Cryptographers' Feedback on the EU Digital Identity's ARF

Carsten Baum
Technical University of Denmark

Olivier Blazy
École Polytechnique

Jan Camenisch
Dfinity

Jaap-Henk Hoepman
Karlstad University
& Radboud University

Eysa Lee
Brown University

Anja Lehmann
Hasso-Plattner-Institute,
University of Potsdam

Anna Lysyanskaya
Brown University

René Mayrhofer
Johannes Kepler University Linz

Hart Montgomery*

Ngoc Khanh Nguyen
King's College London

Bart Preneel
KU Leuven

abhi shelat
Northeastern University

Daniel Slamanig
Universität der Bundeswehr München

Stefano Tessaro
University of Washington

Søren Eller Thomsen
Partisia

Carmela Troncoso
EPFL

June 2024

Executive Summary

The eiDAS 2.0 regulation (electronic identification and trust services) that defines the new EU Digital Identity Wallet (EUDIW) is an important step towards developing interoperable digital identities in Europe for the public and private sectors. The regulation, if realized with the right technology, can make Europe the front runner in private and secure identification mechanisms in the digital space, and act as a template for future digital identity systems in other regions.

Unfortunately, we believe that some of the currently suggested design aspects of the EUDI and its credential mechanism fall short of the privacy requirements that were explicitly defined after extensive debate in the Digital Identity regulation. The main reason for this shortcoming in the current proposal is that it relies on cryptographic methods that were never designed for such requirements. We do not see a way to fix the proposed solution to meet all the privacy features as required by the regulation; we believe that a larger redesign is in order.

In this document, we propose to use a different cryptographic mechanism instead; namely, *anonymous credentials*. Anonymous credentials were designed specifically to achieve authentication and identification that are both secure and privacy-preserving. As a result, they fully meet the requirements put forth in the eiDAS 2.0 regulation. Moreover, they are by now a mature technology. This technology was developed more than twenty years ago, and extensive efforts have been expended to analyze, improve, implement, standardize, test, and deploy it. Anonymous credentials are well understood by the scientific community.

Our specific recommendation is to use the BBS family of anonymous credentials. For BBS, thanks to prior work by the W3C, the Decentralized Identity Foundation, IETF/IRTF, ISO, and other standardization

*Writing as an individual and speaking for himself.

bodies, as well as the availability of open-source software libraries, the EC can develop a standard and reference implementation with only a modest effort. We additionally recommend that the EUDI be designed following the principle of crypto-agility, meaning that its underlying technologies can be upgraded quickly in the future if the need arises.

We thank the EC for this opportunity to weigh in. We would be excited to continue to provide feedback on this important endeavor, and see this document as the beginning of a longer dialogue.

1 Introduction

The Digital Identity Regulation entered into force in May 2024 [eID24]. It establishes the European Digital Identity Framework, which proposes the EU Digital Identity Wallet (EUDI). The regulation aims to produce a wallet that shall be a "fully mobile, secure and user-friendly" service, enabling users to identify themselves to public and private online services. All member states are now required to offer such an EUDI wallet to all their citizens and residents by 2026.

The EUDI Wallet Team of the European Commission invited subject-matter experts (i.e. cryptographers) to participate in a Webex meeting on June 5th or 6th, 2024, in which they presented to us their current design of the EUDIW (ARF version 1.4.0 [ARF24]), and requested feedback. They specifically requested feedback concerning attestations and zero-knowledge proofs. This document represents our **consensus opinion**.

We start by stating the security and privacy requirements expressed through the Digital Identity Regulation. We then analyze the proposed EUDIW design along these requirements, and suggest a better approach that satisfies the desired requirements.

1.1 Security & Privacy Properties of the EUDIW

The regulation [eID24] specifies several security and privacy requirements for the EUDI, that *shall* be satisfied by the technical realisation. Article 5a (*European Digital Identity Wallets*) states:

- §4. European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to:
  - (a) securely [..] authenticate to relying parties [..] while ensuring that selective disclosure of data is possible;
  - (b) generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet;
- §16. The technical framework of the European Digital Identity Wallet shall:
  - (a) not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user;
  - (b) enable privacy preserving techniques which ensure unlinkability, where the attestation of attributes does not require the identification of the user.

These legal regulations correspond to the following technical properties:

Selective Disclosure: A user can decide how much or how little information about himself to disclose in a transaction; and software applications making use of EUDIW can be designed with data minimization principles in mind.

Unlinkability: Unlinkability is a technical term; in the digital credentials literature, it means that transactions of the same user cannot be linked or traced. In fact, it comes in three different forms depending on the corruption setting.

- Unlinkability with respect to Relying Parties (RPs): If a user presents his credential to different RPs, they cannot determine whether these two transactions correspond to the same user or to two distinct users[1]. Note that RPs may have access to additional information to correlate the transaction data with, and unlinkability needs to hold regardless of auxiliary information. Moreover, unless the user is explicitly required to establish a persistent identifier (pseudonym) with the RP and always interact with it using this pseudonym, unlinkability should also hold when the user presents his credential twice to the same RP.
- Unlinkability with respect to Identity Provider (IdP): The IdP should not be able to learn anything about when, where, and to which relying parties a user presents his credential. This is sometimes also referred to as *unobservability*, as it requires the IdP to not be able to observe the user's behaviour while providing its issuance service.
- Unlinkability with respect to IdP & RPs: The previous two variants capture security towards corrupt RPs *or* corrupt IdP (but not both), whereas this notion guarantees unlinkability even when the IdP and RP collude. That is, the IdP that issues credentials to the user cannot obtain any data from the RPs that allows it to track and re-identity the user behind a transaction. This is sometimes referred to as *untraceability*, as it requires the IdP and RPs to be unable to trace a user's credential usage.

Unlinkability is extremely important for privacy: it ensures that even if the IdPs and RPs get compromised, or are even controlled by a malicious entity, or simply fail to safeguard their data[2], the users' activities still cannot be traced. For example, if one uses the EUDIW for public transportation, unlinkability ensures the privacy of the users' physical location. Without unlinkability, an RP to whom the user has presented a credential just once will be able to trace this user's activities throughout the system and observe everywhere the user has been, like a virtual stalker, completely violating the user's privacy rights.

All three types of unlinkability are mandated. By not allowing that the user's activities be "tracked, linked or correlated" and requiring that the technology "enable privacy preserving techniques which ensure unlinkability," **Article 5a §16(a) and (b) of the current regulation requires all three types of unlinkability**.

Pseudonymous Authentication: Pseudonymous authentication allows user to securely authenticate without the need of unique identification across his transactions. That is, the user can authenticate towards each RP under a *pseudonymous* identifier. Depending on the use case, pseudonyms can be derived fresh for each purpose, or also be limited, e.g., ensuring that each user can only have a single pseudonym per RP. Such pseudonyms allow for secure re-authentication and to generate a consistent relationship with RPs. Across RPs, these pseudonyms must not interfere with unlinkability, i.e., still ensure that different pseudonyms – albeit belonging to the same user – cannot be correlated.

Unforgeability and Non-Transferability: It is also important that users not be able to present fraudulent credentials. Users should also be unable to share credentials with other, unauthorized users.

1.2 Document Overview

We have analyzed the proposed EUDIW design, and found that it fails to provide the desired privacy features. As the EUDI Wallet Team is already aware, it does not provide unlinkability: if the same attestation is used in two transactions, these transactions can be linked. A natural question is: what if the user obtains several

[1] More precisely, in a setting where the users reveal a subset of attributes, for example, their eligibility for a senior discount, the RPs cannot tell whether they are interacting with the same user, or with two different users with the same attribute value (e.g., the same senior discount eligibility status).

[2] Even without assuming explicitly malicious behavior, there are many realistic threat scenarios that can lead to intentional or unintentional collusion, potentially long after the original transaction has happened: leaks of key material, previous access/transaction logs, internal databases, etc. happen regularly even under the best intentions and have to be assumed to happen to IdPs and RPs under this architecture.

EUDI attestations, a separate and unlinkable one for each of its transaction? Unfortunately, in this case, unlinkability would come at the expense of non-transferability. We present more technical details in Section 2.

In this document, we also suggest a better approach, one that does indeed satisfy the desired privacy requirements (as well as, of course, the desired security and identity assurance requirements). This approach is based on the well understood, provably secure methodology of anonymous credentials. In Section 3 we explain what anonymous credentials are at a high level and review the appropriate scientific literature. In Section 4 we go over relevant standards for anonymous credentials. In Section 5 we survey open-source implementations and real-world deployments of anonymous credentials. Finally, we address potential concerns posed by quantum computers in Section 6.

2 Analysis of the ARF and Its Shortcomings

The currently proposed solution [ARF24], suggests the issuance of credentials on individually hashed user attributes $h = H(s_i, a_i)$. When s_i is of high entropy (and per-attribute random), this allows selective disclosure of the signed values towards the Relying Parties (RP). An advantage is that this salted-hash solution can be immediately deployed and is compatible with every signature scheme. This approach to selective attribute disclosure is specified in ISO/IEC 18013-5 [ISO21] (mobile driving license) and already implemented in standard smartphone wallets and various national driver's license issuers based on existing smartphone keystore hard- and software and (cloud) hardware security modules. The main disadvantages of this approach are:

1. No unlinkability with respect to RPs, i.e., unlinkability across presentations, due to static hashes and the static IdP signature on the salted-hashes structure (called Mobile Security Object (MSO) in ISO/IEC 18013-5). This can only be partially avoided via batch issuance of multiple credentials (single-use MSOs, never to be re-used after a single showing with the respective subset of disclosed attributes).

2. No unlinkability with respect to IdP and RPs, i.e., no untraceability of issuance and presentation, due to linkage via the static hashes and signature values. That is, **unlinkability cannot be ensured** under the assumption of collusion between IdP and RP, making this solution incompatible with Regulation 2024/1183[3].

User-specific credentials must be strictly bound to their designated owner, in order to satisfy the non-transferability requirement. This is typically done by including a public key in the credential and requiring a fresh proof of ownership of the corresponding secret key.

If unlinkability with respect to RPs is aimed for through batch issuance of multiple credentials, supporting this in a user-binding and non-transferable way is not straightforward. Germany's ARF [Ger24] for the EUDI mentions batch issuance for "ephemeral keys". This is neither ideal for security nor usability. If the user has to create a fresh key pair for every unlinkable credential he wants to obtain, he has to securely store and manage a large number of keys on his device[4]. To establish pseudonymous identities, and enable re-authentication under a previously established pseudonymous public key, this also requires him to remember which key has been used towards which RP. There is also nothing that binds the keys together, or establishes a real digital identity, as every credential/key pair can be used independently – making credential sharing or pooling hard to prevent. If these ephemeral keys are meant to be hardware-attested, e.g., being transferred over a device-authenticated channel, this hardware-attestation is likely to introduce linkable identifiers again. Solutions to hardware-based yet *unlinkable* authentication exist, but are based on zero-knowledge proofs (see Section 5.2 below).

[3] The EUDI regulation *Article 5a, §16 (b)* does not limit its requirement of unlinkability to only prevent identification of users under the assumptions the IdPs do not intentionally share or unintentionally leak current or previously issued credentials and/or national bodies compel both RP and IdP to correlate their respective logs.

[4] Note that current smartphone implementations only support a limited number of keys stored directly in secure hardware and may have to rely on more complex constructions with encrypted key blobs stored outside the secure hardware enclaves to deal with larger numbers.

From a security perspective, relying on a *single* key pair by the user is better—but this immediately destroys unlinkability with respect to RPs again, even when batch issuance of single-show credentials is used.

Thus, of the required privacy properties in the eIDAS regulation, the salted-hash solution laid out in the ARF satisfies selective disclosure and, at best, only a partial form of unlinkability/unobservability by the IdP and wallet issuer. Even the most privacy-friendly version of this approach — achieved, as explained above, at the expense of non-transferability — will leak the number of credentials used in a time period and, realistically, approximate timing of use depending on the validity period of credentials[5]. Notably, it cannot ensure unlinkability/untraceability with respect to colluding IdP and RPs, nor do we see a viable solution even for unlinkability with respect to RPs only that also provides non-transferability. Overall, we conclude that it **cannot ensure unlinkability** which is a mandatory ("shall") requirement in the regulation.

3 A Better Approach: Anonymous Credentials

In this section, we describe anonymous credentials, explain how to instantiate them, and analyze why they meet the mandated requirements.

3.1 Overview of Anonymous Credentials

What an anonymous credential looks like. A user receives a signature on his (hidden) secret key and a set of attributes; some of the attributes may also be hidden from the issuer (but known to the user), and some may be known to the issuer. The hidden attributes may, for example, serve as pseudorandom seeds for generating pseudonyms that are unique to this user's (wallet holder's) relationship with a particular verifier. The attributes that are known to the issuer may be ones that represent some meaningful information about the user, such as his age or place of residence, as attested by the issuer. In order to obtain an anonymous credential, the user and the issuer run a secure two-party computation protocol, in which only the user receives an output and neither party learns anything about the other's secret values.

What happens when a user presents his anonymous credential. The user may choose to reveal no information at all other than the fact that his credential attributes satisfy a particular policy, for example that the attribute corresponding to the user's date of birth is within a certain range that, say, qualifies this user for a senior discount. In a different context, the user may choose to reveal a lot of information about himself, for example, he may choose to reveal the exact values of some subset of attributes. In yet other situations, a user may choose to additionally reveal a pseudonym that uniquely corresponds to this user's relationship with a particular verifier; for example, this may be desirable in order to maintain a pseudonymous relationship over time, and to ensure that the user does not create Sybils of himself.

Other than the information that the user chooses to reveal, and who issued the credential, no other information, and no persistent identifiers that can be linked to another transaction of the same user, are revealed. Using a zero-knowledge proof, the user proves that the revealed information has been certified by the issuer. (Recall that in a zero-knowledge proof system, a prover—in this case, the user—convinces a verifier that a statement is true without revealing any information as to the evidence for why it's true.)

(There are cryptographic methods, called delegatable anonymous credentials, that would also hide the identity of the issuer among a set of trusted issuers such as the IdPs representing EU member states; however, they are not as well-established as the "vanilla" anonymous credentials we discuss here. In the future, it would be desirable to adopt them, however, as the identity of the credential issuer leaks a lot of information about the user, especially in the case when the user has credentials from several issuers.)

If the verifier algorithm accepts a credential presentation, that corresponds to a guarantee that it is talking to a user algorithm that is in possession of the cryptographic material (and, in particular, the secret key) that has been certified by the issuer.

[5] E.g., the Austrian implementation of ISO/IEC 18013-5 mDL uses validity periods below 1 hour at the time of this writing, forcing holders to fetch credentials immediately before use.

What public-key infrastructure is required to make this work. Similarly to the infrastructure for the Covid-19 digital credentials, all issuers need to establish public keys and obtain certificates from relevant authorities. A verifier will need to be able to ascertain that a given public key corresponds to a valid issuer.

Can a user share his credential with his friends? Any type of digital credential, anonymous or not, can be copied from one device to another. Any proposal for a digital credential needs to grapple with this fact. Mitigation strategies (outside the scope of this position paper) include storing the users' keys in secure enclaves (so that they are hard to transfer to another device) and rate limiting credential presentations (if the rate is exceeded, a user's secret is revealed and the user can be revoked). In fact, with the DAA [BCC04, DAA] and EPID [INT] protocols supported by TPM and SGX chips, solutions for privacy-preserving authentication based on anonymous credentials with hardware-protection of the secret key already exist and are in deployment.

Another approach is to bind credentials to custom-made hardware tokens that cannot be cloned; a user's photograph can be printed on a token like that so that if the user presents a credential in real life, a human verifier can verify the user's photo; this mitigation approach works with anonymous credentials as well [HSS23]. Finally, all-or-nothing credential sharing could make it sufficiently risky for holders to share their key material to disincentivize in practice.

Can anonymous credentials be revoked? Revocation is a hard problem in practice. Even for regular certificates (those without unlinkability guarantees, such as browser certificates) revocation is often not solved through cryptographic means in practice. The debates on CRLs and OCSP for WebPKIs have resulted in ISO/IEC 18013-5 mDL using short credential lifetimes instead of explicit credential revocation to accommodate practical deployment issues.

This approach works for anonymous credentials as well. To realize revocation through short-lived validity, the anonymous credential would contain an expiration date as dedicated attribute. When showing the credential, the owner then either discloses the attribute or proves in zero-knowledge that his credential hasn't expired yet.

3.2 Digital Signature Schemes Compatible with Anonymous Credentials

There are specific signature schemes that were designed with anonymous credentials in mind and come with highly efficient protocols for both issuing and presenting anonymous credentials. We consider anonymous credentials based on the BBS/BBS+ the ones that can be used "off the shelf", as there are various industry efforts for standardization and implementations available. This will be detailed in Sections 4 and 5.

BBS/BBS+ Signatures. The to-date most popular signature scheme supporting anonymous credentials is BBS [BBS04, CL04]. As the original BBS scheme did not have a proof of security, a slightly less efficient provably-secure variant, called BBS+, was proposed [ASM06, CDL16]. Recent work [TZ23] proves however that the original BBS achieves the same guarantees as BBS+. BBS can easily be extended to support blind credential issuance and pseudonyms, and a number of reference implementations are available. The size of BBS credentials is 80 bytes, whereas 112 bytes are needed by BBS+. BBS and BBS+ rely on special types of elliptic curves known as pairing-friendly, for which a number of libraries exist, as described for example in [SKSW22]. BBS credential presentation is very simple, and hinges upon the same simple zero-knowledge proof mechanisms that also underlie widely adopted signature schemes such as Schnorr Signatures and EdDSA.

Alternative schemes and approaches. There are a number of signature schemes in the same vein as BBS/BBS+, which however are not so popular in the industry setting. In particular, Camenisch-Lysyanskaya (CL) signatures from RSA-related assumptions [CL01] or also in pairing-friendly elliptic curve groups [CL04]. Moreover, there are Pointcheval-Sanders (PS) signatures [PS16].

We also want to briefly mention another line of work that builds anonymous credentials that are not multi-show unlinkable, i.e., where only the issuing and a single showing a unlinkable [BL13, KLR23].

Finally, in theory anonymous credentials can be instantiated with any digital signature scheme, together with general-purpose two-party computation and zero-knowledge proofs. For such generic techniques with existing widely adopted signature schemes (such as Schnorr Signatures and ECDSA), we highlight zero-knowledge proof systems in the Interactive Oracle Proof (IOP) model. IOPs have short and prover-efficient (i.e. user-efficient) proofs that only rely on collision-resistant hash functions.

3.3 Anonymous Credentials Fulfill the Regulation's Requirements

Selective disclosure. As we explained above, anonymous credentials enable selective disclosure. The user may choose to reveal a subset of his credential attributes, or nothing at all other than the fact that his attributes satisfy a given policy. The user then convinces the verifier, via a zero-knowledge proof, of the authenticity of the disclosed information.

Unlinkability. First, let us see that unlinkability with respect to Relying Parties (RPs) holds: When presenting a credential, recall that the user in an anonymous credential system provides (1) the selectively disclosed credential attributes (or a function of the attributes); and (2) a zero-knowledge proof that the revealed information is authentic. Since the proof is zero-knowledge, it does not reveal anything about the user other than what is revealed in (1), and thus the situation where the same user presents his credential twice is indistinguishable from the interaction with two distinct users with identical selectively disclosed attributes.

Next, let us see why this approach guarantees unlinkability with respect to Identity Provider. When a user presents a credential, all that needs to happen is that the user talk to the Relying Party. The only information that the Relying Party needs to obtain about the Identity Provider (IdP) is the Provider's public key and, in case a credential revocation mechanism is deployed, the latest revocation data. This is independent from who the user is. In fact, any architecture in which the RP does not query the IdP for verification and instead carries out verification locally by cryptographic means will satisfy unlinkability with respect to Identity Provider.

Finally, let us argue that unlinkability with respect to IdP & RPs holds. This is similar to unlinkability with respect to RPs: when presenting a credential to an RP, the user only reveals some selectively disclosed attributes. If the RP colludes with the IdP, together they cannot tell which user it is, unless there is only one user with this specific value for the selectively disclosed attributes.

Pseudonymous authentication. Enabling the usage of pseudonyms with an anonymous credential can be done by adding a cryptographically strong pseudorandom function seed s as a hidden attribute to a user's credential, and using this value s to establish the user's pseudonym(s) with RPs. In the use case where a user is only allowed one unique pseudonym with an RP R, this pseudonym can be $P = F(s, R)$, where F is a pseudorandom function. In case the use case allows for as many distinct pseudonyms as the user wants, it can be $P = F(s, N)$ where N is a fresh random nonce (drawn from a sufficiently large domain). In either case, in order to show that the owner of the pseudonym has a credential, the user will need to act as the prover in a zero-knowledge proof of knowledge of the seed s that is a valid hidden attribute of the user's credential. Note that the pseudonyms do not interfere with unlinkability since they are pseudorandom.

Unforgeability and Non-Transferability. Anonymous credentials provide at least the same level of unforgeability and non-transferability as their non-anonymous counterparts. In order for a Relying Party to accept a credential presentation, the user needs to carry out a zero-knowledge proof of knowledge of a signature; thus, the Identity Provider must have issued this credential, guaranteeing unforgeability.

Since any digital credential is represented by data, and data can be copied, steps must be taken to ensure that a user cannot simply copy a credential and give this copy to another user. In order to make this harder to do, it is important (no matter which underlying credential mechanism is used!) that each credential presentation be live/fresh, and require possession of a cryptographic key that is stored in secure hardware, so that it would be difficult to clone. These techniques work for anonymous credentials just as for any other type of credential. Moreover, an anonymous credential can be tied to a secure hardware token, as explored in the literature [HSS23] and briefly discussed in Section 3.1.

4 Standardization Efforts Related to Anonymous Credentials

We survey standardization efforts related to BBS(+) and other schemes related to anonymous credentials. We note that pairing-friendly curves (that are necessary for BBS) are not currently implemented in trusted phone hardware, and encourage the EC consider looking into the standardization of pairing-friendly elliptic curve groups.

World-Wide Web Consortium (W3C). The World-Wide Web Consortium (W3C) is the main standardization entity for web technology, and currently maintains a working group dedicated to verifiable credentials. The working group develops in particular standards to guide the adoption of verifiable credentials on the web, with the optional support of anonymity. Examples are a data model for verifiable credentials [W3C24b] and a ciphersuite for pairing-based BBS signatures [W3C24a] to support anonymous verifiable credentials.

The Linux Foundation. Although mostly known as a code organization (rather than a standards organization), the Linux Foundation does have a number of standards efforts focused on anonymous credentials and digital identity.

- **Hyperledger AnonCreds**: as the name suggests, this is a standard for anonymous credentials [Ano]. AnonCreds, short for "anonymous credentials", is a set of standards for verifiable credentials that support important privacy-preserving capabilities through the use of zero-knowledge proofs. The Hyperledger AnonCreds project contains specifications for AnonCreds, documentation, implementations and tests. Implementations of AnonCreds are present in other Linux Foundation efforts, including the Open Wallet Foundation and the Hyperledger Foundation.

  The current version of AnonCreds (version 1.0) is based on CL-signatures, but future versions (2.0) will be based on BBS signatures.

- **Decentralized Identity Foundation and RFC draft**: the Decentralized Identity Foundation involves a number of industry players, and promotes the development of standards for technologies which include anonymous credentials. Working groups are in particular responsible for the development of RFC drafts aimed at the standardization of cryptographic primitives that underlie anonymous credentials. Specifically, an RFC draft for BBS signatures [LKWL23] is currently being developed. This signature scheme possesses desirable properties making it the favored building block for a number of anonymous credential solutions. Two further RFC drafts build on top of it: A first one to support blind issuance of BBS credentials [KB24b] and one to include pseudonyms in BBS showing proofs [KB24a].

Internet Engineering Task Force (IETF). Within its IRTF Crypto Forum Research Group (CFRG) several Requests for Comments (RFCs) around the BBS signature scheme are currently developed. Specifically, an RFC for BBS signatures [LKWL23] is currently being developed. Two further RFCs build on top of it: A first one to support blind issuance of BBS credentials [KB24b] and one to include pseudonyms in BBS showing proofs [KB24a].

International Organization for Standardization (ISO). The anonymous credential protocols supported by TPM 2.0 are standardized in ISO/IEC 11889 and include one construction based on the BBS+ signature. There is also an ongoing standardization effort in form of a new work item proposal (NP) within ISO on *Privacy-Preserving Attribute-Based Credentials* within the ISO/IEC JTC1/SC 27 WG 2. It will consider anonymous credentials based on BBS(+) and PS signatures, and the standardization process is supposed to start this year.

5 Real-World Examples of Anonymous Credentials

Though standardization efforts for anonymous credentials are ongoing, anonymous credentials have been used in quite a few real-world systems. These include some projects funded by the EU, such as the EU-project PrimeLife and the EC-funded project Attributes based Credentials for Trust (ABC4Trust). PrimeLife implemented an Idemix-based system [Pri] that uses anonymous credentials, and one of the selected solutions for ABC4Trust also used Idemix.[6] We outline open-source implementations and real-world use cases outside of the EU/EC below.

5.1 Open-Source Implementations

We list a number of open-source implementations of anonymous credentials below.

The Linux Foundation. There are quite a few code projects in the Linux Foundation that are essentially focused on anonymous credentials. These include the following:

- **Aries Bifold**, in the Open Wallet Foundation [OWFa]. Bifold is designed to make it easy for users to handle their digital identities and digital credentials. Bifold is based on React Native, so it can run smoothly on many different devices and platforms like iOS and Android. Bifold is based on the Aries stack so it currently supports CL signature-based credentials, but will eventually support BBS+ when AnonCreds 2.0 is released.

- **Credo**, also in the Open Wallet Foundation [OWFb], is an agent framework written in Typescript that implements the Aries RFCs. Thus, it currently supports CL signatures.

  As a side note, Credo is one of the few open-source digital identity projects that is primarily maintained by development teams based out of Europe.

- **Hyperledger Aries**, in the Hyperledger Foundation [Ari] is a project that contains a number of subprojects that support many different use cases in decentralized identity and verifiable credentials. These include ACA-Py, Aries Framework .Net, and Aries Static Agent Python. Each of these projects support anonymous credential presentations, and they also use CL signatures. Future plans include moving to BBS+ signatures.

The Yivi App & IRMA. Yivi is a Dutch app that implements anonymous credentials based on Idemix, together with all necessary backend infrastructure. The app can be used with some Dutch municipalities and government services, as well as the private sector. It consists of an app which stores user credentials on a phone. In addition, a backend system called IRMA allows issuing credentials as well as implementing communication with the app for the verifier. The implementation is open sourced, and contains advanced features such as proofs of non-revocation. See https://irma.app/docs/what-is-irma/ for more information.

5.2 Real-World Use Cases

There are a number of use cases where anonymous credentials have been actively deployed.

[6] A search using the search term "anonymous credentials" in the CORDIS database (https://cordis.europa.eu/) actually yields 11 projects funded by the European Commission that are related to this topic.

Unlinkable Hardware Attestation (DAA/SGX EPID). Establishing trust with high assurance guarantees often requires secure hardware, e.g., TPMs or secure enclaves. The secure element can be used to authenticate a secure channel, to bind (ephemeral) keys to a device, or attest further information. This requires the recipient of the hardware-attested information to verify that it is indeed communicating with a trusted hardware anchor. Realizing such hardware-based authentication with standard signatures would make all attestations linkable. To avoid this, dedicated anonymous credential protocols have been developed and are already implemented in millions of devices. The Direct Anonymous Attestation (DAA) protocol of the Trusted Computing Group is part of the TPM 1.2 specification since 2004 [BCC04]. The first version used an RSA-based protocol, which was revised in 2014 with TPM 2.0 [DAA] switching to elliptic-curve schemes for efficiency and crypto agility. The interfaces standardized and implemented in TPM 2.0 can be used by a suite of protocols, all only relying on a small *device-binding* part by the TPM. As mentioned in Section 4, the anonymous credential protocols supported by TPM 2.0 are standardized in ISO/IEC 11889, and include the BBS+ signature. Similarly, Intel's SGX uses a DAA variant in their Enhanced Privacy ID (EPID) protocol for hardware attestation, and more than 2.5 billion Intel EPID credentials have been issued since 2008 [INT].

Government of British Columbia Use Cases. The government of British Columbia, Canada has been extremely effective at open-source participation and bringing open-source standards and implementations of anonymous credentials into practice. We outline some of their efforts below. We note that these use cases use the Linux Foundation stack of tools, and are thus currently based on CL signatures. However, the BC Government has expressed interest in moving to BBS+-based credentials in the future, or even post-quantum versions of PS signatures [JRS23].[7]

- **British Columbia Energy and Mines Digital Trust** [BCG]. Energy & Mines Digital Trust (EMDT) uses decentralized identity tools to support sustainable economic development while maintaining transparency and high levels of environmental protection for British Columbia's natural resources. More precisely, EMDT enables mining and energy operators to prove where and how their products were made in a way that is both secure and efficient using digital credentials.

  In order to compete in global markets where provable sustainability is important, mining and energy operators need to be able to prove to suspect customers that there methods are, in fact, sustainable. Digital credentials enable operators to efficiently and transparently demonstrate their commitment to environmental, social and governance goals, increasing trust in global supply chains.

- **The Justice Project** [BCJ]. The justice project is a system of digital credentials for lawyers in British Columbia. It enables these lawyers to access sensitive court documents online in a privacy-preserving manner.

- **OrgBook BC** [Org]. OrgBook is, to our knowledge, the first production use case of anonymous credentials by government. OrgBook BC enables organizations and citizens to easily access verified information about registered BC organizations. OrgBook BC has over 1.4 million active legal entities, has over 3.8 million VCs, and is usually updated within minutes of a new or changed registration. This has proved its ability, and Hyperledger Aries' and Indy's abilities (upon which it is based), to scale and support real-world scenarios.

SITA Digital Travel Credentials. From an announcement [SIT]: "SITA, the leading IT provider to the air transport industry, and the Government of Aruba today showcased the successful implementation of verifiable digital credential technology, eliminating the need for passengers to show their physical passport when arriving on the island. Speaking together in a keynote discussion at the ICAO TRIP conference taking place in Montreal this week, Jeremy Springall, SVP of SITA AT BORDERS, and Andrew Hoo, Director of Immigration for the Government of Aruba, highlighted that the development of Digital Travel Credentials

[7] We encourage you to check out their statements on this in the AnonCreds v2 specification github [Ano] or even reach out to them directly on this topic; they are almost always available in the Hyperledger and Open Wallet Discords.

enables passengers to securely create a digital version of their physical passport on their mobile device in line with the International Civil Aviation Organization (ICAO) standards. ”

These digital credentials use the Linux Foundation anonymous credentials stack, including Hyperledger AnonCreds and Aries projects. SITA also employs CL signatures.

Signal Messenger. The secure messaging app Signal uses (keyed-verification) anonymous credentials to implement private groups [CPZ20][8].

6 Countering Future Quantum Threats

Due to the prevalence of the quantum threat topic and the planning to migrate to quantum safe (aka post-quantum) cryptography, we feel that it is important that this also needs to be discussed in context of anonymous credentials. We first note that anonymous credentials are used for authentication and thus the integrity protection is very short lived and does not need to be guaranteed for a very long time. Consequently, as for most use-cases of signatures (apart from specific use cases like long-term archiving), the switch to post-quantum alternatives is not extremely urgent. This is in stark contrast to encryption schemes, where due to the “store now decrypt later” problematic a switch to post-quantum encryption schemes needs to happen timely. Otherwise data that needs to be kept confidential for a longer period of time is endangered.

Moreover, in context of anonymous credentials there is another important aspect to note from a privacy perspective. Namely, if the privacy property of an anonymous credential system is *unconditional* then even when instantiated from building blocks that could be broken by a hypothetical quantum computer, the privacy is not endangered and will hold forever (even when given unlimited computing power). We note that for the BBS family of anonymous credentials, the privacy property holds unconditionally.

Currently, there do not exist anonymous credential schemes that are plausibly post-quantum secure, scalable to the eIDAS setting and have high quality software implementations. At the same time, the hash and signature-based mechanism currently being proposed is neither post-quantum secure nor privacy-preserving. It is therefore prudent that processes exist so that the cryptography being deployed in the EUDI can be updated to a new, post-quantum standard whenever it becomes necessary and possible.

Following the success in the NIST Post-Quantum Standardization [NIS], it seems very likely that constructions based on lattice assumptions will form the future foundation of quantum-safe public-key cryptography. Hence, naturally several constructions of lattice-based anonymous credentials have recently been proposed [LCL$^+$23, BLNS23, JRS23], together with a proof-of-concept implementation [LSS24]. Although, as of now, the current constructions do not seem well-studied enough in terms of security and efficiency for such a wide deployment, such lattice-based solutions for anonymous credentials may likely become one of the most efficient quantum-safe options in a few years time.

References

[Ano] Hyperledger anoncreds. URL: https://wiki.hyperledger.org/display/anoncreds.

[ARF24] The european digital identity wallet architecture and reference framework, 2024. URL: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/.

[Ari] Hyperledger aries. URL: https://github.com/hyperledger/aries.

[ASM06] Man Ho Au, Willy Susilo, and Yi Mu. Constant-size dynamic k-TAA. pages 111–125, 2006. doi:10.1007/11832072_8.

[8] https://signal.org/blog/signal-private-group-system/

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. pages 41–55, 2004. doi:10.1007/978-3-540-28628-8_3.

[BCC04] Ernest F. Brickell, Jan Camenisch, and Liqun Chen. Direct anonymous attestation. pages 132–145, 2004. doi:10.1145/1030083.1030103.

[BCG] Energy & mines digital trust. URL: https://digital.gov.bc.ca/2023/07/26/energy-mines-digital-trust-pilot/.

[BCJ] Justice project. URL: https://digital.gov.bc.ca/digital-trust/justice-project/.

[BL13] Foteini Baldimtsi and Anna Lysyanskaya. Anonymous credentials light. pages 1087–1098, 2013. doi:10.1145/2508859.2516687.

[BLNS23] Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Alessandro Sorniotti. A framework for practical anonymous credentials from lattices. pages 384–417, 2023. doi:10.1007/978-3-031-38545-2_13.

[CDL16] Jan Camenisch, Manu Drijvers, and Anja Lehmann. Anonymous attestation using the strong diffie hellman assumption revisited. In Michael Franz and Panos Papadimitratos, editors, *Trust and Trustworthy Computing - 9th International Conference, TRUST 2016, Vienna, Austria, August 29-30, 2016, Proceedings*, volume 9824 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2016. doi:10.1007/978-3-319-45572-3_1.

[CL01] Jan Camenisch and Anna Lysyanskaya. An identity escrow scheme with appointed verifiers. pages 388–407, 2001. doi:10.1007/3-540-44647-8_23.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. pages 56–72, 2004. doi:10.1007/978-3-540-28628-8_4.

[CPZ20] Melissa Chase, Trevor Perrin, and Greg Zaverucha. The Signal private group system and anonymous credentials supporting efficient verifiable encryption. pages 1445–1459, 2020. doi:10.1145/3372297.3417887.

[DAA] Trusted platform module library specification. URL: https://trustedcomputinggroup.org/resource/tpm-library-specification/.

[eID24] Regulation (eu) 2024/1183 of the european parliament and of the council of 11 april 2024 amending regulation (eu) no 910/2014 as regards establishing the european digital identity framework, 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1183/oj.

[Ger24] Architecture proposal for the german eidas implementation, 2024. URL: https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept/-/blob/main/architecture-proposal.md.

[HSS23] Julia Hesse, Nitin Singh, and Alessandro Sorniotti. How to bind anonymous credentials to humans. In Joseph A. Calandrino and Carmela Troncoso, editors, *32nd USENIX Security Symposium, USENIX Security 2023, Anaheim, CA, USA, August 9-11, 2023*, pages 3047–3064. USENIX Association, 2023. URL: https://www.usenix.org/conference/usenixsecurity23/presentation/hesse.

[INT] INTEL. A cost-effective foundation for end-to-end iot security. URL: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/intel-epid-white-paper.pdf.

[ISO21] ISO/IEC 18013-5:2021. Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application. International Standard, International Organization for Standardization, 2021.

[JRS23] Corentin Jeudy, Adeline Roux-Langlois, and Olivier Sanders. Lattice signature with efficient protocols, application to anonymous credentials. pages 351–383, 2023. doi:10.1007/978-3-031-38545-2_12.

[KB24a] Vasilis Kalos and Greg M. Bernstein. BBS per Verifier Linkability. Internet-Draft draft-vasilis-bbs-per-verifier-linkability-00, Internet Engineering Task Force, March 2024. Work in Progress. URL: https://datatracker.ietf.org/doc/draft-vasilis-bbs-per-verifier-linkability/00/.

[KB24b] Vasilis Kalos and Greg M. Bernstein. Blind BBS Signatures. Internet-Draft draft-kalos-bbs-blind-signatures-00, Internet Engineering Task Force, January 2024. Work in Progress. URL: https://datatracker.ietf.org/doc/draft-kalos-bbs-blind-signatures/00/.

[KLR23] Julia Kastner, Julian Loss, and Omar Renawi. Concurrent security of anonymous credentials light, revisited. pages 45–59, 2023. doi:10.1145/3576915.3623184.

[LCL+23] Qiqi Lai, Chongshen Chen, Feng-Hao Liu, Anna Lysyanskaya, and Zhedong Wang. Lattice-based commit-transferrable signatures and applications to anonymous credentials. *IACR Cryptol. ePrint Arch.*, page 766, 2023. URL: https://eprint.iacr.org/2023/766.

[LKWL23] Tobias Looker, Vasilis Kalos, Andrew Whitehead, and Mike Lodder. The BBS Signature Scheme. Internet-Draft draft-irtf-cfrg-bbs-signatures-05, Internet Engineering Task Force, December 2023. Work in Progress. URL: https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/05/.

[LSS24] Vadim Lyubashevsky, Gregor Seiler, and Patrick Steuer. Lazer: a lattice library for zero-knowledge and succinct proofs, 2024. URL: https://iacr.org/submit/files/slides/2024/rwc/rwc2024/125/slides.pdf.

[NIS] Nist post-quantum cryptography standardization. URL: https://csrc.nist.gov/projects/post-quantum-cryptography.

[Org] Orgbook bc. URL: https://digital.gov.bc.ca/2023/07/26/orgbook-bc/.

[OWFa] Aries bifold wallet project. URL: https://github.com/openwallet-foundation/bifold-wallet.

[OWFb] Credo. URL: https://github.com/openwallet-foundation/credo-ts.

[Pri] Primelife identitiy mixer cryptographic library. URL: http://primelife.ercim.eu/results/opensource/55-identity-mixer.

[PS16] David Pointcheval and Olivier Sanders. Short randomizable signatures. pages 111–126, 2016. doi:10.1007/978-3-319-29485-8_7.

[SIT] Sita and aruba demonstrate how physical passports can be held as a digital identity on your mobile device. URL: https://www.sita.aero/pressroom/news-releases/sita-and-aruba-demonstrate-how-physical-passports-can-be-held-as-a-digital-identity-on-your-

[SKSW22] Yumi Sakemi, Tetsutaro Kobayashi, Tsunekazu Saito, and Riad S. Wahby. Pairing-Friendly Curves. Internet-Draft draft-irtf-cfrg-pairing-friendly-curves-11, Internet Engineering Task Force, November 2022. Work in Progress. URL: https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves/11/.

[TZ23] Stefano Tessaro and Chenzhi Zhu. Revisiting BBS signatures. pages 691–721, 2023. doi:10.1007/978-3-031-30589-4_24.

[W3C24a] Data integrity bbs cryptosuites v1.0, 2024. URL: https://www.w3.org/TR/vc-di-bbs/.

[W3C24b] Verifiable credentials data model v2.0, 2024. URL: https://www.w3.org/TR/vc-data-model-2.0/.