Technical Overview

13 March 2025

Technical Overview

Table of Contents

SIROS Foundation

SIROS Foundation is a new non-profit organisation established in December 2024, headquartered in Stockholm, Sweden, with a mission to provide the next-generation digital identity platform for the Internet. Our solution builds on the wwWallet project, an open-source project initiated by GUnet, Sunet, and Yubico. Our unique Internet-first approach relies on open standards, including FIDO Passkeys for strong authentication, OpenID and ISO/IEC 18013-5 as identity protocols, and eIDAS 2.0 as a regulatory framework in the EU. Watch the demo video for the Funke German ID wallet competition.

Strongest security

By building on FIDO Passkeys, integrated into all leading platforms and browsers, our solution offers phishing-resistant end-to-end security, no single point of failure, a minimum attack surface, and a path to obtain eIDAS HIGH assurance certification. The user can combine syncable Passkeys, integrated directly into computers and phones, with physical hardware Passkeys, enabling a wide range of security requirements and scenarios.

Best level of privacy

Our solution never collects user data in any form. Using FIDO passkeys, all user data is encrypted with a key only the user can control. The user's data cannot be shared with anyone unless the user has given their explicit permission. There are no backdoors, and it is possible for the user to protect their data from the mobile platform. Also, we are working to support zero-knowledge-proof (ZKP) technology with FIDO Passkeys.

Easy to use

Our solution offers unprecedented usability improvements over all alternatives by combining native platform support for FIDO passkeys with complete encrypted data portability across all devices. We can provide solutions for shared devices, legal entities, and representation, a solution for phone-restricted areas, disaster and emergency services, and a fully customisable user interface.

Cost efficiency

Based on free and open-source software, our solution has no proprietary technology and relies only on standardised web and Internet technologies. Using FIDO passkeys makes backup hardware affordable, minimising account recovery and support costs. By relying entirely on standardised web technologies, we can deploy our solution without requiring web or app downloads. Building on open standards, we create a marketplace where credential issuers, identity providers, relying parties, integrators, and hardware authentication vendors compete and develop value-added services.

About us

We are an international team of cybersecurity and digital identity experts. Our board consists of Stina Ehrensvärd, Leif Johansson, Nat Sakimura, and Ruth Puente. SIROS is an acronym for *Secure Identity Research Organisations*. The name is also inspired by *Sirius*, the brightest star in the night sky, and our goal is to help Internet users navigate their digital journey. Committed to the word *serious,* we will help ensure long-term security, viability, stability, and privacy for frictionless, borderless digital identity for all.

Documentation Summary

In this whitepaper, we will describe how the wwWallet application (referred to in this paper as just the wwWallet) works and the ecosystem that wwWallet project is a part of. Several countries and verticals have developed identity platforms in recent years that may appear quite similar to SIROS; we will show just how different our approach is and why betting on SIROS is the right choice for the future.

SIROS Foundation is supporting the development of the open-source wwWallet project. GUnet initiated the development in 2022 (a Greek government agency providing IT infrastructure for higher education). The goal was to provide a web-based alternative to digital wallets independent of mobile platforms. In 2023 and 2024, the project was further developed as a collaboration between GUnet, Sunet (a sister organisation in Sweden), and Swedish authentication innovation company Yubico, including adding support for the FIDO/Passkeys strong authentication standard. The project and software code is hosted on GitHub under an open-source licence.

The wwWallet and all its associated technology are not and will not be dependent on any single commercial company in the future. As an independent and non-profit entity, our goal is to preserve user security and privacy and serve as a bridge between large platform providers, security companies, and EU regulators. SIROS and Yubico are committed to the future development and integration of the FIDO Passkey ecosystem and the EUDI wallet, which we believe will provide an open and secure anchor for the EUDI wallet ecosystem.

The SIROS Technical Architecture

The SIROS architecture is an example of a *direct presentation flow* identity architecture, sometimes also known as an “identity wallet” architecture, in which an entity (typically an organisation or a company) that holds information about users issues digitally signed *credentials*. The user can then, at their discretion, share information gleaned from those credentials with a service provider, which in exchange, provides some form of personalised service to the user based on the information received.

The architecture rests on two main security promises, namely that the information conveyed to the service provider is both correct and unchanged as it is conveyed to the service provider.

In the physical world, we are used to receiving some information, possibly printed on paper or plastic and protected from forgery, that we display at some later point. Things like hotel keys, driver’s licences, movie tickets, and passports are examples with varying degrees of value to the owner.

The purpose of direct presentation flow architecture and of SIROS is to enable such use cases to move into the digital domain, putting the user in control with as much flexibility and as little friction as possible.

The basic flow can be illustrated like this:

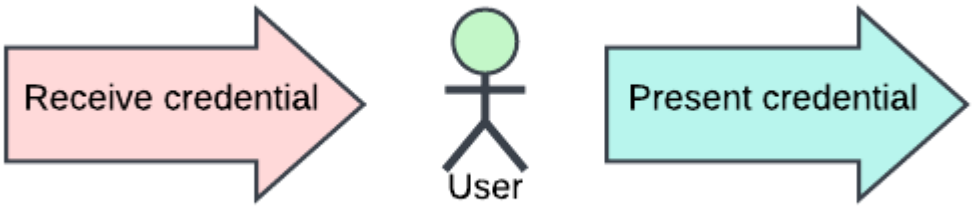


Figure 1: Basic Credential Flow

The user receives and stores digital credentials in a piece of software that is often called a *digital identity wallet*. The term *identity wallet* can be misleading because it suggests that the user is somehow engaged in a payment transaction when sharing information with services or that the digital credentials are fungible objects akin to credit cards. This is not the case in most situations and we avoid this terminology whenever possible.

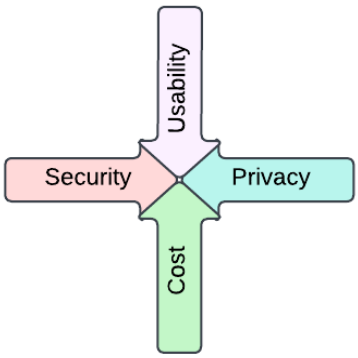
Instead, we refer to the user as the *holder* of digital credentials. We will also use the term holder to refer to the software used by the user to receive, store, and *present* digital credentials.

We follow the standard terminology for direct presentation flow architectures and use the term *credential issuer* to denote the entity that provides credentials to users. Similarly, we use the term *credential presentation* to denote the process by which the holder sends credential information to the service provider. The service provider is sometimes also referred to as a *verifier*.

Digital credentials are meant to mimic well-known flows in the physical world such as having a driver's licence, a library card, a university diploma, or the licence to operate a forklift or to practice medicine.

The goal of the SIROS technical architecture is to establish online solutions that allow us to establish counterparts to these well-known artefacts from the physical world while enabling the development of completely new use cases. We critically need to achieve these goals without endangering individuals' safety and privacy.

Four parameters must be optimized to achieve this goal: **security, privacy, usability, and cost**.



The system must be secure in the sense that it is hard to attack. The privacy of the users must be ensured in order to establish faith and trust in the ecosystem by the user.

The system must also be easy to use or users will simply not use it. It must also be easy to integrate with services. Finally, the whole thing must be highly cost-efficient for all parties.

We believe that the SIROS approach is the most secure, privacy-preserving, user-friendly, and cost-effective approach to third-party presentation flow possible. We also believe that in order to maintain these properties, the wwWallet must develop as part of an open standards and open-source ecosystem.

Open Standards

We believe in open standards and open source. Our core infrastructure is based on these open standards:

- FIDO passkeys[1],[2] ensure that our solution has the best possible security, privacy, and usability. Passkeys are universally available and unlike solutions that rely only on mobile platforms, our solution can work in phone-restricted environments.
- Our main user interface is a progressive web application that relies on W3C web specifications, ensuring maximum usability and deployability. We are a web-first solution for digital identity.
- Multiple credential formats are supported, including Selective Disclosure JSON Web Tokens (SD-JWTs) and ISO/IEC-defined mdocs.
- Interfaces for service providers and issuers are based on industry-standard OpenID[3] and ISO/IEC 18013-5[4] protocols. These standards are fully compliant with the EU eIDAS implementing acts and emerging specifications.

Security and Privacy

Security means many things. When we talk about security in the SIROS architecture, we mean the ability to protect the user and the services, issuers, and other components in the ecosystem from online attacks. Sometimes, security is a goal that is hard to combine with privacy, but we believe that in the digital identity world, security is both possible and necessary to align with privacy.

In the physical world, it is possible to borrow somebody's driver's licence and present it as one's own, but unless your appearance resembles the photo on the driver's licence, this will probably not yield the desired result.

It is possible to borrow *some* forms of credentials; a non-personalised ticket, such as a movie ticket, for instance, is not tied to any person, and anyone in possession of the ticket can present it at the movie theatre. This is not a huge problem in the physical world since people rarely try to forge and duplicate low-value credentials such as movie tickets.

In the digital world, however, we try to avoid creating confusion about whose credential is being presented and who is vouching for its authenticity. Such problems are often much more challenging in the digital domain than in the physical world, partly because it is much easier to duplicate digital objects than it is to duplicate credentials in the physical world.

The service looks for two key properties when receiving a digital credential: First, that the credential is authentic, and second, that the credential actually belongs to the user. The authenticity of the credential is ensured by the signature from the credential issuer, which means that the service must have some way to trust the credential issuer. The fact that the credential

[1] W3C WebAuthn Community Adoption Group and FIDO Alliance. 2025. "Terms." Passkeys.Dev. January 6, 2025. https://passkeys.dev/docs/reference/terms/#passkey.

[2] Cappalli, Tim, Michael Jones, Akshay Kumar, Emil Lundberg, and Matthew Miller, eds. 2025. "Web Authentication: An API for Accessing Public Key Credentials Level 3." Editor's Draft, March 12, 2025. https://w3c.github.io/webauthn/#passkey.

[3] Openid. 2025. "OpenID for Verifiable Credentials - OpenID Foundation." OpenID Foundation - Helping People Assert Their Identity Wherever They Choose. February 18, 2025. https://openid.net/openid4vc/.

[4] "ISO/IEC 18013-5:2021." 2021. ISO. 2021. https://www.iso.org/standard/69084.html.

belongs to the user is ensured by a property called *holder binding*, which is a digital signature that proves to the service provider that the credential has been under the holder's control ever since it was issued to the holder by the credential issuer.

To ensure the issuer's security promise to the service provider, the holder doesn't simply send the credential to the service provider but rather generates a new digitally signed object that contains both the digital signature binding the holder to the credential and the digital signature authenticating the credential by the credential issuer. This new object is called a *credential presentation*.

In many situations, the service provider also doesn't need all the information present in the credential. In the SIROS architecture, the holder implements something often called *selective disclosure*, which means that the holder allows the user, in conjunction with policy imposed by the credential issuer, to choose a subset of the information available in the credential(s) to present to the service provider. The precise nature of the credential and the policy governing the issuer and service provider will determine exactly how the user can choose this subset.

Selective disclosure is key to ensuring privacy: the user is fundamentally in control of the digital credentials and is always, at some level, involved in the decision to generate and present a cryptographic proof of the credential to the service provider. Legal and regulatory limitations will sometimes limit what the user is able to control and there are situations where the user is compelled to present all the information in a digital credential (e.g., when showing your driver's licence to the police), but in many situations, the user can and must be allowed control over what information to share.
Holder privacy is the ultimate goal of the wwWallet project and the core principle behind the direct presentation flow architecture. Privacy in the context of the identity holder encompasses a broad range of design considerations, and it remains a work in progress, particularly when viewed through the lens of post-quantum cryptography and Zero-Knowledge Proof (ZKP).
In its current version, the wwWallet ensures privacy by generating unique, unrelated key pairs for each verifier at which a credential is presented. This ensures that cryptographic keys do not compromise unlinkability, preventing tracking by relying parties, provided the holder does not use the same credential instance for multiple presentations. It also supports selective disclosure mechanisms, enabling it to be used.

Usability and Cost

Usability is a form of cost. Bad usability incurs costs in the form of wasted time for users as well as direct support costs for all parties in the ecosystem: Confused users either abandon a tool or seek help. Since the flows in the direct presentation architecture are inherently complex, users will often seek help from the wrong party, which leads to even higher support costs. They may also say negative things about their experience to others.

Selective disclosure is critical to achieving user control and privacy. That said, it is also one of the most challenging usability issues in the ecosystem simply because of the volume of credentials the user can choose from to complete a transaction with a service provider. In order to fulfil the requirements of data minimisation and privacy by design that is at the heart of most modern privacy legislation, the service provider will request only the minimum data necessary to provide service.

Furthermore, a given credential is useful in some but not all circumstances. For instance, a driver's licence doesn't make sense when borrowing a book at the library. The credential issuer knows what context a service belongs to and what regulatory constraints may apply. The service provider and the technical platform must, in turn, be able to convey that information to the

application managing the credentials on behalf of the issuer so that the user can be presented with reasonable choices tailored to the situation.

Ultimately, the user app will be responsible for helping the user choose from among all the available credentials in order to fulfil the service provider's request. Consider, for instance, a service provider that needs to know that the user is of legal age to buy and consume alcohol. The user may have more than one credential with an authenticated birth date in it. However, even if the driver's licence is the only credential the user can choose, the user still needs help to avoid accidentally sharing their home address along with their birthday.

The holder app must obtain information from the credential issuer and service provider about the legal and business context that applies to the given application as part of the trust model for the ecosystem in order to produce a UX that adapts to each situation. This approach also means that the holder app, in some limited form, becomes a trusted extension of the credential issuer and service provider as well as a tool for the user.

Usability is, of course, not the only consideration; when deploying direct presentation flow for a particular use case, you also need to consider direct costs such as the costs of strong authentication, service integration, support, etc. All of these costs are, to some extent, unavoidable but can be minimised by relying on open standards and open source as much as possible. Open standards lower costs by increasing competition; open source lowers costs by making it possible to build solutions without incurring direct licencing costs.

The wwWallet Application

The holder in the SIROS technical architecture is called 'wwWallet' and consists of all the components required to operate a digital identity "wallet" according to the EU ID regulation. Use of the wwWallet is not limited to the European jurisdiction, however, and can easily adapt to a wide range of jurisdictions and use cases. We have chosen to base our design on the fundamental principles of the Internet: open, permissionless innovation within the confines of a technical framework that ensures essential interoperability.

The wwWallet application is based on the wwWallet open source project, whichYubico, Sunet, and GUnet started as part of the EU ID large-scale pilot projects DC4EU and EWC. The wwWallet project is, at its heart, a progressive web application that is also provided as a native application for major mobile platforms.

In many situations, the progressive web application is all that is needed; users can use most features of a digital credentials ecosystem without downloading a new app. The wwWallet can be deployed easily in situations where traditional "native" mobile apps are not possible to use, such as where phone use is restricted or where connectivity is restricted to wired networks. Users do not need to have access to a phone to use the wwWallet. The only requirement is that the user has access to a FIDO passkey that supports the FIDO/WebAuthn psuedo-random function (PRF) extension, which enables symmetric key data encryption using a FIDO security key. All major platforms and several leading hardware FIDO key manufacturers support this extension.

A security key with the PRF extension in the hands of the user is all that is needed for the user to access their wwWallet online **from any browser**. We will talk about some use cases where this radical approach to data mobility becomes important, but one immediate consequence is that **any user can use any device** as long as their FIDO passkey is available. Unlike many similar solutions and technology stacks, the wwWallet project supports full data portability out of the box. Another consequence is that SIROS already has a solution for the backup of data: If you choose to use the wwWallet with a phone, you don't have to worry about losing your phone.

Your wwWallet is automatically on your new phone or in your desktop browser whenever and wherever you present your FIDO passkey.

Another consequence of using symmetric encryption of all user data is that no data is available to anyone other than the user. There are no backdoors to the data stored in wwWallet instances, and unless the user uses their FIDO security key or passkey, the data belonging to the user remains encrypted, protected, and impossible to access for anyone other than the user.

This user-focused design is a fundamental difference between SIROS and similar solutions where the keys that are used to protect the user's information are often stored in some server online and protected only by the goodwill of the service owner. In the SIROS case, the protection is built into the fabric of the wwWallet project using FIDO tokens.

There is no concept of an "account" in wwWallet. No information about the user other than the public keys of the FIDO tokens is ever stored outside the protection of the FIDO encryption. When signing up to use the wwWallet, the user is not asked to provide a name, username and password, e-mail address, or anything else that could be used to identify the user. The only thing the app will ever ask for is a FIDO passkey. In the terminology of the EU ID ecosystem, the FIDO passkey is the Wallet Security Cryptographic Device (WSCD) of the wwWallet *wallet instance*.

Every bit of personal information that the user stores in their wwWallet is in the form of a digital credential provided by some issuer and every digital credential in wwWallet is encrypted with the FIDO passkey that the user controls.

The wwWallet relies on several standard libraries and will, as part of the proposed project, integrate support for ISO/IEC 18013-5 based on the official reference implementation. The wwWallet relies on standard progressive web application technology (PWA), and the native application versions of the wwWallet are based on the same UX/UI solution. This means that the wwWallet is easy to customise and white-label and that parts of the wwWallet could potentially be integrated into other applications.

The design for the specific platforms can be easily adapted to support the platform-specific design guidelines, such as the respective ones for the Android or iOS apps, as well as other guidelines, such as Web Content Accessibility Guidelines (WCAG). The wwWallet is both a PWA web application and, based on the PWA core, supports native apps for both Android and iOS within a unified UX framework. Settings and controls are therefore presented in a uniform fashion, and users recognise themselves regardless of which platform they are using.

This design approach also makes it easy to move between different platforms; for instance, it is possible and easy to use the native app to establish an age credential by reading a passport and then use the web version (e.g., at a kiosk) to access the same credentials based on having access to the user's FIDO token.

The wwWallet interfaces with issuers using OpenID4VCI and with service providers (verifiers) using either OpenID4VP or ISO/IEC 18013-5. These open, internationally recognised standards form the basis for most large-scale deployments of the direct presentation flow architecture, including eIDAS.

Digital Trust

Another important consideration for the architecture is the trust model. The trust model is fundamentally about technical solutions for representing business relationships. Trusting an

entity in the digital domain means that you are willing to engage in some exchange of information with that entity and rely on the information you receive.

There are two main aspects to digital trust related to digital credentials. Firstly, the issuer has to trust the service provider (verifier) to adhere to rules and legal requirements governing the use of credentials. Secondly, the service provider has to trust the issuer to provide accurate information in digital credentials. Since the credential issuer is decoupled from the service provider, the holder has to, to some extent, be part of the chain of trust.

The holder acts as an agent of the user in the sense that it only shares information from credentials when the user chooses to interact with a service provider, but the holder also represents the legitimate requirement of the service provider to adhere to the legal requirements that may apply to the credentials. For instance, when the police request to see your driver's licence it is illegal to attempt to hide parts of your driver's licence from the police. In this case, selective disclosure is not fully at the user's discretion, and in the interest of providing good UX, the holder application should probably not even offer the user the option of making the wrong choice. However, when using a driver's licence to prove your age, it makes perfect sense for the user to fully control what information to share.

Initially, the wwWallet will operate using a simple trust model based on a trusted list of issuers. We are currently developing a trust model for service providers that will initially be based on registration in a trusted list. In time, we may employ more dynamic solutions for trust management, such as OpenID Federation or other technologies that follow the basic model of the open, permissionless innovation of the Internet.

We follow the principle of making the simple easy and the complex possible. The SIROS holder app will, in addition to policy controls put in place by the jurisdiction we operate in (such as the EU eIDAS framework), support a set of simple modalities for enhancing the user experience based on the policy provided by the issuer, service provider or jurisdiction:

- **Required:** Credential presentation where the regulatory framework requires the user to preset a certain set of information to the service provider. This will be limited to clearly defined legal requirements.
- **Anonymous:** When the user presents only a single non-personal property such as legal age, human status (the user is a human user), or citizenship; no other information is conveyed to the service provider.
- **Conditional:** Where the service provider asks the user to present a well-defined set of information regulated by a third-party trust framework to which the service provider belongs. This will be limited to recognised bona fide trust frameworks.

The wwWallet will always clearly signal to the user which of these three modalities is in operation.

Credential Formats and Signing Schemes

The wwWallet can be adapted to support multiple credential formats and signing schemes. The current codebase supports SD-JWT and credentials that use batch-issuance as a mechanism for partial unlinkability, but as part of the current proposal, the wwWallet project will develop support for additional credential formats, including JSON Web Proofs (JWP) and BBS signatures based on Lehman et al.[5], which will provide a full ZKP solution for age verification.

[5] Lehmann, Anja. n.d. "Publications." Hasso-Plattner-Institut. https://hpi.de/lehmann/publications.html.

Anticipating that the verifiers will need some time to implement JWP-based credentials and BBS Signature verification, the wwWallet project will continue to support SD-JWT and mdoc-based credentials in parallel with newer ZKP-based credentials.

For signing in to the wallet, the wwWallet uses WebAuth for strong, phishing-resistant authentication. This enables a high Level of Assurance (LoA) for this authentication stage, thanks to WebAuthn's authenticator attestation feature. During WebAuthn credential registration, the wwWallet can enforce a policy on what kinds of authenticators are acceptable. The newly created credential may then include cryptographic proof that an authenticator of an approved model holds the WebAuthn credential private key. This proof enables the wallet provider to ensure that users' authenticators satisfy the requirements of LoA High.
Cryptographic functions required for device binding and end-to-end encryption of the content stored in the wwWallet, including all proof signing keys, are performed on the client side. This is achieved using keys derived via the WebAuthn PRF extension. The encryption keys are not sent to the server, so users' proof signing keys are secure against a breach of the server side. Once the user is authenticated using WebAuthn, the user can download their encrypted wallet contents and decrypt them on the client side.
The currently used WebAuthn PRF extension only enables derivation of software keys, so the wwWallet does not currently achieve LoA High for (Q)EAA proof signing keys. To achieve LoA High, the wwWallet project's roadmap includes plans to implement newer proposed WebAuthn and Client to Authenticator Protocol v.2 (CTAP2) extensions.[6] These extensions would enable the wwWallet to generate hardware-bound asymmetric key pairs, whose public keys can be tied as proof keys during credential issuance, while the private keys never leave the secure element of the WebAuthn authenticator. During credential presentation, the wwWallet would invoke WebAuthn with the extension to have the WebAuthn authenticator sign the presentation with the hardware-bound private key. This would ensure the user has sole control of their Qualified Electronic Attestations of Attributes (QEAA) proof keys, even if encryption keys are compromised.

Future versions of the wwWallet will include support for credential presentation based on BBS Signatures combined with zero-knowledge range proofs. BBS Signatures are a multi-message digital signature scheme, supporting unlinkable Verifiable Presentations (VPs) based on Zero-Knowledge Proofs of possession of a valid signature over a vector of signed messages (attributes) while selectively disclosing any (possibly empty) subset of those messages. Range proofs are Zero-Knowledge Proofs of possession of an attribute that lies within some range. Range proofs will not only allow for high privacy guarantees but also for flexible deployments since the specific range can be adjusted on a per VP basis (i.e., to account for different minimum legal drinking age across EU countries, etc.).

There are many proposed constructions of range proofs, with the more prevalent ones being bulletproofs [Bunz et al., 2018][7] and schemes based on hiding polynomial commitment [Boneh et al., 2020][8]. These protocols work by providing a commitment to a secret value to the verifier and then proving knowledge of that value as well as that it lies within the specified range. We can easily extend the above protocol to prove that the secret value behind the commitment is the age attribute of a JWP credential signed with BBS Signatures (i.e., that the committed secret value is also signed by the BBS Signature in a predefined position for the age attribute). We will examine the different range-proof approaches on the basis of performance (targeting constructions optimised for relatively small ranges), usability (i.e., solutions that do not require

[6] W3C. 28 May 2024. "Add 'Sign' Extension by Emlun · Pull Request #2078 · W3C/Webauthn." GitHub. https://github.com/w3c/webauthn/pull/2078.
[7] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille and G. Maxwell, "Bulletproofs: Short Proofs for Confidential Transactions and More," *2018 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2018, pp. 315-334, doi: 10.1109/SP.2018.00020.
[8] Boneh, Dan, Ben Fisch, Ariel Gabizon, and Zac Williamson. 2020. "A Simple Range Proof From Polynomial Commitments - HackMD." HackMD. February 20, 2020. https://hackmd.io/@dabo/B1U4kx8XI.

complicated or trusted setups), and extensibility (i.e., solutions that will still be efficient for larger ranges, to support future use cases).

The main drawback of BBS Signatures is the limited hardware support, forcing most native implementations to expose the user/device binding keys to software. To provide the required assurance level, this project plans to examine and propose the necessary extensions to the WebAuthn and CTAP2 frameworks. Using [Yang et al., 2021][9], these extensions will be minimal, essentially boiling down to the implementation of one of the required elliptic curves (e.g., BLS12-381) and the Schnorr signature algorithm as part of a WebAuthn authenticator. This, in fact, is the approach followed by the TPM2.0 specification and the recent work by IBM on implementing BBS on NXP secure elements [Androulaki et al., 2024][10], which will provide a good baseline and reference for the WebAuthn extension interface.

This project will also explore different options to provide compatibility with a wider range of devices, such as BBS#[11], zk-SNARKS approaches, and ZKP for ECDSA[12]. Additionally, if requested, the project will investigate a new innovative solution that will improve performance by binding multiple user public keys (or different commitments to a single user public key) to a JWP credential signed with BBS Signatures while requiring minimum overhead by the user (i.e., use a single HW protected key-pair and require small or even constant size state to be stored by the user).

Example Use Cases

The wwWallet can be made to support any number of use cases. We have selected a few for a deep dive that hopefully will illustrate the potential inherent in the approach we have chosen. The use cases we will look at are:

Age Verification: Checking that somebody is of legal age to consume alcohol, consent to enter into financial contracts, or access restricted content online in such a way that no other information is shared about the person.

Human Status: Checking that somebody is human and not a bot for the purpose of limiting access to discussion groups to humans, again without sharing any other information about the person.

Disaster Management: Access to critical resources in the event of a disaster when infrastructure may be affected and online access may be compromised.

We are going to look a bit deeper into the age verification case because it contains several components that are common to many other use cases.

Age Verification

Age verification is the ability to check that a user is above a given age and is typically used in some legal context. For instance, certain computer games have an age limit and when logging

[9] K. Yang, L. Chen, Z. Zhang, C. J. P. Newton, B. Yang and L. Xi, "Direct Anonymous Attestation With Optimal TPM Signing Efficiency," in *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2260-2275, 2021, doi: 10.1109/TIFS.2021.3051801.

[10] Elli Androulaki, Angelo De Caro, Kaoutar El Khiyaoui, Romain Gay, Rebekah Mercer, and Alessandro Sorniotti. *"Secure and Privacy-Preserving CBDC Offline Payments Using a Secure Element."* Cryptology ePrint Archive, Paper 2024/1746, 2024. https://eprint.iacr.org/2024/1746.

[11] U Digital Identity Wallet, comment on issue #193, *GitHub*, March 2024, https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/issues/193#issuecomment-2179355934.

[12] Cloudflare, *zkp-ecdsa* repository, *GitHub*, accessed March 2024, https://github.com/cloudflare/zkp-ecdsa.

into an online game, the service provider needs a way to verify that the user “is of legal age”. Age verification would be easy if we take privacy out of the picture. Without privacy requirements, the user would simply show their passport (in some digital form) to the game provider, and the game provider would admit the user or not based on their age.
Privacy in this context means restricting the information shared with the game provider to the minimum required for the game provider to make a decision to admit the user or not. This minimum requirement is for the user to prove that they are above the legal age to access the game. This is now the goal for age verification: instead of sharing the full information from the passport or even just the birth date, only share digital cryptographic proof that the user is of legal age to be admitted into the service.
In order to implement this use case with the wwWallet, we need only one thing: an entity that can issue credentials that minimally contain the user’s birth date We call this an age credential issuer. In practice, we also need to provide some format for the age credentials themselves. In our example below, we have chosen this approach: First, the *age credential Issuer* delivers the functionality of issuance of proof of age. A simple way to obtain age information is to support officially issued documents that contain the NFC chip and follow the ICAO Doc 9303 standard; e.g., passports and other travel documents. Second, the *age credential format* is built on the SD-JWT credential format to minimise personal data disclosure.

In the figure below, objects denoted in green would be in the scope of the age verification use case.

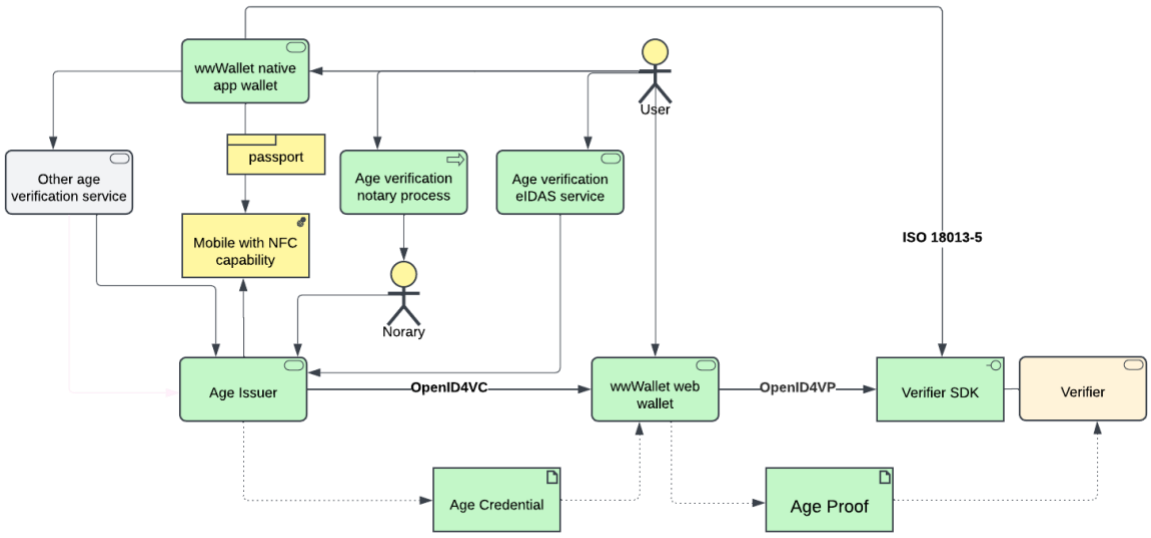


Figure 2: The Architecture of the Example Use Case.

Travel Documents

An age credential issuer must be able to draw upon some type of authentic document or process that yields true information about the person's age. One example of such a document is the ICAO Doc 9303 standard, which defines biographical and biometrical data and digital signatures for securing the data on documents with embedded contactless NFC chips.

Nowadays, many passports, identity cards, and residence permits globally have embedded contactless NFC chips that follow this standard. The EU in 2004 in Council Regulation (EC) No. 2252/200417 already specified that passports should follow the ICAO Doc 9303 standards, with the requirement to use the ICAO-compliant contactless chip for storing facial and fingerprint images in the contactless chip.

During the identity verification process, the user first takes an image of the front page of the document, allowing for OCR reading of the MRZ (Machine Readable Zone) of the document, which is needed to derive the key to access the data from the NFC chip. The user then places the document next to the NFC reader of the device, at which point the data from the chip is read. Finally, the user takes a self-photo, providing a face image for comparison and data for a liveness check and prevention of presentation attacks.

Decoupled Authorisation

In addition to reading official documents or obtaining age information from eID logins, it is possible to create a mechanism based on a pre-authorised flow where a notary verifies and authenticates some documentation attesting to age. The result is then conveyed in an issued credential. This mechanism could be useful in situations where official documents are missing or impractical to use. The flow is summarised in the diagram in Figure 2 below.

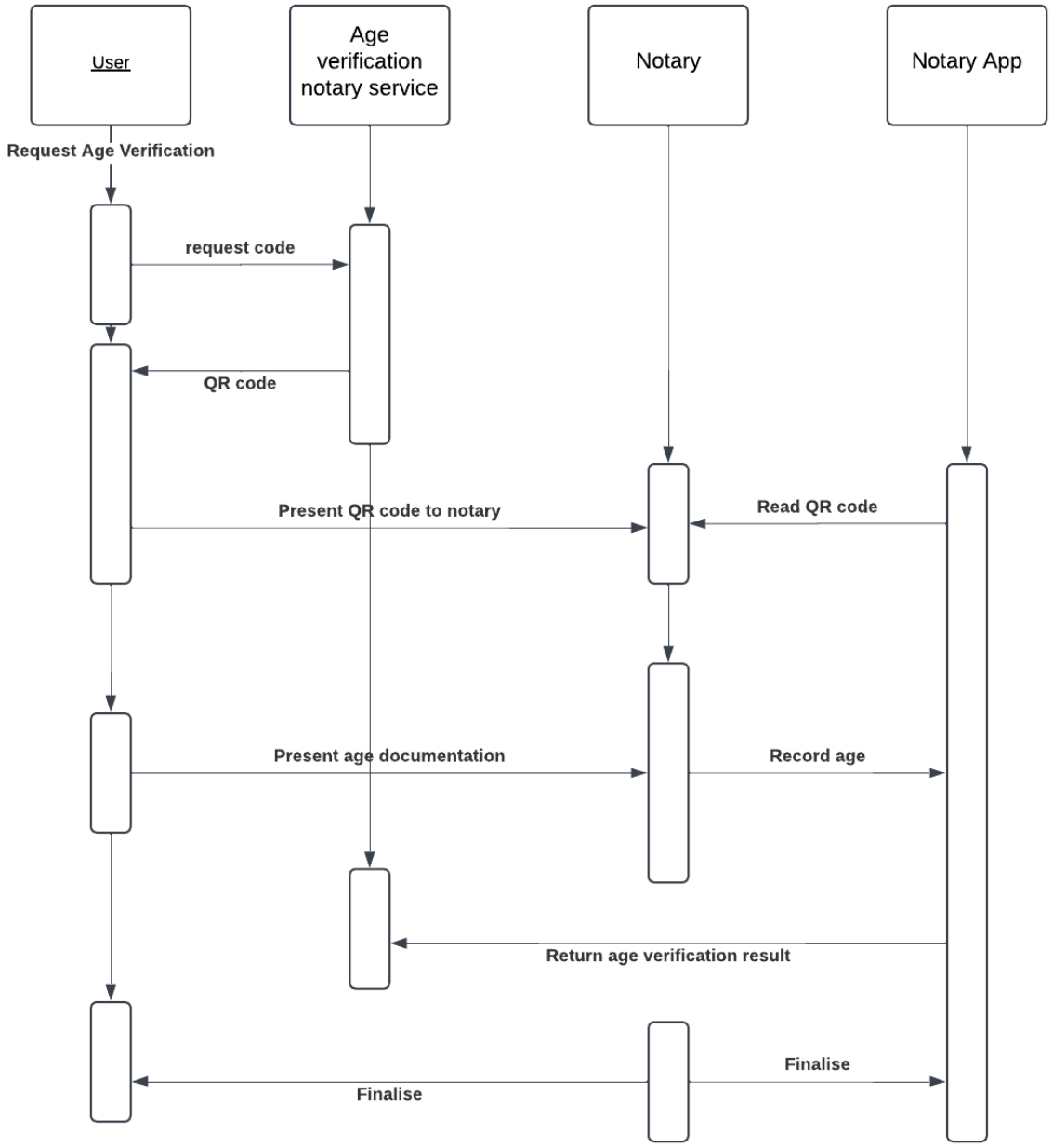


Figure 3: OpenID Flow for the Decoupled Issuance Based on Pre-authorised Code

Putting It All Together

These two choices—a simple issuer based on reading travel documents combined with a simple credential format based on SD-JWT—are enough to provide a very high degree of security and privacy for users. Using the wwWallet and these two components makes it possible to support both online and offline presentations of completely anonymised proof of age. An approach based on SD-JWT does not afford complete protection against collusion between the age credential issuer and the service provider (verifier). In order to achieve this, the solution would need to use zero-knowledge-capable credentials.

As a practical approach and to allow the market to catch up to new technologies, it is advisable to proceed in two steps: First, release a version based on SD-JWT and control the age credential issuer to ensure that it does not collude with any of the service providers and second, release a version based on ZKP credentials when additional age credential issuers would be able to issue credentials into the wwWallet. In both cases, the privacy of the user is fully ensured.

The first version of the age credential issuer could be built to support official national eID schemes. The age credential issuer could also include one of the many commercially available components for reading and authenticating documents with NFC chips following the ICAO Doc 9303 standard (i.e., passports, national e-IDs, and residency permits). There are several options on the market for such components. The result would be a credential issuer where the user is asked to present either their travel document or login using one of the recognised national eID solutions and the result would be a credential containing the birth date delivered to the wwWallet. This credential would be the basis for age proofs using SD-JWT hashed attributes.

In the second phase, a new credential scheme would be developed based on JSON Web Proofs (JWP) using unlinkable BBS Signatures based on the recently proposed scheme by Lehman[13] et al., extended with range proofs for fine-grained and privacy-preserving Age verification. The project will also provide efficient solutions for achieving LoAHigh when using JWP credentials with BBS Signatures. It would also be advisable to consider a credential scheme based on JWP and the post-quantum ZKP solution proposed by IBM in the Plaza Project (which is the subject of a European Research Council (ERC) Consolidator Grant).

This new ZKP-based scheme would be integrated into the same credential issuer—only the signature would change—so that the user would see the same process as before.

Human Verification Credentials

Human verification credentials are about telling humans apart from bots. Arguably, the biggest technical problem on the Internet today is the fact that malicious bots create so much online content that it is hard, if not impossible, to tell fact from fiction.

A solution for distinguishing humans from bots is very much a privacy problem. It is generally accepted that free speech is good and that it is sometimes important for a person to be able to protect themselves when speaking out or commenting online. The need for people to be anonymous is important online, but this has unfortunately led to a surge of bots and other artificially created online content. Additionally, it is important to be able to tell human content apart from AI-generated content in order to minimise the risk of AI being trained on its own output.

A human verification credential is, simply put, a digital proof that the user is a person. The foundation for issuing such credentials is similar to issuing an age verification credential. A person who can demonstrate ownership of an official government eID or travel document could follow a similar process to generate a credential proving they are human. In fact, the same credential used for age verification could likely be used with minor modifications

Disaster Management

In contrast to the use cases described above, let us look at a case where privacy doesn't matter but where the wwWallet project's unique approach could be used to great advantage: disaster or crisis resource management.

In a disaster or crisis situation, it is common to establish emergency communications between everyone involved in relief efforts. Often a disaster or crisis leaves enough infrastructure intact to use existing broadband infrastructure as a basis for communications. Volunteers and local coordinators need to get access to reserved frequencies or bandwidth. Instead of distributing

[13] Hasso Plattner Institute, Publications – Prof. Dr. Christoph Lehmann, accessed March 2024, https://hpi.de/lehmann/publications.html.

radios, a task that can be very challenging in itself, it is often possible to use the radios most people are familiar with: mobile phones. Most mobile networks already have the ability to prioritize traffic and reserve spectrum for certain users.

All that is needed is for relief workers to have the ability to prove their affiliation with a relief organisation for the mobile network to authorise them. For instance, the Red Cross could issue an affiliation credential to the wwWallet that could be the basis for unlocking disaster functions in the network. Because the wwWallet is completely device-independent, it would be possible for members of volunteer organisations to have a credential in their wwWallet that is available from any device, regardless of whether the device was borrowed, found, commandeered, or distributed for the relief efforts. All the relief worker needs is a phone and their FIDO hardware key. It would be possible for the relief worker to borrow a phone from anyone and, using their wwWallet, authenticate to the wwWallet with their hardware security key for the borrowed phone to turn into an emergency communications tool.

With the native app version of the wwWallet, it is possible to do most of the tasks described above, even when connectivity to the Internet is limited. For instance, it is possible to present proof that you are a relief volunteer based on an existing credential in your wallet, even if your phone is completely offline. Such a flow, referencing ISO/IEC 18013-5, is based in part on BLE.