# The Security and Privacy Benefits of Including Decentralized Identifiers (DIDs) in the European Digital Identity Wallet Architecture and Reference Framework

Posted 9 July, 2024

## Introduction

Privacy, security, and individual empowerment are fundamental considerations for a digital identity system. We commend the European Digital Identity Wallet Architecture and Reference Framework (EUDIW ARF) team for their dedication to the goals of "user-centricity, privacy, security, and cross-border interoperability"[1] and commitment to a wallet architecture based on privacy-by-design. In its design principles, the ARF underscores:

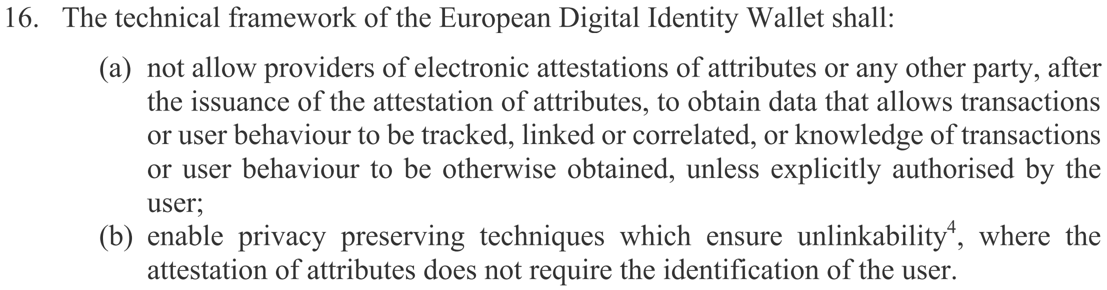
> "...the protection of user data is a fundamental pillar of the wallet's design. The principle of data minimisation guides the collection of personal information, ensuring only what is necessary is gathered."[2]

Further, we also thank you for fostering an open feedback process. In that spirit, we recommend that incorporating Decentralized Identifiers (DIDs) into the ARF will further enhance these goals and enable a more robust, resilient, and interoperable ecosystem.

## Summary of Concerns

### 1. Privacy and Linkability

Regulation (EU) 2024/1183[3] establishing the European Digital Identity Framework sets a high bar with regard to user privacy concerns including tracking, linking, and correlation. Article 5a specifies that:



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[4], where the attestation of attributes does not require the identification of the user.

The ARF does not currently evaluate the behavior of the selected technical standards against these requirements; however, in section 7.4, it outlines plans to develop a common risk register to “categorise threats such as spoofing, tampering, information disclosure, or linking”[5] and use a risk-based approach to evaluate vulnerabilities.

The common risk register and risk-based approach are sound elements of a solution. However, the current technical selections of the ARF set it at a disadvantage in meeting the regulatory requirements, as described in this section.

The ARF’s approach to ensuring non-transferability of credentials is based on “device binding”, or proving that an attestation is bound to a specific device by request, via cryptographic keys bound to the device. However, the current method of approximating unlinkability across presentations of the credential is through use of batch issuance of credentials, using a distinct key for each intended use of the credential. Note this turns each credential instance into effectively a single-use credential, and does not satisfy the requirements of full unlinkability.[6]

As Cryptographers' Feedback[7] outlines, this partial solution to unlinkability results in large numbers of hardware-bound keys and credentials per credential type. This approach is already difficult for wallets to manage properly and will continue to be impacted by the capacity of a hardware device’s secure element. This problem is further compounded by the need for wallets to request entirely new batches of credentials from Issuers on key rotation or expiration. These factors complicate the financial and operational costs[8] for the ecosystem.

A further avenue for privacy risks is the “phone-home” challenge associated with JWT VC Issuer Metadata[9], which could enable issuers and verifiers to track the use of credentials. The mitigations and recourse for the user are currently underdeveloped in contrast to other alternatives, outlined below.

## 2. Technical Neutrality

The EU ARF acknowledges in Section 7.2.1 that “the amending [eIDAS 2] Regulation is technology and architecture neutral”. As such, it is crucial to distinguish between, on the one hand, what constitutes a “technology” decision, and on the other hand, what constitutes a “governance” decision of how that technology is implemented in a particular scheme to meet a required level of assurance.

Like X.509 certificates, DID implementations are a container for storing key agreement and authentication mechanisms. Both technologies can support a variety of cipher suites, cryptographic curves and protocols with agnosticism. However, one crucial difference between these two technologies is that X.509 certificates have operated within “governed” schemes to establish trust, such as eIDAS 1.0. Yet, simply because X.509 certificates have proved a successful model for trust establishment historically, we should not preclude new governance schemes from choosing another container for key management, especially when there is no detriment to cryptographic security and an increase in anti-correlation capabilities.

This is particularly pertinent for the EU ARF which seeks to establish a toolbox within which **both public and private entities** can operate, as well as, supporting **both "qualified" ((Q)EAA) and "non-qualified" Electronic Attestation of Attribute (EAA) providers**. For example, take a "non-qualified EAA" that operates in the EU, but is accredited under the Swiss eID scheme. Under the Swiss scheme, the EAA has a DID accredited by a Swiss Public Governance Authority, verifiable against a DID-based trust registry. The EAA can use this DID to issue digital credentials with complete compatibility with EUDI wallets. A relying party in the EU should be able to trust the Swiss-issued credential if it: (1) Meets a certain level of assurance and conforms to the cryptography requirements for interoperability in the EU; and (2) Meets the required governance requirements for Switzerland and can be verified against a recognized trust registry, regardless of the container that the underlying keys are stored in. Fundamentally, without a broader stroke approach to technical neutrality, and acknowledging the potential for DIDs to act as a key management format, the EU ARF risks stifling progression, innovation and interoperability between "qualified" and "non-qualified" EAAs.

## Decentralized Identifiers

Decentralized Identifiers (DIDs)[10] became a full W3C Recommendation in July 2022, enabling verifiable digital identifiers controlled by individuals and organizations. This new class of Internet identifiers support cryptographic best practices, such as key rotation, which reduce the key and credential management challenges outlined above. DIDs enable the cryptographic agility necessary to future-proof against emerging threats. In combination with zero knowledge signature schemes and Peer DID implementations, DIDs provide privacy improvements that inhibit the correlation of people, devices, and activities. Additionally, DIDs provide robust security across communication channels, enabling endpoint discovery and mutual authentication.

## Improved Privacy and Empowerment for Individuals

DIDs offer EU citizens greater control over their credentials while promoting privacy and cryptographic best practices. DID identifiers "resolve" to a DID document that contains cryptographic keys, service endpoints, and other communication metadata. This allows updates to the DID document, such as cryptographic key rotation, without changing the DID itself.

When used by Issuers and Holders, DIDs enable the following improvements for subjects:

1. Verifiable Credential (VC) robustness:
    a. Holders can continue to use VCs that were signed by an Issuer with a DID, even if the Issuer has rotated the corresponding cryptographic key. (If needed, issuers can explicitly revoke VCs, but key rotation does not necessarily invalidate previously issued claims.)
    b. Holders can rotate their cryptographic keys and continue to prove they control the credentials associated with a DID.

2. Improved privacy:
    a. DIDs support a protocol-neutral way of distributing and retrieving issuer metadata including public keys, with clear mitigations for reducing the ability for tracking.
    b. Combined with zero-knowledge mechanisms like BBS Signatures[11], DIDs allow the credential Holder to prove valid possession of the credentials while not revealing trackable identifiers or unnecessary metadata.
3. Interoperability:
    a. DIDs enable a provider-neutral way of establishing verifiable trust.
    b. EU member states are tasked with creating at least one digital wallet, which must conform to interoperability requirements. Systems may be interoperable, yet based on different technologies.
    c. Adding DID support will enable EU member states to support wallets, credentials, apps, etc. (each having compatible security and privacy-enhancing features), which can be based on distinct technology implementations while remaining interoperable with other member states and commercial solutions.

In this manner, DIDs avoid tight coupling between cryptographic keys, identifiers, credentials, and cryptographic signatures, reducing key management complexity and offering improved privacy guarantees.

## Broad Existing Implementations and Support

DIDs are widely used and deployed today. DIDs are a core component of European Blockchain Services Infrastructure (EBSI)[12] and are already in use in the DC4EU Large Scale Pilots[13]. They are used in other major European projects and infrastructures, including Gaia-X[14] and Catena-X[15]. Adopting DIDs in the ARF would simplify interoperability with these other major EU initiatives.

DIDs are used across a range of industries, including trade, retail, travel, and education, and by organizations, including those listed in Appendix: Partial List of DID Deployments.

## Interoperability and Future-Proofing

DIDs have been increasingly selected across industries and organizations for their ability to enable interoperability across technical stacks and ecosystems. Introducing DIDs into the ARF increases interoperability with the deployments listed in the Appendix: Partial List of DID Deployments. One example of this recommended interoperability would be to enable the integration of EBSI and its trust model into the EUDI Wallet. Emerging draft specifications such as W3C DID-Linked Resources provide a mechanism to bind digital files.  This binding may include status lists, schemas, trust registry data, etc. to be controlled and updated using DID controllers, which provide a decentralized mechanism that addresses some of the key challenges facing EUDI.

Another key advancement that using DIDs introduces is a convenient way of achieving cryptographic agility.  This facilitates adding improved cryptographic mechanisms to a constant standard as cryptographic advancements emerge. Additionally, this allows seamless integration of privacy-enhancing technologies, such as private holder binding and non-correlatable signature schemes, without reissuing credentials.

## Addressing Misconceptions

1. **DIDs result in a correlatable identifier**: In fact, Issuers (commonly, legal entities) and Subjects (commonly, natural persons) use different types of DID methods appropriate to their requirements. For example, Digital Credentials for Europe (DC4EU) educational & professional qualifications rulebook specifies the use of decentralized PKI (dPKI) certificates using did:ebsi for legal entities and did:key for natural persons. Legal entities register DIDs in the EBSI DID registry, while natural persons do not, enabling GDPR compliance. In other scenarios, after initial identification, both legal entities and natural persons may employ Peer DIDs, which are unique to their specific connection and not correlatable.
2. **DIDs are only for blockchain-based systems:** DIDs can be implemented in various contexts, including centralized and distributed systems, including non-blockchain methods like did:dht, did:tdw and did:web. The DID Core specification and DID methods provide a unified set of properties for resolution of public keys and other metadata needed for digital identity use cases. This technical stack-agnostic approach explicitly supports technology evolution.
3. **DIDs are complex and difficult to implement:** DIDs are Uniform Resource Identifiers (URIs), similar to standard website URLs. This makes them very familiar to typical web users and easy to use by non-web users alike. The DID Core specification and associated standards are designed to be straightforward, with numerous resources and tools available to simplify implementation. Adoption is sufficiently mature that there are open-source libraries, SDKs, and services for developers to reuse if they don’t want to work directly with the DID specification.
4. **DIDs are not widely adopted or supported:** DIDs have significant and growing support across governments, as well as multiple industries and market verticals, with real-world implementations demonstrating their effectiveness. Gaps around DID resolution and dereferencing are actively being addressed by the rechartered[16] W3C DID working group.
5. **There are nearly 200 DID methods, building support for them all is unrealistic**: Implementations choose which DID methods to support based on their particular requirements. Evaluation frameworks[17] are available to help implementers navigate DID Methods, and the W3C DID WG is further clarifying conformance requirements[18]. This work intends to showcase the more serious, feature-complete methods that prioritize interoperability and advanced functionality such as key rotation, delegation, diverse verification method relationships, DID URL dereferencing and DID-Linked Resources.
6. **The benefits of DIDs can be achieved using traditional PKI**: Decentralized identifiers (DIDs) can interoperate with Public Key Infrastructure (PKI) and, paired with Verifiable Credentials, can support a broader range of assertions to be verifiably conveyed through a trust chain. Removing the dependence on Certificate Authorities allows scalability and adaptability to different trust frameworks. As highlighted previously, this includes EBSI.

## Specific Requests

For the reasons outlined above, we request that the EUDI Wallet ARF explicitly includes support for DIDs as defined by the W3C DID Core Specification to ensure interoperability and future-proofing.

We further invite ongoing collaboration with the DID community, including organizations like the World Wide Web Consortium (W3C), Decentralized Identifier Foundation (DIF), and Trust Over IP (ToIP), to stay aligned with best practices and leverage the collective expertise of the community.

## Conclusion

In conclusion, we believe the inclusion of Decentralized Identifiers (DIDs) in the EUDIW ARF will significantly enhance the framework's security, privacy, resilience, interoperability, and future-proofing. We sincerely appreciate the opportunity to provide feedback and we would welcome any questions.

**Endorsed By:**

Decentralized Identity Foundation
Digital Credentials Consortium
Trust Over IP Foundation

## Appendix: Partial List of DID Deployments

**Education**

- Arizona State University Trusted Learner Network (ASU TLN)[19]
- Digital Credentials Consortium (DCC)[20], a consortium including Delft University of Technology (The Netherlands), Georgia Institute of Technology (USA), Harvard University (USA), Hasso Plattner Institute, University of Lille (France), University of Potsdam (Germany), Massachusetts Institute of Technology (USA), McMaster University (Canada), Tecnológico De Monterrey (Mexico), Technical University of Munich (Germany), University of California, Berkeley (USA), University of California, Irvine (USA), University of Milano-Bicocca (Italy), University of Toronto (Canada), Western Governors University (USA)

**Finance**

- Block with TBD and tbDEX[21]
- Privado (formerly Polygon)[22]

**Government**

- Bhutan Government National Digital Identity (NDI)[23]
- California Department of Motor Vehicles (DMV)[24]
- Government of British Columbia (BCGov)[25]
- New Zealand COVID-19 vaccination certificates[26]
- Singapore National Digital Identity (NDI)[27]
- Swiss E-ID & Trust Infrastructure[28]
- U.S. Citizenship and Immigration Services[29]
- US Customs and Border Protection (CBP)[30]
- US Department of Homeland Security (DHS)[31]

**Travel, Aviation, and Automotive**

- International Air Transport Association (IATA) Digital Identity[32]
- Catena-X[33]

**Retail & Age Verification**

- The National Association of Convenience Stores, TruAge, and Verifone[34]

**Workforce and Human Resources**

- Jobs for the Future Foundation Interoperability Profile[35]
- Velocity Network[36]

### Digital Public Infrastructure

- European Blockchain Services Infrastructure (EBSI)[37]
- Gaia-X[38]
- MOSIP (Modular Open Source Identity Platform)[39]

[1] The European Digital Identity Wallet Architecture and Reference Framework, 2024. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/

[2] The European Digital Identity Wallet Architecture and Reference Framework, 2024. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/

[3] REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 11 April 2024, https://eur-lex.europa.eu/eli/reg/2024/1183

[4] Correction from "unlikeability" [SIC]

[5] The European Digital Identity Wallet Architecture and Reference Framework, 2024. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.4.0/arf/

[6] ETSI TR 119 476 V1.2.1 (2024-07), section 7.3.3 note 2, https://www.etsi.org/deliver/etsi_tr/119400_119499/119476/01.02.01_60/tr_119476v010201p.pdf

[7] Cryptographers' Feedback on the EU Digital Identity's ARF, 2024, https://github.com/user-attachments/files/15904122/cryptographers-feedback.pdf

[8] Also highlighted in ETSI TR 119 476 V1.2.1 (2024-07), section 7.3.3 note 1, https://www.etsi.org/deliver/etsi_tr/119400_119499/119476/01.02.01_60/tr_119476v010201p.pdf

[9] SD-JWT-based Verifiable Credentials (SD-JWT VC), https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/

[10] Decentralized Identifiers (DIDs) v1.0, https://www.w3.org/TR/did-core/

[11] The BBS Signature Scheme, https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/

[12] DID method is determined by the user type (legal entity or natural person) and their respective privacy requirements. DC4EU educational & professional qualifications rulebook specifies use of decentralized PKI (dPKI) certificates using did:ebsi for legal entities and did:key for natural persons. Legal entities register DIDs in the EBSI DID registry, while natural persons do not (enabling GDPR compliance)

[13] https://www.dc4eu.eu/

[14] https://gaia-x.eu/wp-content/uploads/2022/06/SSI_White_Paper_Design_Final_EN.pdf

[15] https://catena-x.net/fileadmin/user_upload/Standard-Bibliothek/Update_September23/CX-0049-DIDDocument-v.1.0.0.pdf

[16] Decentralized Identifier Working Group Charter, 25 April 2024, https://www.w3.org/2024/04/did-wg-charter.html

[17] This includes DID Method Rubric v1.0 https://www.w3.org/TR/did-rubric/ and an upcoming DIF work item called "DID Traits"

[18] DID WG Charter, 2024, https://www.w3.org/2024/04/did-wg-charter.html

[19] https://tech.asu.edu/initiatives/trusted-learner-network

[20] https://digitalcredentials.mit.edu/docs/white-paper-building-digital-credential-infrastructure-future.pdf

[21] https://developer.tbd.website/docs/web5/learn/decentralized-identifiers/

[22] https://docs.polygon.technology/pos/how-to/polygon-did/

[23] https://mobileidworld.com/case-study-details-bhutans-pioneering-digital-id-effort/

[24] https://www.dmv.ca.gov/portal/ca-dmv-wallet/opencred-for-developers/

[25] https://diacc.ca/wp-content/uploads/2021/10/DIACC_BC-Governments-Verifiable-Credential-Issuer-Kit_Proof-of-Concept-Report_ENG.pdf

[26] https://github.com/minhealthnz/nzcovidpass-spec

[27] https://www.developer.tech.gov.sg/our-digital-journey/digital-government-exchange/files/DGX%20DIWG%202022%20Report%20v1.5.pdf

[28] https://github.com/e-id-admin/open-source-community/blob/main/tech-roadmap/tech-roadmap.md

[29] https://www.dhs.gov/science-and-technology/news/2024/07/09/feature-article-question-who-you-are

[30] https://www.cbp.gov/trade/innovation/leading-global-interoperability-standards

[31] https://www.dhs.gov/science-and-technology/news/2023/06/22/st-seeks-solutions-privacy-preserving-digital-credential-wallets-verifiers

[32] https://www.iata.org/contentassets/1f2b0bce4db4466b91450c478928cf83/oneid-factseet-verified-credentials.pdf

[33] https://catena-x.net/fileadmin/user_upload/Standard-Bibliothek/Update_September23/CX-0049-DIDDocument-v.1.0.0.pdf

[34] The National Association of Convenience Stores, TruAge, and Verifone also support them across their point of sale product line (which is 60% of the checkout systems in the US; 1,650+ retail brands) https://www.convenience.org/Media/Daily/2023/October/4/1-Verifone-Integrates-With-TruAge_Tech

[35] https://kayaelle.medium.com/jff-vc-edu-plugfest-1-892b6f2c9dfb

[36] https://www.velocitynetwork.foundation/main/career-wallets-key-management

[37] DID method is determined by the user type (legal entity or natural person) and their respective privacy requirements. DC4EU educational & professional qualifications rulebook specifies use of decentralized PKI (dPKI) certificates using did:ebsi for legal entities and did:key for natural persons. Legal entities register DIDs in the EBSI DID registry, while natural persons do not (enabling GDPR compliance)

[38] https://gaia-x.eu/

[39] https://connect.mosip.io/resources_pdf/2.%20Inside%20MOSIP%20-%20Shrikant,%20Resham,%20Harini.pdf, https://github.com/mosip/inji-verify/blob/091b7cd22cfe3c267360dfd6702c9d3ab84fa672/inji-verify/src/utils/did-utils.ts#L5