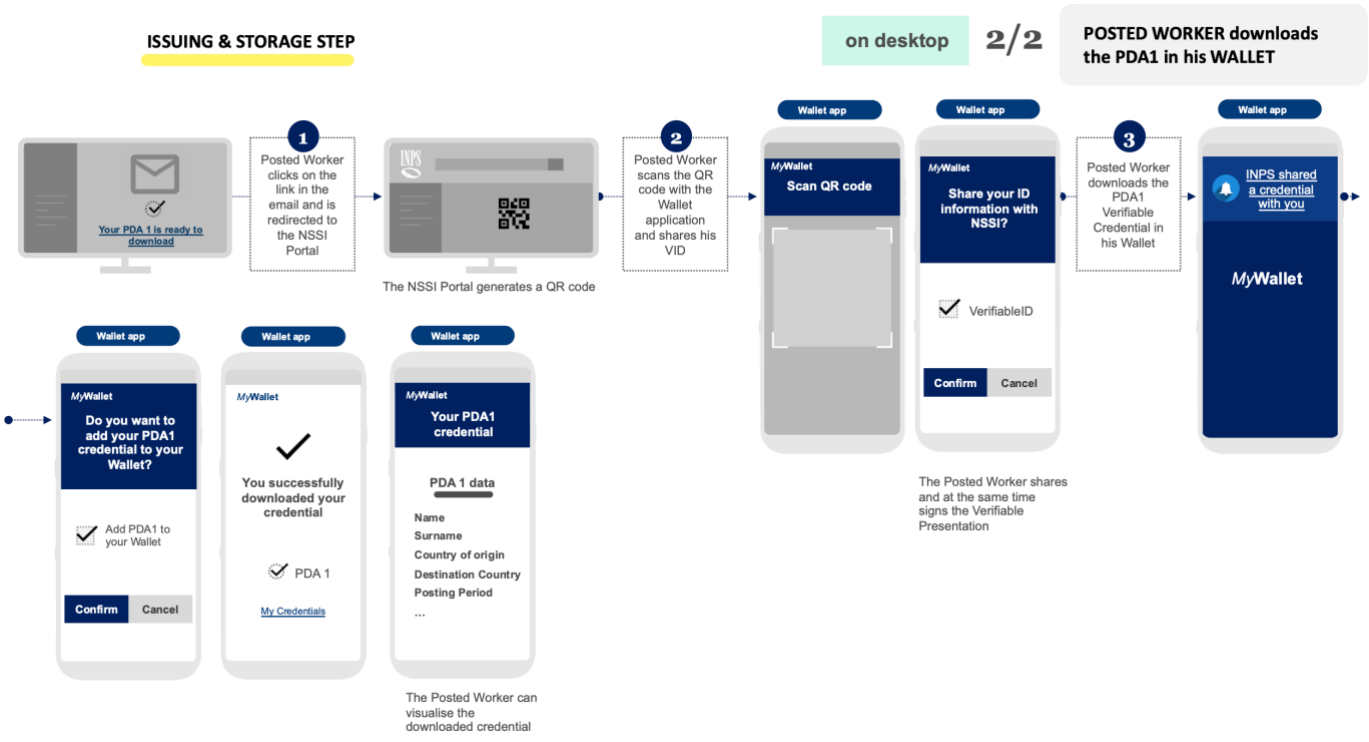
ACTOR	DESCRIPTION	ROLE
EMPLOYER	**The Employer** is the party requesting the PD A1 form to the issuer Institution (a National Social Security Institution). The employer is the responsible party for sending the posted worker abroad to work. *Remark: a self-employed person for the purposes of this description is named also the employer.*	Requester
CLERK	**The Clerk** is the clerk of the National Social Security Institution that will manage the business process for issuing the PD A1, after a request from the Employer. The NSSI is responsible to issue the PD A1 form and the related 'Verifiable Credential'.	Issuer
POSTED WORKER	**The Posted Worker** is the person carrying out the requested work abroad and is 'holding' the PDA1 Verifiable Credential.	Holder
INSPECTOR	**The Inspector** is the person who requests/validates the Verifiable PD A1. S/he will check if the posted worker is in possession of a valid PD A1 form and validate the PD A1 Verifiable Credential, on behalf of the National Social Security Institution mandating this check.	Verifier

0. SET UP of a Trusted Issuer

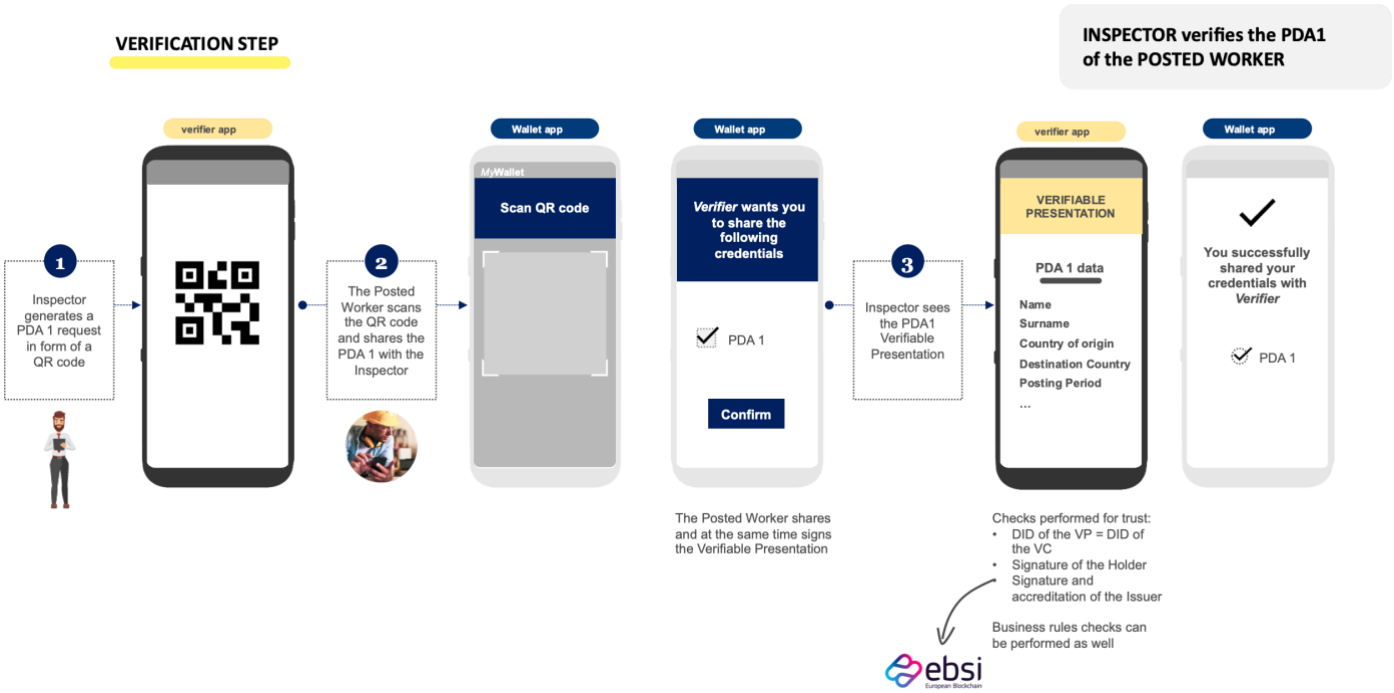


1. ISSUING AND STORAGE of the PDA1 Verifiable Credential





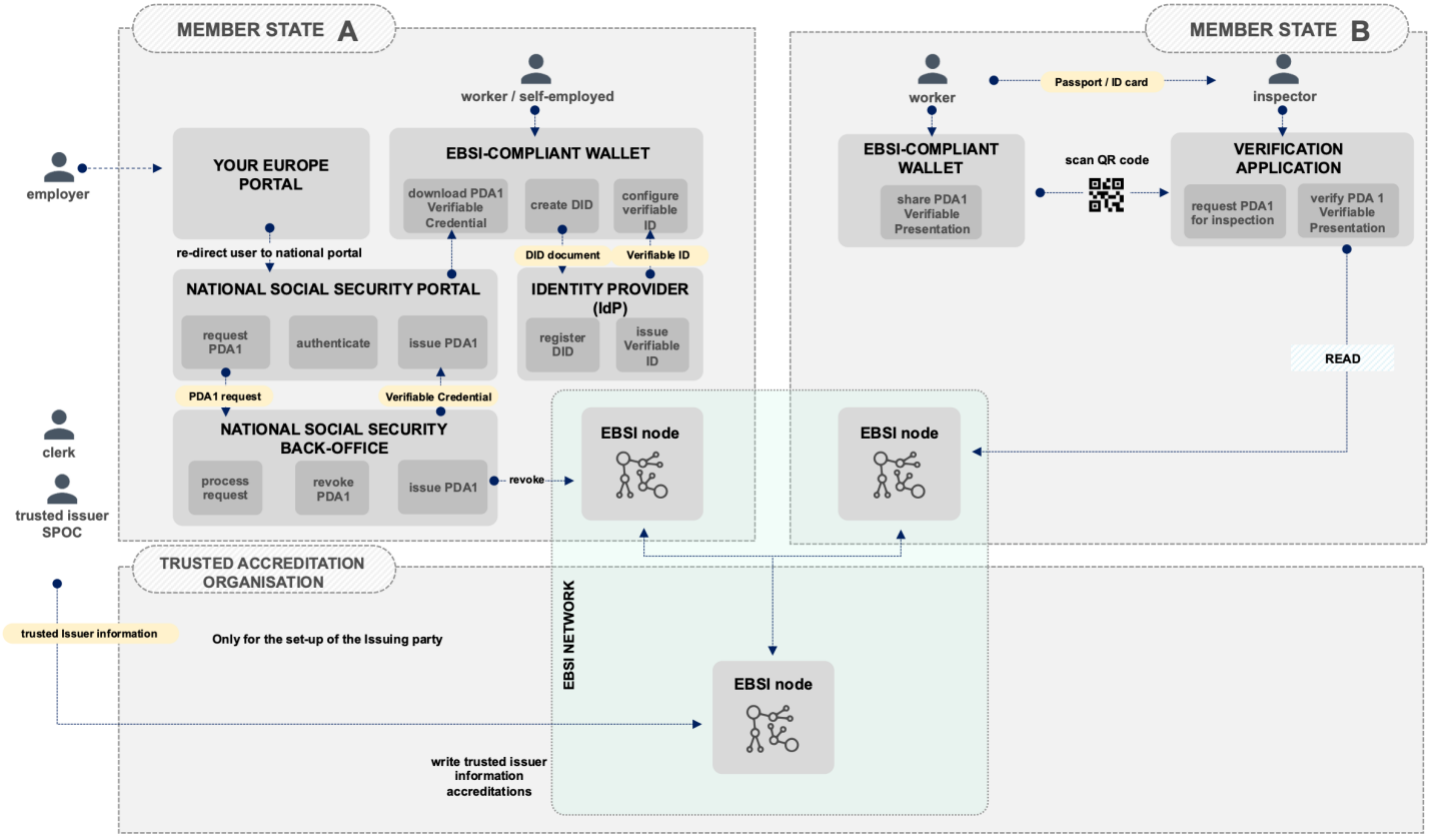
2. VERIFICATION of the PDA1 Verifiable Credential by an Inspector on site



***Notes**:*

- ⇨ *A web application can be used on e.g. desktop devices instead of a mobile application that is represented in this user flow diagram.*
- ⇨ *The verification process could be also carried out "offline" where the Holder would present the PDA1 in a PDF format containing a QR code that the Verifier scans.*

Architecture



Solution concept diagram

Standards

ESSPASS uses EBSI, which is based on the following specifications:

Verifiable Credentials W3C specification

The Portable Document is issued as a “verifiable credential”. Verifiable credentials can represent the same information that physical credentials represent. The W3C specification provides a standard way to express digital credentials in a way that is cryptographically secure, privacy respecting, and machine-verifiable.

More about W3C Verifiable Credentials specification

Decentralized Identifiers (DIDs) W3C specification

Decentralized Identifiers (DIDs), as defined in the W3C specification are a new type of globally unique identifier. They are designed to enable individuals and organizations to generate their own identifiers using systems they trust. These new identifiers enable entities to prove control over them by authenticating using cryptographic proofs such as digital signatures.

More about W3C Decentralized Identifiers specification

OpenID Connect specification

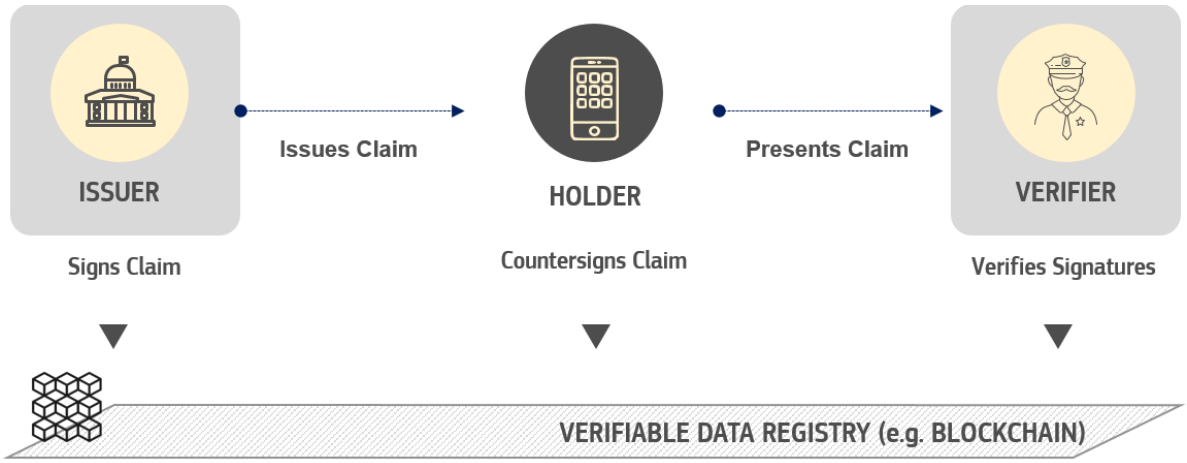
OpenID[3] Connect is the protocol used to exchange Verifiable Credentials between the Wallet and the Issuer and between the Wallet and the Verifier.

More about OpenID Connect specification

Main concepts

Self-Sovereign Identity

Self-Sovereign Identity (SSI) is an approach that allows an individual to own and control their identity. SSI addresses the difficulty of establishing trust in an interaction[4]. In an SSI interaction, the holder of the credential presents it to a verifying party, who can verify that the credentials came from an issuer that they trust.



[3] https://openid.net/
[4] Wikipedia entry on Self-Sovereign Identity: https://en.wikipedia.org/wiki/Self-sovereign_identity

Verifiable Credentials

Citizens use credentials to provide different kinds of proofs, e.g. that they have sufficient level of education (diploma), that they are nationals of a country (ID), that they have social security coverage (PDA1), etc. In the physical world, these are usually cards, certificates or other portable documents.

According to W3C, a verifiable credential can represent the same information that a physical credential represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts[5].

Verifiable credentials essentially provide digital watermarking of claims through public key cryptography and privacy-preserving techniques to prevent correlation. Moreover, third-parties are instantly able to verify this data without having to call upon the issuer.

Holders of verifiable credentials can generate and instantly share verifiable presentations upon request of a verifier. This allows the verifier to trust the information that is shared, in a face-to-face or online interaction, i.e. that the issuer of the credential is a trusted issuer, that the credential has not been tampered with and that it belongs to the person who presents it.

Verifiable credentials are essentially tamperproof, secure and verifiable, avoiding cumbersome back-and-forth between verifiers and issuers. The holder keeps control and ownership of her/his data.

Digital Wallet

A digital wallet allows you to **securely store and present credentials**, such as PDA1, EHIC or identity credential.

According to the definition of EUDI[6], the European Digital Identity Wallet can be seen as a combination of several products and trust services that enables users to securely request, obtain and store their information allowing them to access online services, share data about them and electronically sign/seal documents.

[5] W3C Verifiable Credentials Data Model v1.1: https://www.w3.org/TR/vc-data-model/#what-is-a-verifiable-credential

[6] European Digital Identity Architecture and Reference Framework, outline document, published on 22.02.2022

05

GET INVOLVED

Different ways you can take part in
the ESSPASS pilot

Institutions can opt for different degrees of involvement in the first phase of the pilot project, depending on their availability of budgetary and human resources. Higher investment would mean improved readiness for a future roll-out phase.

Subject Matter Expert

(Lower investment) ■

The institution will participate in meetings, workshops and can contribute to the drafting of deliverables.

Verifier

(Medium investment) ■■

The institution will develop a prototype of an application, in line with the specifications under the European Blockchain Services infrastructure, for the verification of PD A1 issued by another country. The institution will also participate in interoperability testing sessions.

Light Issuer

(Medium investment) ■■

The institution will update its national system for the issuance of a PD A1, e.g. in PDF format. The PD A1 will be augmented with a QR-code to allow verification in the receiving Member State. The national systems need to be connected to the EBSI network.

Full Issuer

(Higher investment) ■■■

The institution will reuse an existing EBSI-compliant wallet for the storage of the electronic PD A1 as a verifiable credential conforming the World Wide Web Consortium (W3C) Recommendation. The national systems need to be connected to the EBSI network.

For the piloting phase, participating countries can make use of EU funding to support their activities, in particular under **ESF+**, the **Digital Europe Programme** and the **Recovery and Resilience Facility**.

Get in Touch

For more information, your contact is:

Monica.LOPEZ-POTES@ext.ec.europa.eu

06

LINKS

Q&A page on ESSPASS[7]

EBSI – European Blockchain Service Infrastructure[8]

Electronic Exchange of Social Security Information (EESSI)[9]

Single Digital Gateway[10]

Proposal for a European Digital Identity framework[11]

Funding Opportunities

European Social Fund +[12]

Digital Europe Programme[13]

Recovery and Resilience Facility[14]

Standards and specifications

W3C Verifiable Credentials specifications[15]

W3C Decentralized Identifiers specifications[16]

OpenID Connect[17]

ESSPASS Wiki space

Access to the ESSPASS wiki space can be granted upon request.
Please contact us EU-ESSP@ec.europa.eu

---

[7] https://ec.europa.eu/social/main.jsp?catId=1545&intPageId=5540&langId=en
[8] https://ec.europa.eu/digital-building-blocks/wikis/display/ebsi
[9] https://ec.europa.eu/social/main.jsp?catId=1544&langId=en
[10] https://ec.europa.eu/growth/single-market/single-digital-gateway_en
[11] https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation
[12] https://ec.europa.eu/european-social-fund-plus/en
[13] https://digital-strategy.ec.europa.eu/en/activities/digital-programme
[14] https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en
[15] https://www.w3.org/TR/vc-data-model/
[16] https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers
[17] https://openid.net/connect/

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696 or
- by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://op.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

Publications Office
of the European Union