EUDI wallets with OpenID for verifiable credentials

Leveraging identity to securely and privately mobilise personal data with digital wallets

Abstract: This paper comprehensively overviews OpenID protocols leveraging verifiable credentials. We delve into the nuances of OpenID for verifiable credential protocols like self-issued OpenID provider V2 (SIOPv2), verifiable credential issuance (OID4VCI) and OpenID for verifiable presentations (OID4VP), highlighting their pivotal roles in enhancing privacy and fortifying digital identity. Through real-world scenarios, the critical values of OID4VCI and OID4VP are illustrated, emphasising their transformative potential in shaping the landscape of digital wallets, with a focus on the innovative European Union Digital Identity (EUDI) Wallets.

Target Audience: Professionals and stakeholders in the world of verifiable credentials keen on understanding how they map to OpenID, OpenID4VC and OpenID4VP workflows.

Editors: George Padayatti (iGrant.io, Sweden), Lal Chandran (iGrant.io, Sweden), Aron Szabo (E-Group, Hungary)

November 2023

Version 1.0

Acknowledgements

To all contributors who provided valuable inputs to this paper:

- Dr. Peter Lee Altmann (DIGG, Sweden)
- Dr. Godwin Caruana (University of Malta, Former CTO, Government of Malta IT Agency)
- Fredrik Linden (MyData, Sweden)
- Dr. Nikos Triantafyllou (University of the Aegean, Greece)
- Dr. Mikael Linden (Real-time economy project, Gofore Ltd, Finland)
- Dr. Abdul Ghafoor (Senior researcher, RISE, Sweden)
- Ms. Lotta Lundin (Co-founder and CEO, iGrant.io, Sweden)
- Dr. David Goodman (Chief Evangelist, Security, iGrant.io, Sweden)

Special thanks to the following entities for supporting the writing of this paper:

Co-funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the granting authority. Neither the European Union nor the granting authority can be held responsible for them.

Table of contents

1.0 Introduction

In the ever-changing landscape of digital identities and security, EUDI Wallets are at the forefront of a revolutionary shift towards enhanced security, privacy and user control. EUDI Wallets have seamlessly integrated a few pivotal protocols targeting better control of personal data. These include OID4VC (OpenID for verifiable credentials) [1], which in turn specifies OID4VCI (OpenID for verified credentials issuance) and OID4VP (OpenID for verifiable presentations) into their digital wallet ecosystem, alongside a robust suite of other cutting-edge privacy mechanisms and formats such as SD-JWT (selective disclosure JWTs) and those capable of ZKP (zero-knowledge proofs).

This article explores how the OID4VCI and OID4VP could be implemented in digital wallets for organisations and individuals and the fundamental values they provide. These specifications align with the requirements specified in the European Architecture and Reference Framework (ARF) [2].

2.0 OpenID protocols leveraging verifiable credentials

The OpenID Foundation and its communities have developed several protocols to facilitate and implement verifiable credentials (VC) in identity verification and authentication flows.

This section describes the three main protocols within the OpenID ecosystem: SIOPv2, OIDC4VCI, and OID4VP. These offer distinct approaches and advantages tailored to specific use cases and requirements. They signify the OpenID Foundation’s efforts to intertwine decentralised and verifiable data into user authentication while leveraging established principles and flows of OpenID Connect (OIDC). It is crucial to recognise that the technology and standards in this domain are progressively evolving. As such, the most recent advancements should be sourced directly from the OpenID Foundation's documentation and other pertinent authoritative sources (Examples include references [1][3][4][5] etc.).

2.1 OpenID for Verifiable Credentials (OID4VC)

OID4VC provides a set of specifications to help users have more control and privacy over their personal identity details. At its core, OID4VC leverages OIDC, letting users manage their IDs and share identity details directly with those checking it without needing a mediator. This reduces the need for central organisations to manage identities. It consists of three specifications:

- Self-issued OpenID Provider v2 (SIOPv2)
- OID4VCI
- OID4VP

Each of the above is explored further below.

2.2 Self-Issued OpenID Provider V2 (SIOPv2)

SIOPv2 is an OpenID protocol allowing an end-user to control an OpenID provider (OP) and is a fundamental OID4VC/OID4VP ecosystem building block. It enables users to issue VCs, giving them unprecedented control over their identity and personal data. In technical terms, users can self-issue VCs and use decentralised identifiers (DIDs) within the OpenID flow. The key aspects of SIOP v2 are:

Decentralised authentication: A user can authenticate using an identifier they control with a verifier using, for example, a DID. Such a DID can rely on decentralised trust anchors on a decentralised infrastructure.

Standardised interaction flows: By conceptualising user interaction flows, such as login and consent, SIOPv2 aspires to deliver a harmonious user experience across various platforms and applications.

Enhanced DID Integration: Surpassing its predecessors (SIOPv1 and the SIOP DID Profile [6]), SIOPv2 enhances the support and utilisation of DIDs.

2.3 OpenID for Verifiable Credential Issuance (OID4VCI)

OID4VCI sets guidelines for issuing VCs in various formats. As per OID4VCI, an individual's digital wallet requires a key, an OAuth access token, to retrieve a VC. This token is secured through the standard OAuth 2.0 procedure or the pre-authorised code flow (as detailed in Reference [5, Chapter 3.5]). OID4VCI mandates specific online access points (endpoints):

1. The credential endpoint is for VC issuance.
2. A mechanism for disseminating information about which VCs an issuer is authorised to issue.

Additionally, OID4VCI suggests some optional endpoints:

1. The batch credential endpoint is intended to request multiple VCs simultaneously.
2. The deferred credential endpoint facilitates delayed VC issuance.
3. A credential offer endpoint that allows an issuer to initiate the VC issuance to a known individual.

2.4 OpenID for Verifiable Presentations (OID4VP)

OID4VP postulates a methodology focussed primarily on employing VCs for user authentication, enabling users to demonstrate control over a DID and authenticate with a service, negating the need for a centralised identity provider. The key aspects of OID4VP are:

User-centric authentication: OIDC4VP enables the direct use of VCs for authentication, embedding a user-centric paradigm.

Privacy preservation: The protocol is meticulously crafted to mitigate the unwarranted disclosure of personal information throughout the authentication trajectory.

Direct VC presentation: Facilitating users to directly present their VCs to the relying party (verifier) amplifies privacy and user autonomy in data sharing.

3.0 Why do we need OID4VCI and OID4VP?

OID4VCI and OID4VP are introduced to address two fundamental aspects of VCs compared to traditional identity assertions (for example, OpenID Connect). Firstly, they cater to the unique nature of VCs, where a predefined schema (the credential type) and cryptographic holder binding ensure secure, **direct** presentation from individuals to relying parties without the need for credential issuers or intermediaries. Secondly, OpenID is an open standard with a high level of maturity and proven OIDC and OAuth industry standards. Extending this with OID4VCI and OID4VP offers the invaluable ability to configure and adapt to any schema definition, bringing the power of VCs to industry-wide adopted OpenID protocols. This adaptability ensures VCs can represent various attributes and qualifications, meeting the demands of various use cases.

In summary, OID4VCI and OID4VP bridge the gap between traditional identity assertions and the modern, decentralised digital identity landscape by providing security, privacy, user control and the flexibility to define custom schema definitions.

4.0 How does it work?

4.1 OpenID Connect and Verifiable Credentials

To understand how it works, let's look at what a VCs and OpenID workflow look like. In the OIDC workflow illustrated in Figure 1, an individual seeking specific access (Step 1) to a resource is redirected to **authenticate** and **authorise** to the original issuer (Step 3). Here, every data-using service or the verifier has a direct relationship with the issuer, where the verifier requests holder information from the issuer (Step 2) before granting access to the individual.

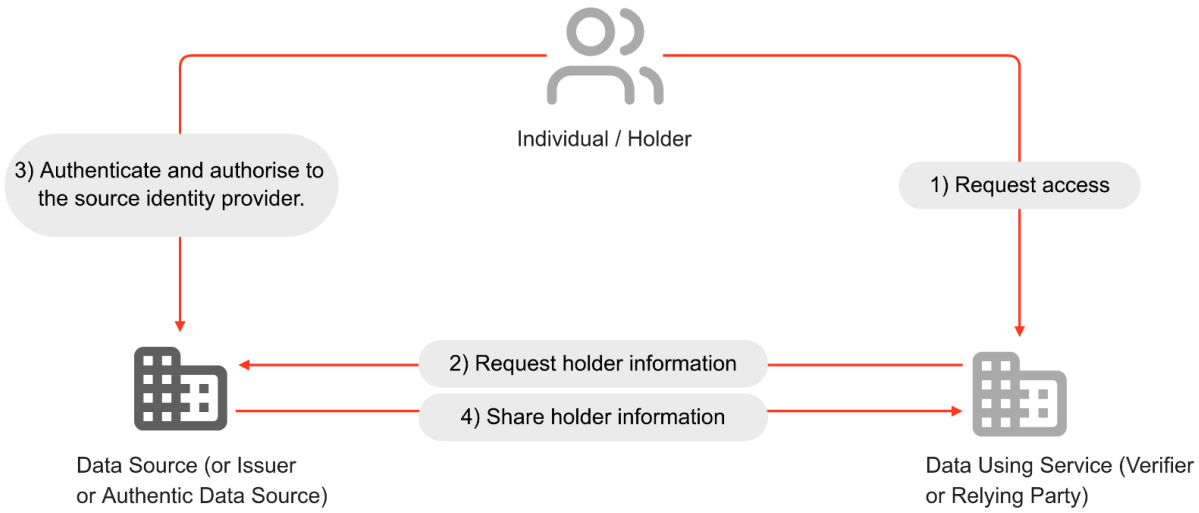

Figure 01: OIDC workflow for providing access to holder data

OIDC uses JSON web tokens (JWT) format for tokens exchanged between the relying party, authorisation server and resource server. JWTs are cryptographic tokens confirming the user's identity after successful authentication. These tokens include claims or assertions about the user, such as the user's identifier and the authentication timestamp, which relying parties can verify using digital signatures. Additionally, JWTs may be used in OIDC to send secure authentication requests and to obtain user information from the user info endpoint, ensuring that sensitive data is handled in a secure and verifiable manner.

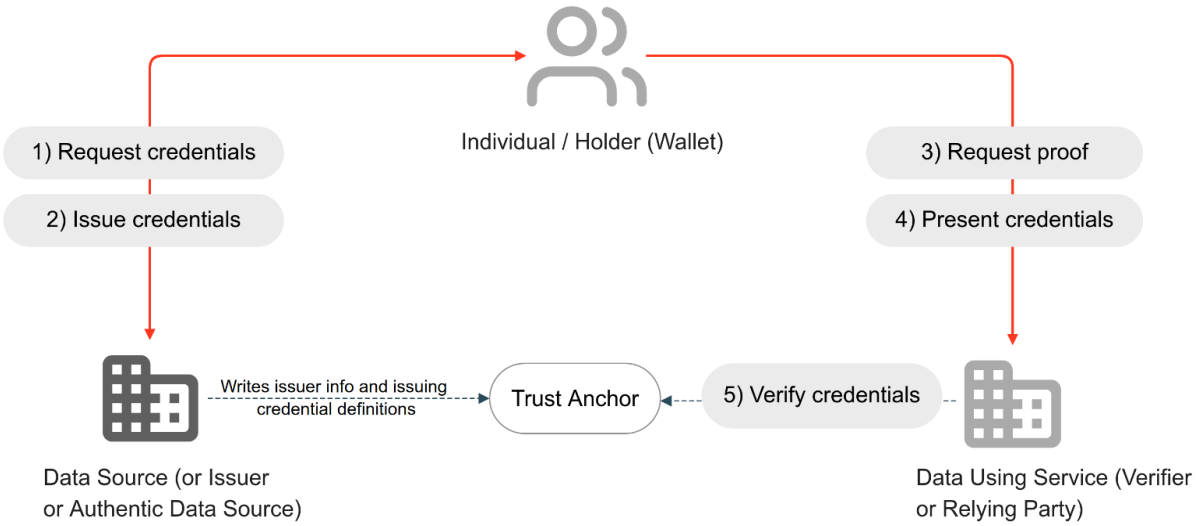

Figure 02: VC workflow for providing access to holder data (with an individual involved in the data exchange transaction in real-time via a digital wallet)

In a VC workflow, illustrated in Figure 02, the ability of the holder wallet to cryptographically bind a credential allows individuals to present their credentials to any verifier directly. Once the issuer registers to the trust registry, when an individual requests a credential (Step 01), the issuer can issue it directly to the individual (Step 02). This is how the physical world has worked for decades. For example, citizens receive their passport or ID card, which they can present to anyone, anywhere, without the need for the verified to have direct access to the original issuer.

When a verifier requests proof (Step 3), for example, proof of identity or proof of any data attribute, the individual concerned presents the credential from their holder wallet to the verifier (Step 4). The verifier can independently verify the proof via the trust anchor, which can be ledger-based or based on an existing PKI infrastructure.

The OID4VCI and OID4VP workflows combine the power of OIDC and leverage existing deployments while being able to adopt powerful, verifiable data exchange mechanisms using verifiable credentials.

4.2 OID4VCI: How does it work?

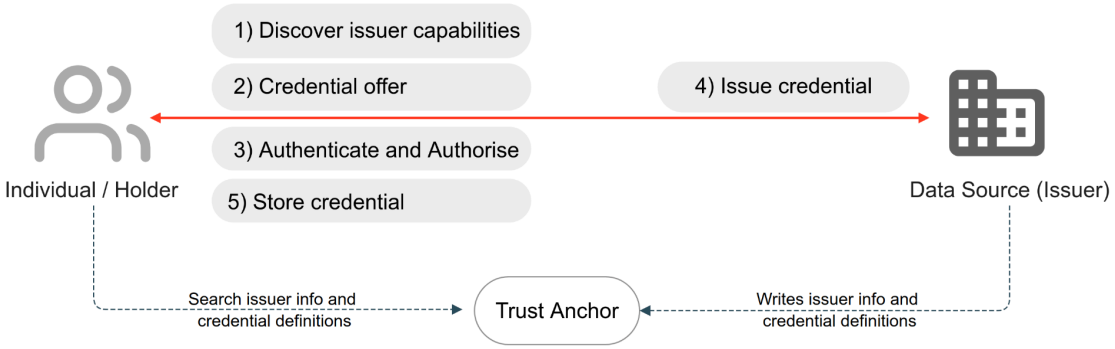

Figure 03: OID4VCI workflow for issuing and storing credentials

The OID4VCI specification defines the APIs that issue verifiable credentials. The issuance involves the following steps. (In brackets, we have used the same term as in the OID4VCI spec chapters 4-7 [4]). These steps are agnostic to any authorisation flow chosen by the issuer (authorised or pre-authorised).

1. Discover VC Issuer capabilities (obtain Credential Issuer's metadata): When an OID4VCI-supported digital wallet client wishes to engage with an issuer, it refers to a well-known configuration as a JSON document, typically hosted at `/.well-known/openid-credential-issuer` URI endpoint on the issuer's domain. This JSON document defines credential issuer metadata, such as credential issuer endpoint, authorisation endpoint, methods, credential endpoint, credential deferred endpoint and other particulars necessary to enable secure, efficient communication and issuance processes between the client and the issuer. Through this standardised issuer discovery technique, the OID4VCI mechanism ensures seamless interoperability. It simplifies the establishment of trust among participants in decentralised identity systems, thereby enhancing user experience and fortifying security across transactions.

2. Credential offer (credential offer endpoint): The credential offer is a cryptographic invitation, typically embedded within a QR code (cross device), an NFC (cross device) or a deeplink (same device), designed to securely convey essential information and directives from the issuer to the holder. This encapsulated data usually includes details about the credential being offered, the issuer's intention, and a callback to the issuer's service endpoints, which will manage the subsequent phases of the credential issuance process.

3. Authenticate and authorise (authorisation endpoint, token endpoint): In OID4VC, the authentication request operates as a pivotal mechanism, anchoring the secure and seamless interaction between the holder, issuer and, potentially, the verifier. This step involves the following substeps:

a. Authorisation request: This is orchestrated by the holder's digital wallet, which communicates with the issuer's authorisation endpoint to initiate the issuance process. This involves initiating an OAuth authorisation request and obtaining an authorisation code from the identity provider (or authorisation server). The authenticate request encapsulates essential parameters such as **`client_id`**, **`response_type`**, and **`scope`**, alongside other parameters that might inform the issuer about the holder's desired credentials and claims. This step is skipped in the pre-authorisation flow as the digital wallet holder already has the authorisation token and may additionally use a user PIN.

b. Token request and response: Once authorised, the digital wallet acquires a valid access token. In the authorisation code flow, the code is exchanged to obtain the access token refresh token pair (as in 3a). In the pre-authorised flow, the token request contains a pre-authorised code and user PIN, which are exchanged to obtain the token response containing the access token and refresh token pair.

4. Issue credential (credential endpoint): The credential endpoint issues a credential the individual/holder requests once a valid access token is presented. The digital wallet client can request the issuance of a credential of a certain type multiple times, e.g., to associate the credential with different public keys/DIDs or to refresh a certain credential. It is also possible to issue multiple credentials within the same request. In that case, it is at the digital wallet client's discretion to decide the order to request the issuance of multiple credentials requested in the authentication request. Credentials can be issued immediately, if available, or after some time using a deferred credential endpoint.

5. Store credential: After the credential has been issued, the individual can store it in their digital wallet client for future verifiable presentations.

4.3 OID4VP: How does it work?

The OID4VP specification [5] defines an extension of OIDC to allow the presentation of claims in various formats, such as W3C VCs.

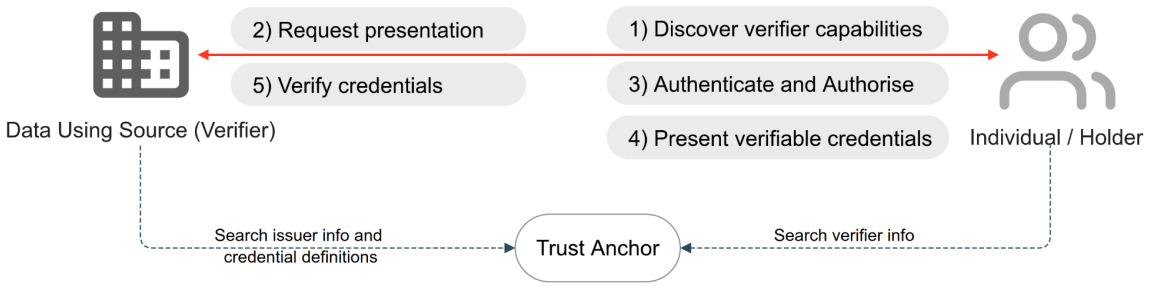

Figure 04: OID4VP workflow for presenting and verifying credentials

The verifiable presentation (VP) involves the following steps:

1. Discover verifier capabilities: This allows for the streamlined discovery of verifier capabilities and configurations through a structured, machine-readable format. It essentially acts as a blueprint that details how digital wallet clients (e.g., holders) should interact with verifiers. Positioned at a well-defined URI endpoint on the verifier's domain, typically under `/.well-known/openid-configuration`, this configuration document is encoded in JSON format and reveals essential information about the verifier.

2. Request presentation: The presentation request, usually encapsulated within a QR code (cross device), NFC device (cross device) or deeplink (same device), is generated by the verifier and contains a structured set of requirements and instructions detailing the specific verifiable credentials or claims sought from the holder. The presentation request is extracted and processed once the individual scans the QR code (or blips the NFC device or clicks the deeplink). The presentation request contains the definition of the presentation by the verifier. For example, a verifier can specify an EU passport attribute as the credential type and a constraint to only select the name of the holder from the credential.

3. Authenticate and authorise: The authorisation request generally encapsulates essential parameters such as `client_id`, `response_type`, and `scope` alongside other parameters that inform the holder about the verifier's desired credentials and claims.

4. Present VCs: A VP is constructed based on the presentation definition shown to the individual for confirmation. Once the individual confirms the data exchange, a `vp_token` is returned to the verifier.

5. Verify credentials: After receiving the `vp_token`, the verifier can cryptographically verify the presentations' authenticity. If the information is present, they can also check a credential's revocation status against a revocation registry.

5.0 Key value of OID4VCI: The path to verified credentials

5.1 OID4VCI: Key values

OID4VCI merges secure, digital ID checks with user-friendly online processes. It brings several essential benefits to digital identity management and user verification in online systems, summarised below:

Increased trust and security: OID4VCI makes digital interactions more secure and trustworthy. Using special digital ID proofs (i.e., VCs), which are hard to fake or alter, ensures that online identity checks are robust and reliable.

User control over identity: It puts users in control of their own digital IDs. People can choose which bits of their identity information to share, ensuring they remain in charge of their personal data when using online services.

Ease of use: OID4VCI combines the safety of VCs with easy-to-use online checks, ensuring that while users enjoy strong and safe ID checks, the experience remains straightforward and friendly. This helps users to get on board easily and continue to use the system without hassle.

High interoperability: It helps different digital systems work together smoothly. Using well-known online check flows (OIDC flows) and combining them with the new technology of VCs ensures that new systems can work well with existing online services and technologies.

Privacy and compliance adherence: OID4VCI helps to protect user privacy and supports rules that let users control their own personal data. Allowing users to choose which identity information to share aligns with laws like the General Data Protection Regulation (GDPR), which focuses on securing data sharing and putting users in charge of their personal information.

5.2 Real-world reference scenario

In the following real-world reference scenario [7][8], illustrated in the figure, we explain the European Social Security Pass (ESSPASS), which aims to simplify how individuals use their social security benefits in EU countries. Here, the issuer is a national social security office that issues ESSPASS PDA1 verifiable credentials to the individual. The individual can present the credentials across the border in Sweden and prove their social status to an inspecting organisation in Sweden. *(**Disclaimer:** ESSPASS PDA1 is only an example of how the workflow could be. The same flow could be applied to any credentials or attestations)*

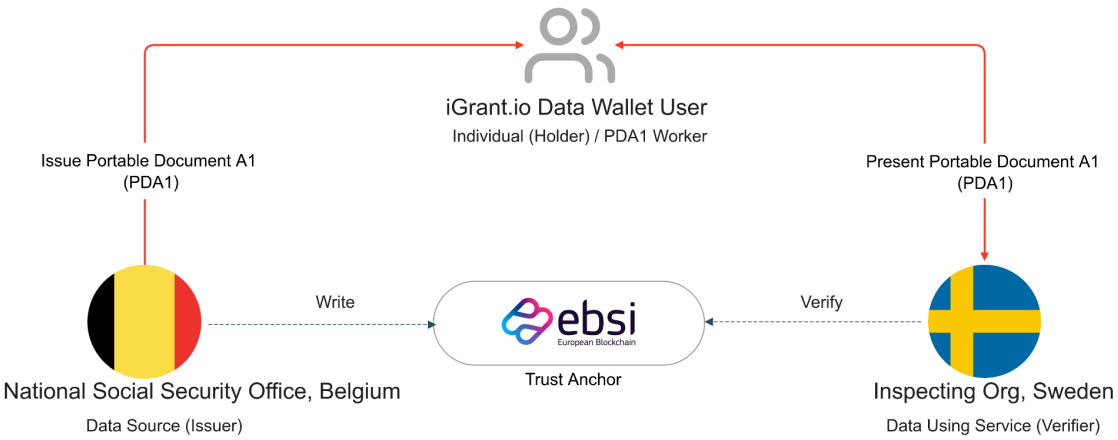

Figure 05: Real-life reference scenario with ESSPASS

The initial stage of ESSPASS focuses on digitally issuing and verifying a portable document A1 (PDA1) [7] that certifies the applicable social security legislation for work in EU member states. Here is how it works:

- Request an ESSPASS - PDA1: An individual verifies their identity and requests the issuance of an ESSPASS - PDA1 as a VC.

- The back office processes the request and issues the individual ESSPASS [7]—PDA1 verifiable credentials, which are then stored in the data wallet.
- Verification: Any third-party organisation needing to confirm the validity of PDA1 credentials can request and verify them against the EBSI trust anchor.

5.3 Reference scenario interactions

Figure 6.0 illustrates the detailed workflow involved in the real-life reference scenario of the National Social Security Office issuing ESSPASS - PDA1 credentials to an individual.

The steps involved in this workflow are:

1. The individual visits the National Social Security Office's webpage and may or may not sign in to their service portal.
2. The individual scans a QR code to request the issuance of a PDA1 document using the digital wallet. Here, the OID4VCI flow is triggered. The issuer can also request additional VCs from the individual during the process. Once identified, a request for the credential issuance is placed with the issuer.
3. The issuer can immediately issue a credential or, after some time (called deferred issuance). Once the credential is received, it is securely stored in the digital wallet for future presentations. The issuer may seek additional verifications as part of an out-of-band KYC process.

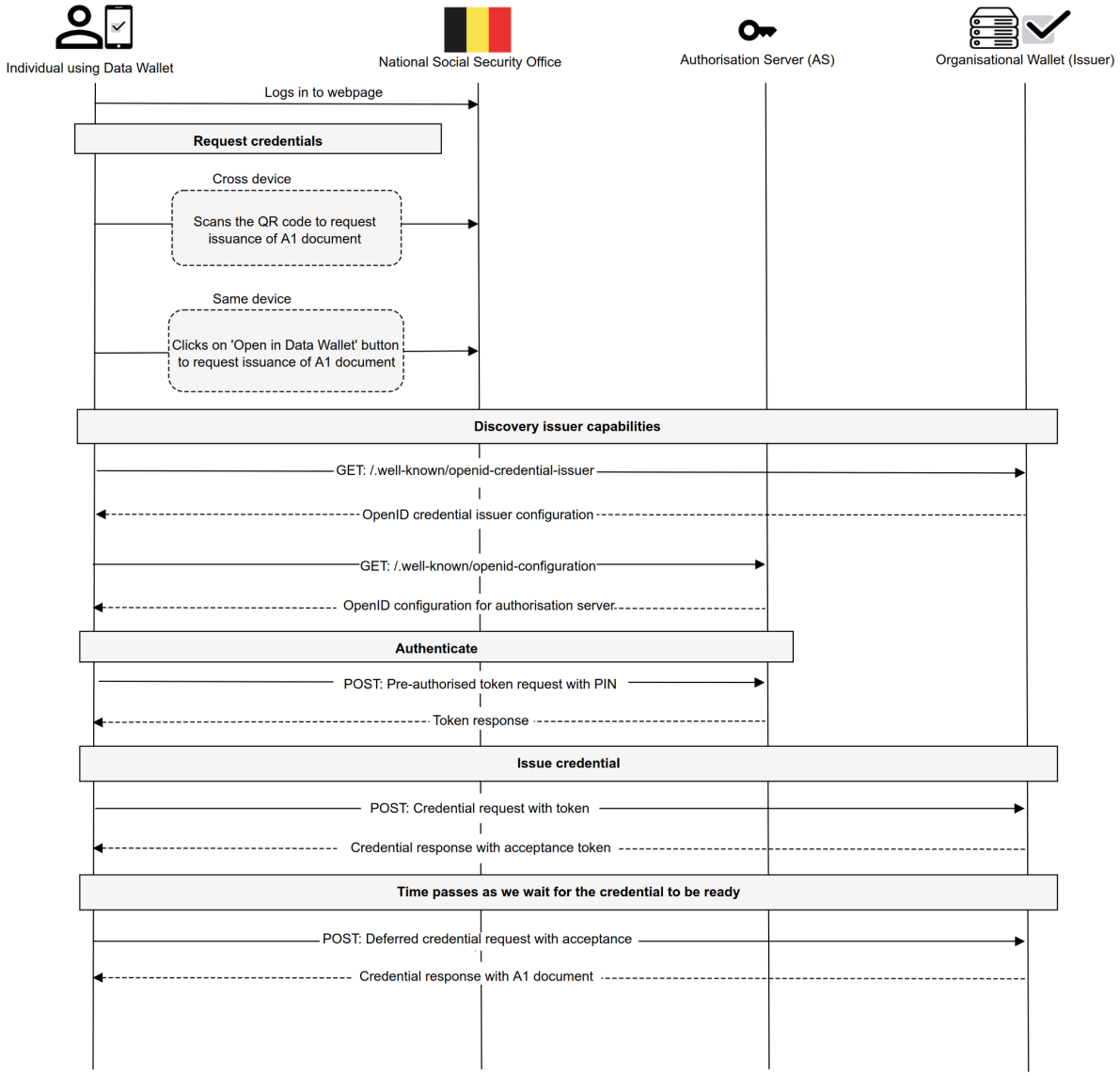

Figure 06: National Social Security office issues ESSPASS - PDA1 credential to Individual

6.0 Key value of OID4VP: The vanguard of privacy-enhanced digital wallets

6.1 OID4VP: Key values

OID4VP combines VP authenticity with OIDC's widely adopted authentication processes. It offers a suite of advantages quintessential for reinforcing digital identity management and user verification.

Enhanced authentication credibility: OID4VP amplifies the credibility of digital interactions by incorporating VPs, which serve as reliable and cryptographic confirmations of digital identity. This strengthens the authentication procedure and ensures the user verification process is secure and reliable.

User-oriented identity management: The protocol allows users to control their digital identity. By enabling users to present their VPs selectively, OID4VP ensures that users can govern the granularity and scope of their shared identity information during the authentication process.

Smooth user interface: Despite its sophisticated underpinning, OID4VP is crafted to offer a smooth and user-friendly interaction. By combining the security facets of VPs with a straightforward authentication process, OID4VP ensures a simplified user journey.

Comprehensive interoperability: OID4VP enables interoperability by combining traditional OIDC workflows with the innovative use of VPs. This combination ensures that OID4VP can be synergistically integrated into existing OIDC-compliant systems, bridging the gap between conventional and contemporary identity technologies.

Privacy and compliance adherence: Emphasising user privacy, OID4VP facilitates a model where users can directly present their VPs to a relying party, minimising unnecessary data disclosure and thereby complying with regulations like the GDPR.

6.2 Real-world reference scenario

In the following reference scenario [7][8][9], we explain that the inspecting organisation verifies the A1 certificate, a form used to confirm the country where an employee or visitor currently pays their social security contributions. Here is how it works:

- Request verification: An individual presents the ESSPASS/PDA1 VC to the verifier.
- The back office checks the VCs inside the presentation and confirms the validity against a trust anchor.

6.3 Reference scenario interactions

Figure 7.0 illustrates the detailed workflow involved in the real-life reference scenario of an inspecting organisation verifying an individual's ESSPASS—PDA1 credential.

The steps involved in this workflow are:

1. The individual visits the inspecting organisation's webpage and may or may not sign in to their service portal.
2. Scan a QR code or click a link to obtain the presentation request.
3. Once the presentation request is received, the individual can verify who they are to the verifier.
4. A digital wallet lets the individual see the credentials the verifier requests. They can then present the credentials of their choosing towards the verifier.

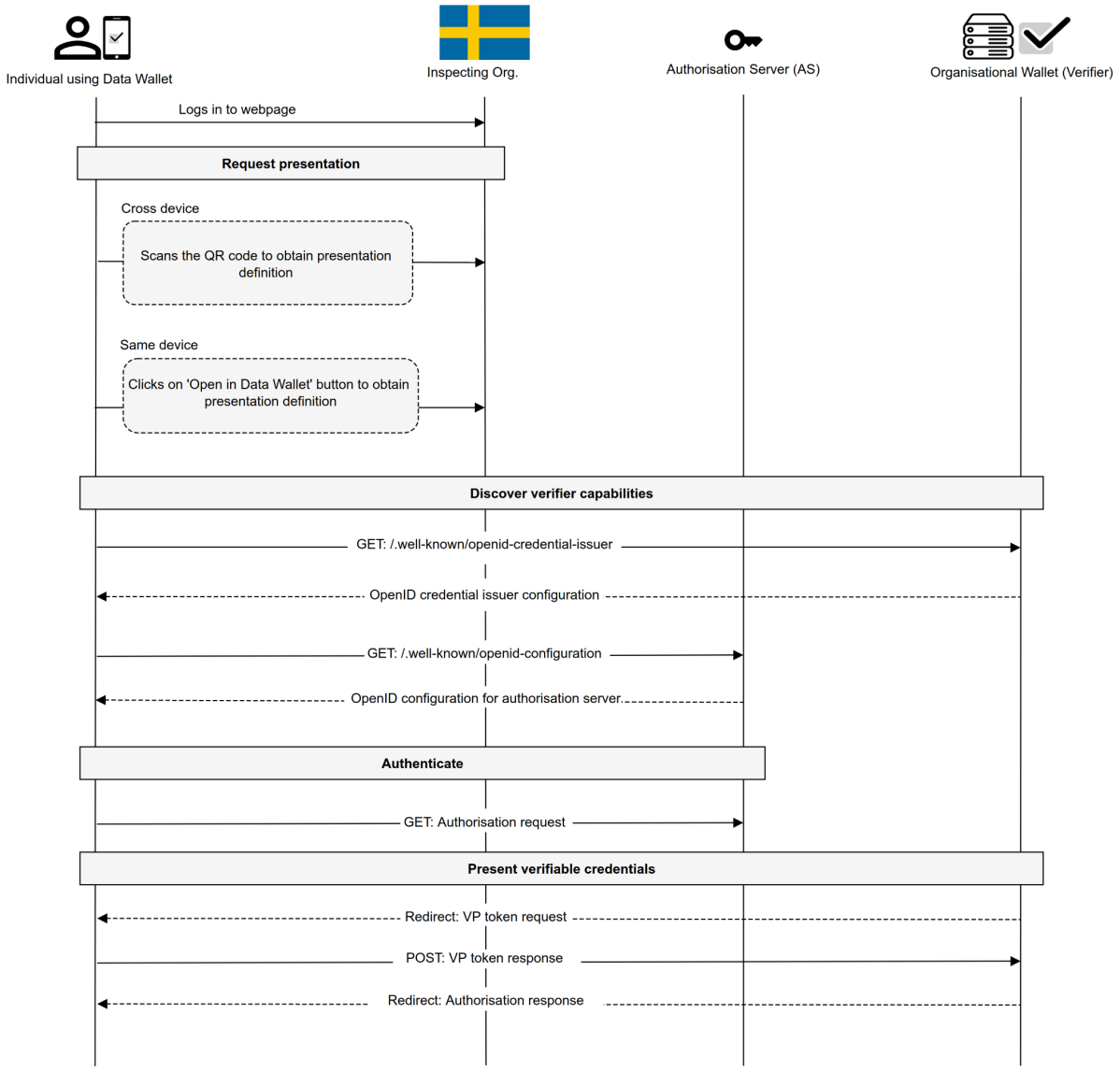

Figure 07: Inspecting organisation verifies ESSPASS - PDA1 credential from an individual

7.0 Bridging to legacy eIDAS systems and SAML

The ARF [2] and new eIDAS regulation [10][14] leans on OpenID-based protocols. However, to ensure interoperability and compatibility of EUDI Wallets with older eIDAS systems, it is essential to map the concepts of SAML [5] to OID4VCI and OID4VP and vice versa. This is also in line with the eIDAS regulation that requires the creation of minimum technical specifications, standards and procedures for the interoperability framework. This chapter provides an introductory mapping of SAML to OID4VCI and OID4VP to SAML. Fortunately, translating between SAML and OIDC is straightforward in most areas. Below are some considerations.

7.1 Authentication workflow

The eIDAS specifications [12][13] discuss the use of specific authentication messages (the authorisation request and response). These messages are relayed primarily using the HTTP POST method. This setup is reminiscent of certain flows in OIDC and SIOPv2. While most of the mapping is straightforward, the latest OID4VCI version presents some complications.

For example, the authorisation request contains the following parameters:

- User authentication type, identification scheme, minimum level of assurance (LoA),
- Identifiers of requested attributes.

The authorisation response contains the following parameters:

- User authentication type
- Retrieved values for the requested attributes.

This 'one-step' request/response flow is similar to that described by OIDC or SIOPv2 (`response_type=id_token`). The OID4VP also supports implicit flow but requires an additional data structure (`response_type=vp_token`). The OID4VCI does not help implicit flow; it describes just authorisation code flow and pre-authorized code flow (`response_type=code`), but both are 'two-step' flows that differ from the 'one-step' flow of legacy eIDAS systems.

Mapping from SAML to OIDC, SIOPv2, or even OID4VP does not require modifications in the communication flow of legacy eIDAS systems, but supporting the current version of OID4VCI is a problem.

7.2 Security: Signatures and encryption

The eIDAS specifications emphasise the importance of security, requiring signatures for authentication requests and both signatures and encryption for responses. While XML-based messages were previously the norm, they are now transitioning to JSON-based ones.

However, the order in which encryption and signatures are applied differs between the old and new systems. For instance, the eIDAS-focused SAML encrypts data before signing the entire message. In contrast, OIDC signs first before encrypting. Both methods have merits, but harmonising them is crucial for maintaining security during the transition.

Mapping from SAML to OIDC, SIOPv2, OID4VP, or OID4VCI requires signature and encryption mechanism modifications. Legacy eIDAS systems and EUDI Wallet, as per eIDAS-2.0, shall have a common method for applying security layers such as sign-then-encrypt-then-sign.

7.3 Passing parameters

Legacy eIDAS details how parameters should be passed through HTTP Redirect or HTTP POST. The method used often depends on the message's size. However, newer systems like OID4VP and SIOPv2 have different size limits, especially when considering QR code uses, where size constraints are more pronounced. Transitioning might require using HTTP POST more extensively, especially when URLs become too lengthy.

8.0 EUDI Wallets: Pioneering the future of digital identity

As explored in this paper, the convergence of EUDI Wallets with OID4VCI and OID4VP represents a transformative leap forward in digital identity and personal data protection. Integrating advanced technologies like SD-JWT instead of simply JWTs in a typical OIDC flow and ZKPs could enhance these solutions towards enhanced end-user privacy and control.

EUDI Wallets, in collaboration with OID4VC, OID4VP, SD-JWT and ZKP, herald a new era in digital identity management - one in which individuals are empowered, data is fortified and privacy is preserved. As these technologies become more integrated into our digital lives, we move closer to a future where the benefits of a connected world can be realised without compromising our personal information and digital sovereignty. The future of digital identity and personal data protection has arrived, and it is both promising and secure!

References

1) OpenID Foundation (2022), ‘OpenID for Verifiable Credentials - Overview’, Available at: https://openid.net/sg/openid4vc/ (Accessed: October 01, 2023)

2) European Commission (2023) The European Digital Identity Wallet Architecture and Reference Framework (2023-04, v1.1.0) [Online]. Available at: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases (Accessed: October 16, 2023).

3) OpenID Foundation (2023), 'Self-Issued OpenID Provider v2 (SIOP v2)', Available at: https://openid.net/specs/openid-connect-self-issued-v2-1_0.html (Accessed: October 01, 2023)

4) OpenID Foundation (2023), 'OpenID for Verifiable Credential Issuance (OID4VCI)', Available at: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-11.html (Accessed: October 02, 2023).

5) OpenID Foundation (2023) 'OpenID for Verifiable Presentation (OIDC4VP)', Available at: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html (Accessed: 02 October 2023).

6) Decentralized Identity Foundation (2022), ‘Self-Issued OpenID Connect Provider DID Profile v0.1 (DEPRECATED)’, Available at https://identity.foundation/did-siop/ (Accessed: 21 October 2023)

7) European Commission (2022) 'European Social Security Pass', Available at: https://ec.europa.eu/social/main.jsp?catId=1545&langId=en (Accessed: 10 October 2023).

8) iGrant.io (2023) 'ESSPASS PDA1 reference scenario', Available at: https://igrant.io/ebsi.html (Accessed: 02 October 2023).

9) iGrant.io (2023) 'ESSPASS: Transforming social security rights with OID4VC and OID4VP in digital wallets', YouTube video, Available at: https://youtu.be/b-dTpMbxHPU (Accessed: October 12, 2023).

10) European Commission (2014) Regulation (EU) No 910/2014 of the European Parliament and of the Council, Official Journal of the European Union, L 257/73. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910 (Accessed: 12 October 2023).

11) Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 (2005-03-15) http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf (Accessed: October 16, 2023).

12) European Commission (2016) eIDAS Technical Specifications, based on Opinion No. 1/2016 and CIR (EU) 2015/1501 (2016-01-26, v1.0) https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+eID+Profile (Accessed: October 16, 2023).

13) European Commission (2023) eIDAS Technical Specifications, based on Opinion No. 3/2023 and CIR (EU) 2015/1501 (2023-04-24, v1.3) https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+eID+Profile (Accessed: October 16, 2023).

14) European Commission, 2021. Proposal for a Regulation of the European Parliament and of the Council of amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281 (Accessed on: 6 November 2023)