

PAXPORT: Privacy Pitfalls in the Spanish Age Verification System

David Balbás
IMDEA Software Institute
david.balbas@imdea.org

Diego Castejón-Molina
IMDEA Software Institute
Universidad Politécnica de Madrid
diego.castejon@imdea.org

Abstract—The European Digital Identity (EUDI) wallet is intended to enable privacy-preserving access to online services across the EU. Spain’s first deployed protocol for age-restricted content, referred to here as PAXPORT, uses government-issued, single-use verifiable credentials that enable users to prove to streaming platforms that they are over 18. In line with previous analysis of EUDI wallet proposals, we argue that PAXPORT fails to provide meaningful privacy guarantees: credential issuance and presentation remain linkable, enabling government-level traceability and user deanonymization. The protocol also presents usability and scalability issues, making it a deficient template for future implementations of the EUDI wallet. We present a minimal modification, replacing standard signatures with partially blind signatures, that guarantees unlinkability. While this fix is practical, we argue that future deployments must adopt anonymous credential-based solutions, ideally incorporating zero-knowledge proofs, to meet the stated privacy goals of the EUDI initiative.

Index Terms—privacy, anonymous credentials, verifiable credentials, digital identity, age verification

I. INTRODUCTION

The European Union (EU) is moving towards a more widespread adoption of European digital identities to regulate the access to content and services in the internet. For this purpose, the EU has recently introduced an interoperable digital identity framework called the European Digital Identity (EUDI) wallet [1]. These initiatives aim to empower users with control over their identity data while prioritizing usability and user privacy.

The government of Spain recently presented the first protocol that relies on the EUDI wallet to restrict access to adult content streaming services only to adults. In this work, we brand this protocol as PAXPORT. PAXPORT involves at least three parties: the government (*registration authority* and *credential issuer*), the citizen (*user*) and the streaming platform (*service provider*). Each citizen register their digital identity with the government, and can use this identity to authenticate and receive a batch of single-use verifiable credentials that prove that their age is over 18. At a later stage, when they connect to the adult content streaming service, the platform requires them to present a valid verifiable credential. If the credential is valid and has not expired (credentials are initially planned to expire after 30 days), the user is granted access to the adult content. Otherwise, access is denied.

Given that this protocol is the first European attempt to regulate the access to digital services and content, it may be used in both Spain and in other EU countries as a template for credential issuance. Our main goal in this paper is to explain why this is not a good idea. PAXPORT, as presented by the Spanish government, has a major flaw that should be

avoided in future iterations: it enables traceability of verifiable credentials and deanonymization of users. We also argue that the current solution falls short in several other aspects that hinder its large-scale deployment. Most of our observations go in line with similar issues that have been raised by the cryptographic community [2] on different design proposals for the EUDI wallet.

Our paper is structured as follows. First, we describe the PAXPORT protocol from a cryptographic standpoint, introduce the system goals, and explain the main design flaw. Second, we show how, with minor adjustments, the same protocol can be enhanced to provide unlinkability, preventing the government from tracking citizens’ actions and minimizing the privacy loss caused by potential data breaches. We do so by leveraging partially blind signature schemes, which can readily replace standard signatures proposed in PAXPORT for credential issuance. Third, we analyse the limitations of our solution and discuss its framing within the broader EUDI wallet framework. We remark that our solution is meant to be a simple patch that allows to deploy a variant of PAXPORT that prevents user tracing by the government. Instead, we strongly suggest that legislators should direct their efforts to implement a solution based on anonymous credentials, which are a well-researched topic [3], [4], [5], [6], [7], [8], [9], [10], [11], [12].

II. PAXPORT AND ITS PRIVACY PITFALL

In this section, we provide an overview of the PAXPORT ecosystem, as described in [13]. Our analysis focuses on the cryptographic aspects of PAXPORT. Similar to anonymous credential systems [5], PAXPORT involves four parties:

- **User**: The party holding a physical, state-provided identity.
- **Registration authority**: The party responsible for registering the digital identity of *users* who possess a valid, state-provided physical identity.
- **Credential issuer**: The party that issues a digital credential indicating whether a registered *user* is an adult.
- **Service provider**: The party that grants access to a specific service only to those users who hold a credential confirming that they are adults.

In PAXPORT, the registration authority and the credential issuer are both controlled by the government, although this may not be the case for all credentials. For instance, a university may give credentials to those users who graduate. PAXPORT involves three interactive protocols between the aforementioned parties, that we denote as *identity registration*, *credential issuance* and *credential presentation*. The latter two

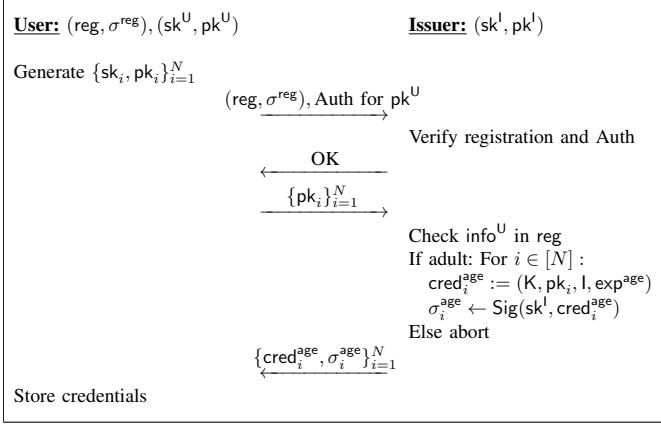


Figure 1. Age credential issuance protocol.

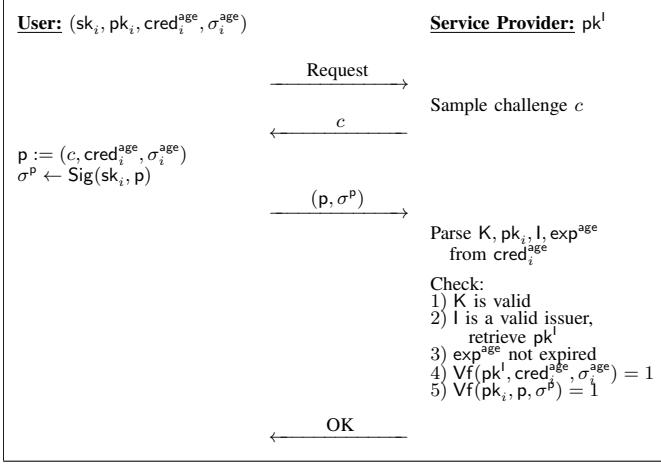


Figure 2. Age credential presentation protocol.

follow the OID4VCI and OID4VP standards for issuance and presentation of credentials, respectively. [14]

Identity registration. In Spain, everyone aged fourteen or older are required to possess a state-provided identity card called the *Documento Nacional de Identidad (DNI)*. The DNI includes a secure enclave (SE) capable of generating key pairs and signing messages. The DNI requires a password to compute a signature or to generate a new key pair. The password can only be modified using the biometric data stored on the card. The registration authority holds a key pair denoted $(\text{sk}^{\text{RA}}, \text{pk}^{\text{RA}})$. To register the key pair $(\text{sk}^{\text{U}}, \text{pk}^{\text{U}})$ in the DNI:

- 1) The user physically goes to a police station and inserts the DNI into a registration machine. The registration machine prompts the user to authenticate using their password.
- 2) The SE of the DNI provides the public key pk^{U} and certain user information info^{U} (e.g., name, surname, date of birth, address) to the registration machine.
- 3) The registration machine prepares a certificate $\text{reg} := (\text{info}^{\text{U}}, \text{pk}^{\text{U}}, \text{RA}, \text{exp}^{\text{reg}})$ containing the user's information info^{U} , the public key pk^{U} , the registration authority identity RA, and the expiration date exp^{reg} , and produces a signature σ^{reg} using sk^{RA} .
- 4) The tuple $(\text{reg}, \sigma^{\text{reg}})$ is stored in the SE of the DNI, completing the identity registration process.

Credential issuance. The user, owning a registration certific-

ate $(\text{reg}, \sigma^{\text{reg}})$ and key pair $(\text{sk}^{\text{U}}, \text{pk}^{\text{U}})$, connects to the age credential issuer to obtain a credential proving that they are an adult. The issuer holds a key pair denoted as $(\text{sk}^{\text{l}}, \text{pk}^{\text{l}})$. The credential issuance proceeds as follows (we outline the protocol flow in Figure 1):

- 1) The user generates N key pairs, denoted as $\{(\text{sk}_i, \text{pk}_i)\}_{i=1}^N$.
- 2) The user connects to the issuer's server. To authenticate, the issuer requires $(\text{reg}, \sigma^{\text{reg}})$ and a proof that the user knows sk^{U} . This is done via a standard challenge-response authentication protocol where the user signs a challenge sent by the issuer.
- 3) Upon successful authentication, the user sends the batch of public keys generated in step (1), $\{\text{pk}_i\}_{i=1}^N$.
- 4) The issuer extracts the date of birth from the user's information field, info^{U} , in reg . If the user is an adult, then for each $i \in [1, N]$, the issuer builds the age verification credential as $\text{cred}_i^{\text{age}} := (\text{K}, \text{pk}_i, \text{l}, \text{exp}^{\text{age}})$, where K is a standard identifier for age verification credential (known by all parties a-priori), pk_i is the ephemeral public key sent by the user, l is the issuer's identity, and exp^{age} is the credential's expiration date.
- 5) The issuer signs each credential using sk^{l} , such that $\sigma_i^{\text{age}} \leftarrow \text{Sig}(\text{sk}^{\text{l}}, \text{cred}_i^{\text{age}})$ and returns the set $\{\text{cred}_i^{\text{age}}, \sigma_i^{\text{age}}\}_{i=1}^N$ to the user, finalizing the credential issuance.

Credential presentation. Consider a user that owns a credential key pair $(\text{sk}_i, \text{pk}_i)$ and an age-verification credential $(\text{cred}_i^{\text{age}}, \sigma_i^{\text{age}})$. To access a service that require age verification, user and service provider proceed as follows (we outline the protocol flow in Figure 2):

- 1) The user connects to the server and the service provider sends a random challenge c .
- 2) The user produces the presentation, $\text{p} := (c, \text{cred}_i^{\text{age}}, \sigma_i^{\text{age}})$ and signs it using their secret key, $\sigma^{\text{P}} \leftarrow \text{Sig}(\text{sk}_i, \text{p})$.
- 3) The user sends the tuple $(\text{p}, \sigma^{\text{P}})$ to the service provider and deletes the credential $(\text{pk}_i, \text{sk}_i, \text{cred}_i^{\text{age}}, \sigma_i^{\text{age}})$.¹
- 4) The service provider parses K , pk_i , l , and exp^{age} from $\text{cred}_i^{\text{age}}$ and checks that:
 - a) K is the identifier of the age-verification credential.
 - b) l is the identifier of the age-verification issuer, and retrieves the public key pk^{l} .
 - c) The credential expiration date exp^{age} has not passed.
 - d) The credential is valid, $\text{Vf}(\text{pk}^{\text{l}}, \text{cred}_i^{\text{age}}, \sigma_i^{\text{age}}) = 1$
 - e) The presentation is valid, $\text{Vf}(\text{pk}_i, \text{p}, \sigma^{\text{P}}) = 1$.
- 5) If all checks pass, user is granted access to the service.

Expiration dates are intended to be short, the initial proposal being 30 days. As credentials are ephemeral, a user may run out of valid credentials before the expiration date. Thus, the credential issuance protocol should be run upon user request.

A. System Goals

The specification available for PAXPORT [13] does not convey the intended security and privacy goals. Based on the specifications, and the eIDAS regulation [1], we infer the goals and why the proponents would argue that they hold.

¹The deletion of the credential at this step is not mentioned in PAXPORT specifications, but we observe that it is needed for forward security, since reusing the same credential may lead to session correlation attacks.

- **Registration unforgeability:** No party other than the registration authority can issue registrations certificates. PAXPORT satisfies this notion since the RSA signature scheme used for identity registration is unforgeable under chosen message attacks.
- **Credential unforgeability:** No party other than the issuer can issue age-verification credentials. PAXPORT satisfies this notion since the EdDSA scheme used for credential issuance is unforgeable under chosen message attacks.
- **Presentation soundness:** The service provider should not be convinced that a presentation is valid unless: (i) the credential was produced by the issuer and; (ii) the presentation is signed by the user. We have already established that credential unforgeability holds. The EdDSA signature scheme used by the user to sign the presentation is unforgeable under chosen message attacks. Therefore, PAXPORT satisfies presentation soundness.
- **Selective disclosure:** No information is given to the service provider except what is strictly required. Since the only information contained in the credential is whether the user is an adult or not (and not their date of birth or any other information in info^U), PAXPORT satisfies this property.
- **Privacy with respect to the service provider:** The service provider should neither learn the identity of the user from the presentation (p, σ^P) nor be able to link different access requests from the same user.² Intuitively, PAXPORT satisfies this property because:
 - The presentation does not contain the field info^U that allows to identify the user.
 - The public key pk_i is ephemeral and single-use.
 - Signatures themselves do not contain any information about the user, given that the relation between a signature σ^{age} and the user is never known to the service provider.

Note that such an assumption breaks if there is a collusion between the issuer and the service provider.

B. PAXPORT enables user tracking

The security notion underlying PAXPORT is insufficient because it considers only the information that the service provider directly receives from the user, ignoring the broader context of information available within the ecosystem. In particular, it overlooks the possibility that the credential issuer may leak information that could enable the service provider, or any other entity, to link presentations to users.

In the literature on anonymous credential systems, the usual privacy notion is called user unlinkability. This property requires that, even if the registration authority, issuer, and service provider fully collude and share all the information they possess, they still cannot determine which user generated a particular credential presentation, or in general correlate two presentations of credentials.

Definition of unlinkability. Formally defining unforgeability for PAXPORT requires to state the latter as a cryptographic primitive with a concrete syntax and to introduce a security game. This is beyond the scope of this work, but we introduce an informal game-based notion below. The game involves a challenger and an adversary \mathcal{A} who proceed as follows:

²We remark that deanonymization may occur by other means, such as by tracking of IP addresses. However, this is out of the scope of our analysis.

- 1) The challenger randomly samples a challenge bit $b \leftarrow \{0, 1\}$.
- 2) The adversary \mathcal{A} has full access to the service provider, the issuer, and the registration authority. It generates keys pk^I and pk^{RA} for the latter two.
- 3) Two users U_0, U_1 obtain a registration certificate from the registration authority.
- 4) Each user obtains a batch of age-verification credentials from the issuer.
- 5) \mathcal{A} queries either U_0 or U_1 to present a credential to the service provider. \mathcal{A} can make multiple queries to the users.
- 6) At some point, \mathcal{A} issues a challenge. Then, user U_b makes a presentation to the service provider.
- 7) Finally (and after potentially more presentation queries from \mathcal{A}), the adversary outputs a bit b' .

The adversary wins the game if $b = b'$. We say that PAXPORT achieves (computational) unlinkability if the winning probability of any polynomial-time adversary is $\Pr[b = b'] = 1/2 + \text{negl}(\lambda)$ for a negligible function $\text{negl}(\lambda)$.

PAXPORT does not satisfy unlinkability. The system trivially allows credential presentations to be traced back to their owners through the following process:

- 1) During credential issuance, the issuer receives info^U and $\{\text{pk}_i\}_{i=1}^N$ from each user. The issuer can create a key-value store where each pk_i serves as a key and the associated info^U as its value.
- 2) The service provider later receives a tuple (p, σ^P) , which can be parsed as $p = (c, \text{cred}_i^{\text{age}}, \sigma_i^{\text{age}})$, where $\text{cred}_i^{\text{age}} = (K, \text{pk}_i, l, \exp^{\text{age}})$.
- 3) The service provider can forward pk_i to the issuer, who looks it up in the key-value store and returns the corresponding info^U , uniquely identifying the user.

One might argue that collusion between the issuer and the service provider is unlikely. However, the core issue with PAXPORT is that the protocol imposes *no technical barrier* preventing the issuer (i.e. the government) from creating such a key-value mapping. Even if the issuer refrains from doing so intentionally, a security breach in the credential issuance infrastructure could expose this information to external attackers, who could exploit it, for instance to blackmail users based on their use of age-verification credentials.

The fundamental problem, therefore, is that the data *exists at all* beyond the user's device. We argue that PAXPORT (and, in general, any future implementation of the EUDI wallet) should be redesigned with user unlinkability as a foundational principle, thereby eliminating all data that enables user tracking. This would protect users privacy even in the event of a severe data breach, or even if the system is misused by a potentially authoritarian government.

III. A SIMPLE FIX FOR PAXPORT

Despite the important privacy flaw in PAXPORT, there are simple ways to fix it. In this section, we introduce a fix that requires minimal changes to the scheme, relies only on standard cryptographic primitives, and can be prototyped and implemented promptly. As we argue in the discussion section, our proposal is not a fully optimal solution, but rather an example for how the current implementation can be improved with minor modifications. Optimal designs can be obtained

$\text{Blind}_{\mathcal{A}}(\lambda)$
1 : $(\text{pk}, t, m_0, m_1) \leftarrow \mathcal{A}(1^\lambda), b \leftarrow \{0, 1\}$
2 : $\forall a \in \{0, 1\} : (\rho_U^a, \text{st}_a) \leftarrow \text{User}(\text{pk}, t, m_a)$
3 : $(\rho_S^b, \rho_S^{1-b}) \leftarrow \mathcal{A}(\rho_U^b, \rho_U^{1-b})$
4 : $\forall a \in \{0, 1\} : \sigma_a \leftarrow \text{Derive}(\text{st}_a, t, \rho_S^a)$
5 : if $\exists a$ s.t. $\text{Vf}(\text{pk}, t, m_a, \sigma_a) = 0$ then
6 : $\sigma_0 = \sigma_1 = \perp$
7 : $b' \leftarrow \mathcal{A}(\sigma_0, \sigma_1)$
8 : return $b = b'$

Figure 3. Security game for partial blindness under chosen keys.

by leveraging zero knowledge proofs, but there are further barriers to their adoption such as a lack of standardized schemes.

Our proposal consists of modifying the credential issuance by using *partially blind digital signatures*, which are standardized in ISO/IEC 18370-2:2016 [15] and which we define below.

Definition 1. A partially blind signature scheme [16] with tag space \mathcal{T} and message space \mathcal{M} , is a tuple of algorithms with the following syntax, adopted from [17]:

- A key generation algorithm $\text{KGen}(1^\lambda)$ that takes the security parameter λ and outputs a public/secret key pair (pk, sk) .
- A user algorithm $\text{User}(\text{pk}, t, m)$ that inputs a public key pk , a tag $t \in \mathcal{T}$ and a message $m \in \mathcal{M}$ and outputs a blind user message ρ_U and a state st .
- A signer algorithm $\text{Signer}(\text{sk}, t, \rho_U)$ inputs a secret key sk , a tag $t \in \mathcal{T}$ and a user message ρ_U and outputs a signer message ρ_S .
- A derivation algorithm $\text{Derive}(\text{st}, t, \rho_S)$ inputs a state st , a tag $t \in \mathcal{T}$ and a signer message ρ_S and outputs a signature σ .
- A verification algorithm $\text{Vf}(\text{pk}, t, m, \sigma)$ outputs 1 if σ is a valid signature on m for tag t under the public key pk , and outputs 0 otherwise.

A secure partially blind signature scheme satisfies *partial blindness* and *one-more unforgeability*. Partial blindness is a privacy notion that prevents the signer (or any observer) to link a signature σ for message m and tag t to any signing session for users using the same tag t . One-more unforgeability is a security notion that ensures that no adversary can output $k+1$ valid signatures given that they have obtained k valid signatures from the signer. We present the details for partial blindness in Figure 3, as we use it later to argue that our construction satisfies unlinkability. A signature scheme satisfies partial blindness if for any polynomial-time adversary \mathcal{A} playing the game in Figure 3 it holds that $\Pr[b = b'] = 1/2 + \text{negl}(\lambda)$.

Credential issuance with partially blind signatures. As in the original protocol, we assume that the user owns a registration certificate $(\text{reg}, \sigma^{\text{reg}})$ and key pair $(\text{sk}^U, \text{pk}^U)$. The user connects to the credential issuer to obtain a credential proving that they are an adult. The issuer holds a blind

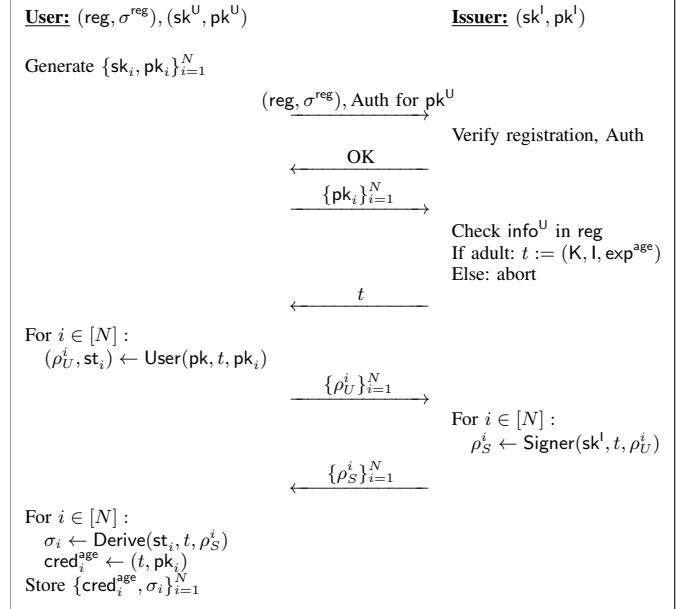


Figure 4. Credential issuance with partially blind signatures.

signature key pair denoted as $(\text{sk}^I, \text{pk}^I) \leftarrow \text{KGen}(1^\lambda)$. The credential issuance with partially blind signatures proceeds:

- 1) The user generates N key pairs, $\{(\text{sk}_i, \text{pk}_i)\}_{i=1}^N$.
- 2) The user connects to the issuer's server. The issuer requires $(\text{reg}, \sigma^{\text{reg}})$ and authenticates the user on pk^U .
- 3) Upon successful authentication, the issuer extracts the date of birth from the user's information field, info^U , in reg . If the user is an adult, the issuer sets a tag to $t := (\text{K}, \text{I}, \text{exp}^{\text{age}})$ and sends it to the user, or aborts otherwise. The tag is shared among all users with age-verification credentials with the same expiration date.
- 4) The user receives the tag t and, for each pk_i in $\{\text{pk}_i\}_{i=1}^N$, computes $(\rho_U^i, \text{st}_i) \leftarrow \text{User}(\text{pk}^U, t, \text{pk}_i)$, and sends the batch of blind messages $\{\rho_U^i\}_{i=1}^N$ to the issuer.
- 5) For each ρ_U^i in $\{\rho_U^i\}_{i=1}^N$, the issuer computes $\rho_S^i \leftarrow \text{Signer}(\text{sk}^I, t, \rho_U^i)$, and returns the batch of blind signatures $\{\rho_S^i\}_{i=1}^N$ to the user.
- 6) For each ρ_S^i in $\{\rho_S^i\}_{i=1}^N$, the user computes $\sigma_i \leftarrow \text{Derive}(\text{st}_i, t, \rho_S^i)$. Finally, the user sets $\text{cred}_i^{\text{age}} := (t := (\text{K}, \text{I}, \text{exp}^{\text{age}}), \text{pk}_i)$ for each pk_i in $\{\text{pk}_i\}_{i=1}^N$.

We summarize the protocol in Figure 4. The protocol requires minimal modifications with respect to the original PAXPORT issuance protocol (Figure 1) and requires one additional round of interaction.

Regarding credential presentation, the service provider now parses $\text{cred}_i^{\text{age}} := (t, \text{pk}_i)$ and checks whether $\text{Vf}(\text{pk}^I, t, \text{pk}_i, \sigma_i) = 1$.

A. Security Analysis

Regarding security, introducing partially blind signatures requires to revise credential unforgeability, presentation soundness and user unlinkability. Regarding credential unforgeability and presentation soundness, we argue that we are substituting a digital signature, secure under unforgeability under chosen message attacks, with a partially blind signature

scheme, secure under one-more unforgeability. Since one-more unforgeability implies unforgeability under chosen message attacks [18], [19], PAXPORT with partially blind signatures for credential issuance satisfies credential unforgeability and presentation soundness. Regarding user unlinkability, we state the property in Claim 1 and argue why it holds below.

Claim 1. *Assume that the partially blind signature scheme achieves partial blindness under chosen keys. Then, our proposed modification for PAXPORT satisfies computational unlinkability.*

Proof: (sketch). Assume that there is an adversary \mathcal{A} that is able to win the unlinkability game for PAXPORT with a probability significantly greater than $1/2$. We show how to build an adversary \mathcal{B} that uses \mathcal{A} to break partial blindness under chosen keys (Figure 3). For simplicity, we let $N = 1$. Setting arbitrary N would require an additional guessing step in the proof involving a linear security loss in N .

- 1) \mathcal{B} initializes \mathcal{A} , who outputs the registration authority public key pk^{RA} and the credential issuer key pair pk^l .
- 2) \mathcal{B} samples user pairs $(\text{sk}^{u_0}, \text{pk}^{u_0})$ and $(\text{sk}^{u_1}, \text{pk}^{u_1})$ and interacts with \mathcal{A} for each key pair the identity registration protocol, obtaining $(\text{reg}_0, \sigma^{\text{reg}_0})$ and $(\text{reg}_1, \sigma^{\text{reg}_1})$.
- 3) Prior to interacting with \mathcal{A} on protocol credential issuance, \mathcal{B} samples key pairs $(\text{pk}_0, \text{sk}_0)$ and $(\text{pk}_1, \text{sk}_1)$.
- 4) \mathcal{B} runs credential issuance as user 0, using $(\text{reg}_0, \sigma^{\text{reg}_0})$. When \mathcal{A} outputs $t := (\text{K}, \text{l}, \text{exp}^{\text{age}})$ in step 3, \mathcal{B} initializes the challenger of partial blindness on chosen keys by providing the tuple $(\text{pk}^l, t, \text{pk}_0, \text{pk}_1)$ and receives (ρ_U^0, ρ_U^1) . In step 4, \mathcal{B} sends ρ_U^0 to \mathcal{A} , receiving ρ_U^0 .
- 5) \mathcal{B} runs credential issuance as user 1, using $(\text{reg}_1, \sigma^{\text{reg}_1})$, and in step 4, sends ρ_U^1 to \mathcal{A} , receiving ρ_S^1 .
- 6) \mathcal{B} returns (ρ_U^0, ρ_S^1) to the challenger, who replies with (σ_0, σ_1) . Now, \mathcal{B} invokes \mathcal{A} on input $(t := (\text{K}, \text{l}, \text{exp}^{\text{age}}), \text{pk}_0, \sigma_0)$, receiving a bit b' .
- 7) \mathcal{B} forwards the bit b' to the challenger.

It is easy to see that \mathcal{B} is a polynomial-time algorithm and that it perfectly simulates the unlinkability game to \mathcal{A} . If \mathcal{A} makes a correct guess for in which of the two credential issuance processes pk_0 was used, then the bit b' forwarded to the challenger is also a correct guess for the shuffling of the blind messages. Hence, \mathcal{B} has the same success probability than \mathcal{A} , breaking partial blindness for chosen keys.

We conclude that if the partially blind signature scheme satisfies partial blindness under chosen keys, then PAXPORT achieves user unlinkability. ■

Computational and statistical unlinkability. In some anonymous credential schemes, unlinkability is achieved unconditionally, meaning that user privacy will be preserved even if other security properties, such as unforgeability, are broken by powerful or future adversaries. In practice, this is a great feature to aim for, as it guarantees the preservation of user privacy against quantum adversaries, against a break of the underlying cryptography, or even against a leakage of the secret keys. In our case, this depends on the choice of the partially blind signature scheme. If the latter satisfies statistical partial blindness under chosen keys, then our proposed modification of PAXPORT will satisfy statistical unlinkability too.

IV. DISCUSSION

A. Framing within the EU Digital Identity Wallet

As we mention, the PAXPORT solution can be framed as a preliminary and bounded-scope implementation of the EUDI wallet. While PAXPORT is only capable of proving one statement, that is “I am over 18”, the EUDI wallet should support more complex statements over different user attributes, such as the possession of a valid driving licence, the (lack of) a criminal record, or the possession of an academic degree. Current proposals for implementations of the EUDI Wallet rely on batch issuance of verifiable credentials, similarly to PAXPORT, and therefore suffer from the same privacy pitfalls. Indeed, these solutions enable selective disclosure but fail to provide unlinkability [20], in the event of a collusion between issuers and verifiers, offering weak privacy guarantees for users.

Privacy is not the only technical concern in the current PAXPORT and other EUDI Wallet designs. There are several other issues with the current solutions, including but not limited to:

- *Non-transferability and device binding.* Credentials should be linked to a device and never be shared with other users. This is not an explicit security goal of the PAXPORT technical specification, but it seems critical to it. In practice, key exfiltration can be prevented (under some assumptions) by storing keys in secure hardware enclaves, also minimizing the risk of security breaches.
- *Storage of cryptographic keys.* For solutions that employ secure enclaves, we note that the storage of these enclaves is reduced, and flooding them with tens or hundreds of one-time keys is not ideal. Besides, hardware attestation for these keys may introduce linkability issues [2].
- *Denial of credentials.* These designs rely on a central party, i.e., the government, to operate as the registration authority and credential issuer. As such, a malicious government could arbitrarily deny digital identities to and credentials to specific citizens, preventing their access to any service that requires EUDI credentials.
- *Server overhead.* The solution requires a frequent interaction with the issuer’s server due to the short living time of the one-time credentials. This puts a large overhead in the server and a temporary server unavailability may have a significant impact in the service.
- *Issuer disclosure.* Hiding the issuer’s identity from the service provider is not possible, as it is part of the tag. In multi-issuer settings (such as the EU with the multiple member states and institutions), disclosing the issuer may be a significant source of information which is not needed by the service provider.
- *Attestation of complex statements.* In the event of having credentials with multiple attributes, these have to be either fully disclosed or not disclosed at all. This prevents users from attesting complex more statements while disclosing the minimal amount of information. For example, an age credential cannot be used to prove “I am over 65” unless one includes a specific attribute for this (or unless the full date of birth is disclosed, deanonymizing the user). It is also impossible to prove disjunctive statements such as “I have a bachelor’s degree or a superior technical diploma”.

Limitations of our solution. As mentioned, while our solution does fix the main privacy flaw of PAXPORT, it is still suboptimal and suffers from most of the limitations we just mentioned. The issuer anonymity limitation is the simplest one to fix: we can simply use partially blind ring signatures where the ring of signers consists of all valid issuers in the EU. In addition, denial of credentials can be also mitigated by accepting registration authorities and credential issuers other than the government e.g., a certificate or a credential signed by an independent notary. We also note that the security of our solution has not been analyzed with sufficient rigour, as we did not develop a formal cryptographic modelling with corresponding security proofs.

B. The golden standard: anonymous credential systems.

Following many rounds of interaction between the academic community and the discussion group for the EUDI Wallet [2], the latter now states an interest in leveraging advanced cryptography, in particular anonymous credential-based systems [21]. These systems are designed with unlinkability as a foundational principle, preventing the design flaws of the current schemes. We argue that this is the right design pattern to pursue for PAXPORT and for the EUDI Wallet; while our proposed fix is simple and practical, these systems should be redesigned more deeply in future iterations.

Among the possible ways of realizing anonymous credentials, the EUDI Wallet is currently evaluating systems based on zero-knowledge proofs [22]. Zero-knowledge proofs [23] allow users to prove statements without revealing any additional information beyond the truth of the statement itself. Such protocols enable holders to generate privacy-preserving proofs that a certain predicate on their credential holds, as well as proving the possession of a valid credential without disclosing it. Nevertheless, there exist multiple challenges towards deploying these systems at scale. These include requirements to rely only on standardized cryptography, lack of secure hardware support for pairing-based cryptography, and efficiency and security trade-offs of proof systems and their implementations. The deployment of zero-knowledge proofs within the EUDI framework is thus expected to be slow, but we encourage both researchers and practitioners to support this or any effort to migrate to an anonymous credential-based system, moving away from the single-use verifiable credential setting.

ACKNOWLEDGEMENTS

This work is supported by the PICOCRYPT project that has received funding from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme (Grant agreement No. 101001283), partially supported by projects PRODIGY (TED2021-132464B-I00), ESPADA (PID2022-142290OB-I00), and EX2024-001471-M funded by MCIN/AEI/10.13039/501100011033/ and the European Union NextGenerationEU / PRTR, and partially funded by Ministerio de Universidades (FPU21/00600).

REFERENCES

- [1] E. Parliament and C. of the European Union, “Regulation (EU) 2024/1183 amending Regulation (EU) 910/2014 as regards establishing the European Digital Identity Framework,” 2024. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/1183/oj>
- [2] C. Baum et al., “Cryptographers’ feedback on the eu digital identity’s arf,” 2024, available: <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/issues/200>.
- [3] D. Bosk, D. Frey, M. Gestin, and G. Piolle, “Hidden issuer anonymous credential,” *PoPETs*, vol. 2022, no. 4, pp. 571–607, Oct. 2022.
- [4] J. Camenisch, M. Dubovitskaya, K. Haralambiev, and M. Kohlweiss, “Composable and modular anonymous credentials: Definitions and practical constructions,” in *ASIACRYPT 2015, Part II*, ser. LNCS, T. Iwata and J. H. Cheon, Eds., vol. 9453, Nov. / Dec. 2015, pp. 262–288.
- [5] J. Camenisch and A. Lysyanskaya, “An efficient system for non-transferable anonymous credentials with optional anonymity revocation,” in *EUROCRYPT 2001*, ser. LNCS, B. Pfitzmann, Ed., vol. 2045, May 2001, pp. 93–118.
- [6] ———, “Signature schemes and anonymous credentials from bilinear maps,” in *CRYPTO 2004*, ser. LNCS, M. Franklin, Ed., vol. 3152, Aug. 2004, pp. 56–72.
- [7] A. Connolly, P. Lafourcade, and O. Perez-Kempner, “Improved constructions of anonymous credentials from structure-preserving signatures on equivalence classes,” in *PKC 2022, Part I*, ser. LNCS, May 2022, pp. 409–438.
- [8] G. Fuchsbauer, C. Hanser, and D. Slamanig, “Structure-preserving signatures on equivalence classes and constant-size anonymous credentials,” *Journal of Cryptology*, vol. 32, no. 2, pp. 498–546, Apr. 2019.
- [9] O. Mir, B. Bauer, S. Griffy, A. Lysyanskaya, and D. Slamanig, “Aggregate signatures with versatile randomization and issuer-hiding multi-authority anonymous credentials,” in *ACM CCS 2023*. ACM Press, Nov. 2023, pp. 30–44.
- [10] O. Sanders, “Efficient redactable signature and application to anonymous credentials,” in *PKC 2020, Part II*, ser. LNCS, A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, Eds., vol. 12111, May 2020, pp. 628–656.
- [11] O. Sanders and J. Traoré, “Compact issuer-hiding authentication, application to anonymous credential,” *PoPETs*, vol. 2024, no. 3, pp. 645–658, Jul. 2024.
- [12] R. Mercer, K. E. Khiyaoui, A. D. Caro, and E. Androulaki, “Efficient aggregate anonymous credentials for decentralized identity,” *Cryptology ePrint Archive*, Paper 2025/1724, 2025. [Online]. Available: <https://eprint.iacr.org/2025/1724>
- [13] Ministerio para la Transformacion Digital y de la Funcion Publica, “Presentacion del ecosistema de verificacion de edad,” Ministerio para la Transformacion Digital y de la Funcion Publica, Espana, Technical report, 2024, v1.0, 30 de junio de 2024. [Online]. Available: https://digital.gob.es/especificaciones_tecnicas
- [14] “Openid for verifiable presentations 1.0,” https://openid.net/specs/openid-4-verifiable-presentations-1_0.html, author=OpenID Digital Credentials Protocols Workgroup, year=2025.
- [15] *Information technology — Security techniques — Blind digital signatures — Part 2: Discrete logarithm based mechanisms*, Std. ISO/IEC 18 370-2:2016, Jul 2016, edition 1; International Standard; Reference No. 62544.
- [16] M. Abe and T. Okamoto, “Provably secure partially blind signatures,” in *CRYPTO 2000*, ser. LNCS, M. Bellare, Ed., vol. 1880, Aug. 2000, pp. 271–286.
- [17] S. Katsumata, M. Reichle, and Y. Sakai, “Practical round-optimal blind signatures in the ROM from standard assumptions,” in *ASIACRYPT 2023, Part II*, ser. LNCS, Dec. 2023, pp. 383–417.
- [18] D. Pointcheval and J. Stern, “Provably secure blind signature schemes,” in *ASIACRYPT’96*, ser. LNCS, K. Kim and T. Matsumoto, Eds., vol. 1163, Nov. 1996, pp. 252–265.
- [19] ———, “Security arguments for digital signatures and blind signatures,” *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, Jun. 2000.
- [20] A. Lehmann, “Eu digital identity and anonymous credentials - a happy end?” Talk given at RWC 2025, 2025, video at <https://youtu.be/UpQHWObCx4I>.
- [21] J. Camenisch and A. Lysyanskaya, “An identity escrow scheme with appointed verifiers,” in *CRYPTO 2001*, ser. LNCS, J. Kilian, Ed., vol. 2139, Aug. 2001, pp. 388–407.
- [22] “Specification for ZKP Implementation in EUDI Wallet,” 2025. [Online]. Available: <https://github.com/eu-digital-identity-wallet/eudi-doc-standards-and-technical-specifications/blob/main/docs/technical-specifications/ts4-zkp.md>
- [23] S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of interactive proof-systems (extended abstract),” in *17th ACM STOC*. ACM Press, May 1985, pp. 291–304.