

Regulatory options for integrating zero-knowledge proofs into the European Digital Identity Wallet

Raül Ramos Fernández¹

Abstract

On 30 April, Regulation (EU) 2024/1183 amending Regulation (EU) 910/2014 as regards establishing the European Digital Identity Framework, known as eIDAS 2.0, was published in the Official Journal of the European Union. This amendment introduces zero-knowledge proof (ZKP) privacy-enhancing technologies to support two key innovations: the European Digital Identity Wallet (EUDIW) and the electronic attestations of attributes ((Q)EAA). In parallel, the European Digital Identity Wallet Architecture and Reference Framework (EUDIW ARF) provide a common set of standards and best practices for the technical implementation of eIDAS 2.0. This paper analyses how the EUDIW can rely on ZKPs since neither the eIDAS 2.0 Regulation nor the EUDIW ARF does so. We propose a software product regime for the cryptographic derivation of data in a ZKP format through three mutually compatible regulatory options: zero-knowledge issuance by default through the EUDIW, through a software product extension of the EUDIW, or a private standalone wallet. These schemes provide the legal basis for the secure use of ZKPs, ensure effective compliance with the GDPR, and contribute to the debate on the value that electronic ledgers introduced by eIDAS 2.0 bring to digital identity.

Keywords: eIDAS 2.0; ZKP; European Digital Identity Wallet; electronic attestations of attributes; data protection; electronic ledgers.

¹ Raul.RamosF@autonoma.cat

<https://orcid.org/0000-0001-7344-6140>

<https://www.linkedin.com/in/raül-ramos-fernández-776208162/>

Department of Public Law and Legal History Studies, Faculty of Law, Building B2, c. de la Vall Moronta, 08193 Bellaterra (Cerdanyola del Vallès) Autonomous University of Barcelona, Catalonia, Spain

1. Introduction

Digital identity is a key concept for the development of the information society and the Digital Single Market in Europe. However, digital identity management poses significant security, privacy, and trust challenges. On the one hand, there is a need to ensure the authentication and identification of digital users and service providers, as well as the integrity and validity of the data and information they exchange. On the other hand, the right to personal data protection and the principle of data minimisation must be respected, avoiding unnecessary or excessive disclosure of sensitive or identifying information. In this context, zero-knowledge proof (ZKP) protocols, as described by Goldwasser, Micali, and Rackoff (1985), emerge as a promising technology to enhance the security and privacy of digital identity by allowing the proof of properties or attributes without revealing the underlying data (Bamberger et al., 2021). These techniques open up a new paradigm in the way digital identity is managed, moving from a model where data is shared to one where only proof of its existence is shared.

To address the challenges of a technological and interconnected society, the eIDAS 2.0 Regulation², published on 30 April in the Official Journal of the European Union, creates for the first time an EU-wide Digital Identity Wallet (EUDIW) as a means of identification for both the public and private sectors, while also acting as a container for digital certifications called electronic attestations of attributes ((Q)EAA) (Schwalm et al., 2022), a new trust service introduced by eIDAS 2.0. Such trust service may be qualified or unqualified, the difference being in the legal value of each and the prior administrative authorisation required to provide qualified services. At the same time, the

² 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. OJ L, 2024/1183, 30.4.2024, ELI: <http://data.europa.eu/eli/reg/2024/1183/oj>

Regulation introduces in its Recital 14 the use of ZKP technologies tied to the EUDIW, but without developing a proper legal regime or making their use mandatory. In contrast, selective disclosure techniques, which allow one credential attribute to be shared while concealing the others, are mandated as a feature for the EUDIW by Article 5a(4a) of eIDAS 2.0.

Selective disclosure is defined in Recital 59 of eIDAS 2.0 as *a concept empowering the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only such information as is necessary for the provision of a service requested by a user*. For example, sharing only a user's age to access a particular electronic resource while hiding other credential fields, such as name, birthplace, or ID number.

Zero-knowledge proofs are explicitly mentioned in Recital 14 of eIDAS 2.0, which states that *Member States should integrate different privacy-preserving technologies, such as zero-knowledge proofs, into the European Digital Identity Wallet*. This recital also introduces a definition of these technologies and the desired properties for the EUDIW by which *those cryptographic methods should allow a relying party to validate whether a given statement based on the person's identification data and attestation of attributes is true, without revealing any data on which that statement is based, thereby preserving the privacy of the user*. Thus, ZKPs should make it possible to prove the user's possession, existence, or performance of a particular computation, such as verifying legal age, without revealing the specific data or underlying metadata associated with the credential and without compromising the verifiability of the credential.

However, the eIDAS 2.0 Regulation excludes the regulatory development of ZKPs in its articles, leaving it to the discretion of Member States to explore these techniques and develop them in their national laws. This means that using ZKP techniques is not mandatory, leading to the fragmentation of the Digital Single Market with the potential for divergent national solutions that are not interoperable and do not enjoy cross-border recognition (Ramos Fernández, 2024).

The mention of ZKPs in Recital 14 of eIDAS 2.0, coupled with the lack of regulatory development in the operative part of the Regulation, means that the choice of selective disclosure techniques for the EUDIW in Article 5a(4a) over ZKP is not justified. As stated by the European Union Agency for Cybersecurity (ENISA) (2022), ZKPs allow for a high level of compliance with the General Data Protection Regulation's³ (GDPR) principles of minimisation (Article 5.1.c), consent (Article 7), and privacy by design and by default (Article 25).

To implement selective disclosure in the EUDIW and translate the requirements set out in the Regulation into a technical format, the European Digital Identity Wallet Architecture and Reference Framework⁴ (EUDIW ARF) document aims to provide the necessary specifications to develop an interoperable solution based on common standards and practices. However, given ZKPs are not compulsory under the eIDAS 2.0, the EUDIW ARF provides no guidance on them.

³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *OJ L 119, 4.5.2016, p. 1–88*

⁴<https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework>. Accessed 21 may 2024.

Therefore, legal governance for ZKP in the eIDAS 2.0 Regulation is needed to ensure their use across the European Union, provide legal certainty, and avoid fragmentation of the Digital Single Market. However, the first step is understanding how ZKPs can be related to the EUDIW. To this end, we present three mutually compatible regulatory options for enabling the issuance of ZKP identity data in the context of the EUDIW: issuance of ZKPs by default as a necessary component of the EUDIW, through a software product extension that could be added to the EUDIW, or as a standalone software product in parallel to the EUDIW.

Our contribution paves the way for discussing the necessary framework for ZKPs in the context of eIDAS 2.0 and highlights existing studies and technical solutions that enable the implementation of ZKPs. This stimulates further work to expand the state of the art in this area and make ZKPs the benchmark for all data processing under Article 25 GDPR. Finally, we offer some insights into how legal governance for ZKPs could be envisaged as future work.

The rest of the paper is structured as follows: Section 2 presents previous work that has addressed the use of ZKP techniques applied to digital identity from a legal perspective. Section 3 discusses how ZKPs have been analysed in the design of identity management systems and conceptualises both eIDAS 2.0 and the EUDIW ARF. Section 4 presents regulatory options for integrating ZKPs into the EUDIW. Section 5 discusses the results obtained. Finally, section 6 presents the main conclusions and suggests directions for future work.

2. Related work

Previous studies on using cryptographic ZKP protocols applied to digital identity from a legal perspective can be found in the European research project ARIES (Saher et al., 2017). This project aimed to reduce the risk of digital identity fraud and related issues. To this end, a pilot was conducted at Leeds Bradford International Airport in West Yorkshire, England, to demonstrate the operation of a centralised system for using different derived identities with varying levels of privacy. This system relied on ZKPs for airport access control, boarding control, and VAT exemption in duty-free shops. As a result, it was possible to prove possession of a valid boarding card for that day without providing any additional information other than possessing the card.

Alamillo Domingo, I., Valero Torrijos, J., Fortune, D., & Martin (2017) analysed the legal implications of such a system within the ARIES project. They concluded that a legal framework within the eIDAS regulation is necessary to address issues such as algorithms, validated or certified software, sound operational practices, and liability to third parties for potential damages. Without this framework, data recipients cannot demonstrate compliance with their obligations to supervisory authorities, as it would be impossible to compare data received in ZKP format with the source data.

This same idea for the need for a legal regime for existence proofs was pursued by Alamillo Domingo (2020) in a report for the European Commission. This report analysed how eIDAS could legally support digital identity and trustworthy transactions using distributed ledger technologies (DLT) in the Digital Single Market. The author argued that ZKPs can legally substitute documents proving personal attributes. For instance, instead of showing a boarding pass with all personal details, a ZKP can confirm that a person has a valid boarding card without disclosing additional data. This approach

enhances privacy and reduces compliance costs for data controllers, provided ZKPs are accepted as substitute evidence in legal proceedings. To ensure this, the author proposed establishing a legal equivalence between the original credential and its derived data in a ZKP.

In the framework of the eIDAS 2.0 Regulation, the Technical Report ETSI TR 119 476 V1.1.1 (2023-08) discusses selective disclosure and ZKPs applied to the (Q)EAA. It provides a comprehensive understanding of signature schemes, credential formats, and protocols that support selective disclosure, unlinkability, and ZKPs. The report recommends how eIDAS 2.0-compliant qualified trust service providers should issue EUDIW personal identification data and (Q)EAA, that provide selective disclosure and dissociability.

Building on this work, Ramos Fernández (2023) proposed a regulatory framework to give legal validity to ZKPs, supported by three pillars: regulation of a software product that integrates with the EUDIW, establishing a functional equivalence between the legal effects of (Q)EAAs and EUDIW identification data transformed into ZKPs, and mandating the acceptance of ZKPs in specific scenarios. Subsequently, Ramos Fernández (2024) evaluated whether the issuance of a ZKP should be considered a product or a service, concluding that the product approach offers the highest privacy and security guarantees. However, the author did not address the regulatory scenarios for integrating ZKPs into the EUDIW.

3. Background

3.1. The use of zero-knowledge proofs in the design of identity management systems

Zero-knowledge proofs convey no additional knowledge other than the correctness of the proposition in question (Goldwasser et al., 1985). Applied to identity management systems, these privacy-preserving techniques enable use cases where proof of data existence is shared instead of the data itself. A prime example is the COVID certificate. During the pandemic, validating this certificate required a QR code with the user's health data and an ID card (Ramos Fernández, 2022). However, using a ZKP through the EUDIW, a user could prove their vaccination status without revealing any additional information, simply answering the question: 'Does the person I am dealing with have a valid COVID certificate? '.

Another example is disclosing a name and surname with proof of age, ensuring the name and surname match those on an ID card without the requester ever seeing the ID card. For instance: 'My name is Alice, I am above 18 years old, and I possess an ID card that corroborates this.' Although the requester may know the name and surname because they requested it, this remains a ZKP as the requester never sees the original credential or obtains the associated metadata needed to verify the information. Thus, zero-knowledge property is always relative to what the verifier needs. This cryptographic protocol minimises the information shared to validate a claim, fact, capability, or identity without revealing any underlying information beyond the claim's validity (Bamberger et al., 2021). ZKPs allow cryptographic verifiability checks of a credential to be performed by the user with full mathematical assurance, ensuring the proof is equivalent to the checks that would have been performed by the requester (Delignat-Lavaud et al., 2016).

From a legal standpoint, ZKPs enable the implementation of two measures outlined in Article 25 of the GDPR: data protection by design and by default and data accessibility limitation (Spanish Data Protection Agency -AEPD- 2020). This implies a transition to a model where, rather than sharing data, existence proof is shared, reducing the risk of identity provider data theft and authentication metadata-based provider profiling (Alamillo Domingo, 2020). However, as noted by the Spanish Data Protection Agency, the weaknesses of zero-knowledge proof systems stem from the gap between the algorithms and procedures and their actual implementation in a specific technical, organisational and legal context. Essentially, key challenges and limitations of ZKP systems for digital identity are related to high computational requirements, implementation complexity, domain expertise, scalability issues related to network latency, user experience challenges, interoperability and standardisation needs, regulatory uncertainty and lack of legal recognition, potential vulnerabilities in case of faulty implementation, high development and operational costs, and adoption barriers in regulated industries.

The application of ZKP techniques to digital identity arises from concerns about privacy loss in electronic environments, the rise of digital commerce, and the growth of new technologies like DLT, including Blockchain. These factors have led to the Self-Sovereign Identity (SSI) approach (Allen, 2016). This model asserts that users should control their personal information, share only the necessary data for each interaction, know what information has been shared and for what purposes, and have the right to withdraw consent at any time (European Union Agency for Cybersecurity -ENISA- 2020). In this context, the idea of a decentralized network based on cryptography emerged, ensuring a root of trust that cannot be compromised and is trusted by all agents (Reed and Preukschat 2021). This led the SSI community to see an opportunity to use

DLT networks and leverage ZKP protocols, successful in cryptocurrencies like Zcash (Ben-Sasson et al., 2014) for digital identity applications.

Several projects have implemented ZKP protocols in their digital identity solutions, supported by distributed ledgers to address scalability and trust issues in systems not publicly recognized and governed by private law or centralized solutions. Examples include identity management systems proposed by Lee et al. (2020), which make use of succinct, non-interactive zero-knowledge arguments of knowledge (zk-SNARK) protocols to ensure that identity data matches the cryptographic commitment issued for validation while convincing the recipient of the execution's correctness. Bandara et al. (2021) proposed a similar system where identity data is stored locally, sharing only the cryptographic material needed to validate the protocol. Sedlmeir et al. (2021) analysed the interaction between digital identities, verifiable credentials, and distributed ledger technology with ZKP. More recently, de Vasconcelos Barros, Schardong, and Felipe Custódio (2022) proposed a ZKP system for sharing COVID vaccination certificates from a digital wallet, proving that the device holder has a valid certificate and that only the holder can present it, solving the identity verification problem. Afterwards, Babel and Sedlmeir (2023) proposed a general-purpose ZKP scheme for flexible privacy, providing credential chaining and hardware binding to modulate the required privacy strength for each interaction.

Leveraging the synergy between DLT technologies and ZKP techniques, solutions for large-scale decentralised elections have been proposed to provide transparency, privacy, universal verifiability, and weak receipt-freeness. Emami et al. (2023) propose a system that ensures each vote is recorded immutably and can be independently verified without revealing the voter's identity, maintaining the confidentiality and integrity of the

electoral process. Whereas, El Kafhali (2024) highlights the potential of ZKP in combination with DLT systems to address the traditional problems of cost, identity management, and human error in the production of national elections. This combination allows for a robust framework that mitigates electoral fraud, preserves voter privacy, and significantly enhances trust in the electoral system.

As for European-funded research, the Horizon 2020 ARIES project developed a technological framework for centralised repositories using ZKPs to demonstrate possession of a valid boarding pass in a real pilot at Leeds Airport (Bernabe et al., 2020).

One of the most prominent commercial projects is the one developed by the Hyperledger Foundation (2018). It provides a modular infrastructure that integrates the verifiable credentials recommendation (W3C, 2022) and Blockchain technologies to decentralise trust in a Self-Sovereign Identity approach. Unlike its counterpart in the European Blockchain Services Infrastructure (EBSI 2022), the Hyperledger project allows for the issuance of ZKPs through AnonCreds (anonymous credentials), a type of verifiable credential that supports ZKP cryptography.

In the international landscape, the Government of British Columbia (BC Gov) uses Hyperledger Aries components to issue and verify privacy-preserving Hyperledger AnonCreds for various purposes, such as driver's licences, proof of age or educational qualifications, and provides the Aries-based BC Wallet to receive and present those credentials⁵.

⁵ <https://marketplace.digital.gov.bc.ca/opportunities/code-with-us/d81f1bb4-4abb-4a4c-8b19-92904e0bd6a6> Accessed 20 June 2024

3.2. The eIDAS 2.0

The eIDAS 2.0 Regulation is an update of the eIDAS 2014 Regulation⁶ on electronic identification and trust services for transactions in the internal market, launched by the European Commission under Article 49 of eIDAS with a strong market-opening nature. It aims to facilitate the interoperability and security of digital services in the European single market and promote the confidence of citizens and businesses in electronic environments. The eIDAS Regulation covers two main areas: cross-border identity management systems ensuring interoperability across the Union, and trust services. The latter are a closed list of public services that deal with a privatised vision of electronic evidence (Alamillo Domingo, 2019): electronic signatures, electronic seals, electronic time stamping, registered delivery services and website authentication. These trust services are legally binding, have evidentiary value, and are subject to strict supervision and regulation.

The core focus of eIDAS 2.0 is to shift from a model that recognises different electronic IDs to a harmonised model involving the private sector. To adapt to market dynamics and technological evolution, the amendment adds three new trust services: electronic archiving, electronic attestations of attributes, and electronic ledgers. Electronic ledgers, which combine time-stamped data and their sequence to ensure data creation certainty, are similar to electronic signatures. They are designed to provide a legal framework for DLTs, allowing projects like the EBSI to gain legal recognition. This trust service is outlined in Article 45k and supports the exchange of decentralised and self-sovereign identity solutions.

⁶ Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC *OJ L 257, 28.8.2014, p. 73–114.*

The amendment addresses shortcomings such as the burden on the private sector to access national public eID systems, the voluntary cross-border use of eIDs by Member States, and the provision by Member States of rigid eIDs far to be user-friendly for citizens and encourage their use (Llaneza González 2021). Accordingly, eIDAS 2.0 introduces a new mandatory eID for EU Member States, the EUDIW, which ensures interoperability across the EU through cross-border identity management systems. It also introduces a new trust service, the (Q)EAA.

On one side, (Q)EAA are defined in Article 3 (44) of the eIDAS 2.0 as *an attestation in electronic form that allows attributes to be authenticated*. These are cryptographically verifiable digital documents linked to an issuer's electronic certificate, attesting to an individual's attributes, such as powers of attorney, large family certificates, bank certifications, or university degrees analogous to the electronic certification and record-keeping acts carried out by public administrations and other entities. In practice, this means that a person with their European Health Insurance Card in the EUDIW can present it to any authority in the EU. This is a paradigm shift: instead of centralizing information in data spaces, it is decentralized under the user's control. Multiple issuers can issue documents related to the user's identity, which are stored in the EUDIW. This gives the user control over their data, including who has requested it and for what purpose, without the issuer knowing how the data is used. Additionally, (Q)EAAs can be stored in the EUDIW or a private wallet, allowing flexible management.

On the other side, the EUDIW aims to provide EU citizens with trusted digital identities, enabling them to control their interactions and online presence by offering an additional means of electronic identification beyond what Member States implement. The EUDIW also addresses two main risks associated with authentication delegation systems,

such as those in the eIDAS interoperability node for the public sector and centralized internet providers, including social networks. These risks are the potential theft of identity data managed by the provider and the monitoring of user behaviour through authentication transaction metadata, which can lead to profiling.

The EUDIW is defined in Article 3 (42) of eIDAS 2.0 as *an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals*. This definition introduces the public good trait of the EUDIW, which, according to Article 5a (2), shall be issued and managed in one of the following ways: directly by a Member State, under a mandate from a Member State, or independently from a Member State but recognised by that Member State. However, nothing in eIDAS 2.0 prevents private wallets from coexisting with the EUDIW. Private wallets, though, will not be considered an identification means, and additional steps would be necessary to authenticate the user, such as showing a physical ID or providing another means of identity proof. This is the example of the COVID certificate, even if the user is in possession of a (Q)EAA, the private wallet does not identify the user as the EUDIW does.

The main novelty of EUDIW compared to the eIDAS 2014 scheme is the obligation under Article 5f of eIDAS 2.0 for certain private sector entities to accept these wallets, in particular very large online platforms as referred to in the Digital Services Act⁷ and those private sector entities that are required by Union or national law to use strong

⁷ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). *OJ L 277*, 27.10.2022, p. 1–102.

user authentication for online identification or where strong user authentication for online identification is required by contractual obligation, including in the area of banking and financial services. Therefore, users will be able to use the EUDIW to create social network accounts or make payments.

In this regard, eIDAS 2.0 introduces several privacy-preserving mechanisms. On the one hand, the right to use pseudonyms, Articles 5 and 5a(4b), so the user can generate them in their EUDIW and keep pseudonyms encrypted. On the other hand, eIDAS 2.0 introduces the use of selective disclosure, included in the basic design of the EUDIW, which, by Article 5a(4a), must allow for *secure request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while ensuring that selective disclosure of data is possible*. This implies, for example, the possibility of using a different pseudonym for each social network in which one wishes to create an account in order to avoid traceability or of disclosing only the data necessary to open a bank account so that irrelevant data contained in the ID card, such as place of birth or parents' names, are not disclosed.

Other privacy-preserving techniques mentioned in the recitals of eIDAS 2.0 but not in its regulatory part are ZKP. Recital 14 states that *Member States should integrate different privacy-preserving technologies, such as zero-knowledge proof, into the European Digital Identity Wallet. Those cryptographic methods should allow a relying party to validate whether a given statement based on the person's identification data and attestation of attributes is true without revealing any data on which that statement is based, thereby preserving the privacy of the user*. The fact that these techniques are only

mentioned in this recital carries the same problems are foreseen as in eIDAS 2014: the voluntary nature of Member States to develop these techniques for their EUDIW, the lack of interoperability with other Member States' systems, the lack of cross-border effects, and the possible existence of 27 regimes leading to fragmentation of the Digital Single Market.

Nevertheless, the mandatory use of ZKP techniques could be understood if no other techniques could ensure compliance with GDPR rights under the same conditions, based on the interpretation of Article 5a (16b): *the technical framework of the European Digital Identity Wallet shall enable privacy-preserving techniques which ensure unlikability, where the attestation of attributes does not require the identification of the user*, and Article 5a (17): *any processing of personal data carried out by the Member States or on their behalf by bodies or parties responsible for the provision of EUDIW as electronic identification means shall be carried out in accordance with appropriate and effective data protection measures. Compliance of such processing with Regulation (EU) 2016/679 shall be demonstrated*. Consequently, ZKP techniques would serve as a benchmark for privacy impact assessments when considering other techniques, such as selective disclosure.

In short, unlike pseudonyms and selective disclosure, which are included as rights in the normative part of eIDAS 2.0, the mandatory use of ZKPs is determined by interpreting its articles in those cases where similar technologies do not meet the same privacy standards as ZKPs. In any case, it is up to the Member States to develop national schemes that allow using ZKPs within the scope of the EUDIW. For this same reason, ZKPs are out of the scope of the EUDIW ARF, which translates eIDAS 2.0 provisions into technical

specifications needed for developing an interoperable European digital identity wallet solution based on common standards and practices.

3.3. The European Digital Identity Framework and Architecture

The European Digital Identity Wallet (EUDIW) Architecture and Reference Framework (ARF) is a dynamic document developed in accordance with the guidelines outlined in Recommendation (EU) 2021/946 of 3 June 2021. This Recommendation urges Member States to collaborate in creating a common Union toolbox, which includes the EUDIW ARF, a compilation of common standards, technical specifications, and a set of guidelines and best practices. The Recommendation establishes that the ARF will be a fundamental reference for implementing the European Digital Identity Framework. Consequently, the ARF itself is not legally binding; only the implementing and delegated acts that adopt it will have legal force.

The primary purpose of the ARF is to define high-level requirements that provide a common framework for the implementation of eIDAS 2.0. It also aims to define the technical specifications, standards, protocols and procedures related to the core functionalities of the EUDIW and its relying parties. These requirements include qualified electronic attestation of attributes, verification against authentic sources, issuance of (Q)EAA by or on behalf of public sector entities, cross-border identity matching, certification of the EUDIW, publication of a list of certified EUDIW and security breaches of the EUDIW.

The scope of the ARF covers the definition of technical and functional specifications for several use cases, which may be extended in the future. These use cases currently include identification and authentication for access to online services, qualified electronic signatures, mobile driving licenses, pseudonyms, healthcare (both national and

cross-border), educational certificates, professional qualifications, digital finance and digital travel documents.

Although the ARF is an evolving document, currently at version 1.4.0⁸, it does not cover how ZKPs could be used in the EUDIW framework; however, this does not mean that in the future ZKP protocols could be evaluated for functional measures, such as detaching the EUDIW's authentication process from the issuing or requesting of credentials to avoid user binding and thus prevent the EUDIW from becoming a pervasive identifier. For internal use of the EUDIW, zero-knowledge proofs would be part of the certification process foreseen in Article 5c of eIDAS 2.0.

As a high-level framework, the EUDIW ARF is designed to allow Member States to define their national specifications as long as the EUDIW's interoperability is maintained. Consequently, Member States could implement zero-knowledge use cases such as the above in the scope of the EUDIW certification to prevent the correlation of a user's activities with their EUDIW. This would allow users to prove ownership or control of the EUDIW without revealing identifying information that could link transactions and create traceable patterns.

As a result, ZKP techniques could be used outside of the EUDIW ARF to verify that a user possesses a credential or meets a condition without linking this proof to a specific EUDIW across different interactions. This approach would prevent the wallet from acting as a persistent identifier, thereby reducing the risk of traceability and correlation across different wallet uses. Nonetheless, the challenge is to design ZKP

⁸ <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md>

protocols that are both secure and efficient and to ensure their seamless integration into authentication and credential issuance processes without compromising usability or privacy.

4. The integration of zero-knowledge proofs into the European Digital Identity Wallet

The provision for additional EUDIW functionalities in recital 21 of eIDAS 2.0, along with the evolving nature, scope and purposes of the EUDIW ARF, enables the development of a ZKP generation module through three mutually compatible scenarios.

The first scenario, introduced by eIDAS 2.0, allows Member States to voluntarily develop or outsource the cryptographic module for ZKPs under their own responsibility, placing the primary responsibility and investment burden on the State. We will also analyse the implications if the development of ZKPs under this vision becomes mandatory in a future reform of eIDAS 2.0.

The second scenario, which requires the most significant modification of eIDAS 2.0 compared to the other options, involves a ZKP generation module that can be plugged into the EUDIW under the sole liability of the manufacturer. This shifts the responsibility and investment burden to the developers.

The third scenario considers the ZKP generation module as an independent private wallet, shifting the responsibility and financial burden to the developers while sacrificing the identification function of the EUDIW. This option is applicable when Member States do not develop ZKP for the EUDIW and there is no obligation to do so. Although this

scenario does not require any legal changes, it lacks legal backing. Figure 1 provides an overview:

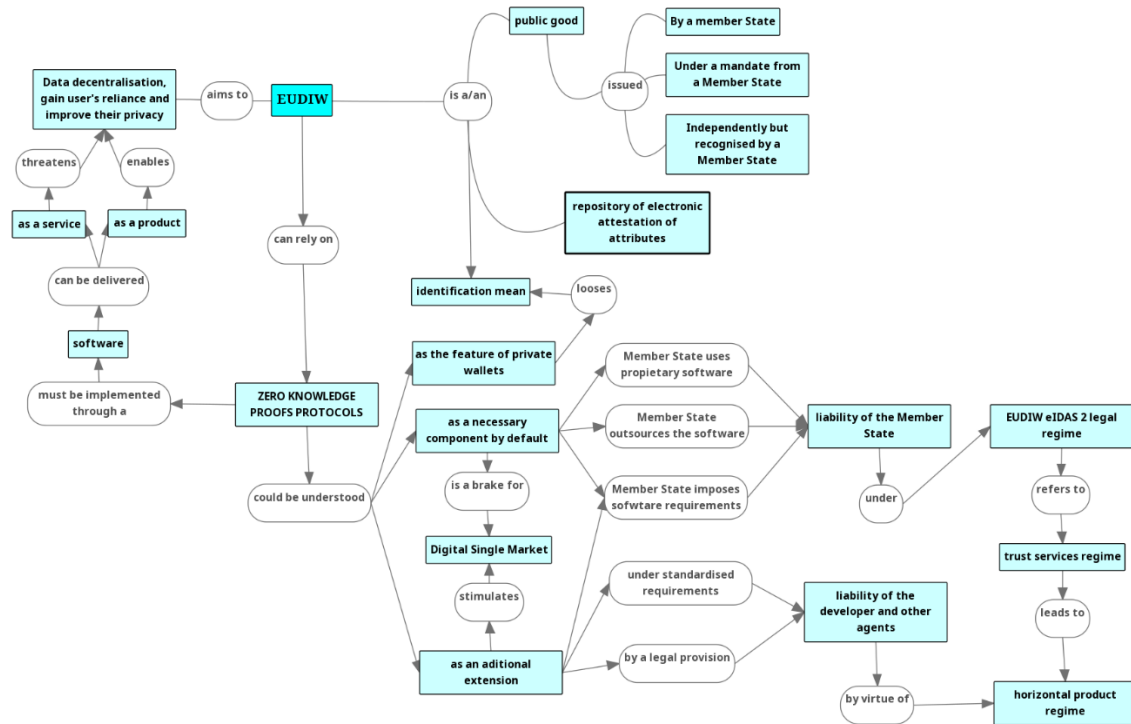


Figure 1. Overview of possibilities for integrating ZKPs into the EUDIW. Own elaboration.

Before analysing the scenarios described above, it is necessary to examine the models for providing ZKP, whether as a service or as a product, to introduce the common framework for the options we assess.

4.1. Approach of the ZKP module as a product or as a service software

Zero-knowledge proofs are cryptographic protocols that must be implemented in a computer program⁹ due to the complex algorithms and mathematical operations involved in ensuring secure communication and privacy. Implementing these protocols translates the algorithms into code that the computer's processor can execute efficiently, optimising

⁹ 'Computer program: a combination of computer instructions and data definitions that enable computer hardware to perform computational or control functions' § 3.726 ISO/IEC/IEEE 24765:2017. Systems and software engineering — Vocabulary.

performance and ensuring compatibility with various computing platforms and devices. This process enables practical and reliable secure communications and data protection. The software's function is to *communicate and work with other components of the system and with its users through a logical system of interconnection and interaction via an interface*¹⁰, whether available as a product or as a service.

The key difference between the two models is how the user accesses the software. In the software-as-a-product model, the program is hosted directly in the user's environment, under their control and liability. The user manages all processed data, and the provider offers periodic updates for the user to install. In contrast, the software-as-a-service model involves cloud computing¹¹, where the program is hosted on the provider's servers. The provider handles data processing, cloud storage, software maintenance, and updates (Wang & LeBlanc, 2016).

The privacy and cybersecurity implications of both models are closely related to the liability assumed by the ZKP software developer or provider. The service model centralises user data at a single point before ZKP derivation, increasing the risk of data breaches and profiling by the provider using associated metadata, risks that eIDAS 2.0 aims to address with decentralised identity management systems. On the other hand, the software-as-a-product approach allows users to control their data, reducing the regulatory and investment burden on service providers to ensure data security.

¹⁰ Recital 10 of the Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. *OJ L 111*, 5.5.2009, p. 16–22.

¹¹ Software as a Service (SaaS): Cloud service category (3.2.10) in which the cloud capabilities type (3.2.4) provided to the cloud service customer (3.2.11) is an application capabilities type (3.2.1)' § 3.2.36 ISO/IEC 17788 Information technology — Cloud computing — Overview and vocabulary.

From a regulatory perspective, the product legal regime applies to processing software whether stored on a device under the user's control¹² or delivered as a product or service¹³, particularly concerning liability for potential damage caused by improper design, compilation, or cybersecurity flaws. Consequently, the service regime is more complex because it includes rules for both services and products, while the product regime involves only product-specific regulations. Managing software under the service model requires compliance with a broader set of regulations, addressing both service and product-specific liabilities and standards, as mandated by eIDAS Article 24.2(e), which requires qualified trust service providers *to use trustworthy systems and products that are protected against modification and ensure technical security and reliability*.

The regime of EUDIW is even more complex, as it is considered a product under Art. 3 (21) of eIDAS 2.0. It also has a provider—the State—and operates under a special regime with specific provisions for trust services. Therefore, if the issuance of ZKP is integrated into the EUDIW architecture, it will also fall under the product regime, as referenced in Article 5a(20) of eIDAS 2.0 and Article 24(2)(e) of eIDAS.

Consequently, ZKP generation software will always be liable under the product legal regime, which is enforced by a consolidated horizontal and modular framework of responsibility, warranty, control, monitoring, surveillance, and industrial safety rules.

¹² Recital 12 of the Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products. Brussels, 28.9.2022. COM(2022) 495 final. 2022/0302(COD).

¹³ Recital 19 of the Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance.). *OJ L 136, 22.5.2019, p. 1–27*.

In terms of product regulation, we currently have Regulation (EU) 2023/998 on general product safety¹⁴, Directive 85/374/EEC concerning liability for defective products¹⁵ and Directive (EU) 2019/770 on certain aspects of contracts for the supply of digital content and services¹⁶. Furthermore, the Product Liability Directive¹⁷ is in the proposal phase and, upon adoption, will be fully applicable to software products.

Regarding cybersecurity requirements, the Cybersecurity Act¹⁸ and the NIS 2 Directive¹⁹, which entrust market surveillance authority functions to the cybersecurity bodies of the Member States, are fully applicable. At the proposal stage are the ENISA candidate scheme based on Common Criteria²⁰ and the Cyber Resilience Act²¹, which mandates the creation of technical standards for establishing requirements for a platform for a data exchange space for software and hardware products to be commercialised in Europe. Consequently, certain products may be banned or undergo a period of experimentation if they do not comply with this Regulation.

¹⁴ Regulation (EU) 2023/988 of the European Parliament and of the Council of 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC. *OJ L 135*, 23.5.2023, p. 1–51.

¹⁵ Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products *OJ L 210*, 7.8.1985, p. 29–33.

¹⁶ Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. *OJ L 136*, 22.5.2019, p. 1–27.

¹⁷ Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products. Brussels, 28.9.2022.COM (2022) 495 final. 2022/0302(COD).

¹⁸ Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *OJ L 151*, 7.6.2019, p. 15–69.

¹⁹ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). *OJ L 333*, 27.12.2022, p. 80–152.

²⁰ Cybersecurity Certification: Candidate EUCC Scheme — ENISA (europa.eu). Accessed 21 May 2024.

²¹ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. Brussels, 15.9.2022. COM(2022) 454 final. 2022/0272(COD).

For technical standardisation, ISO/IEC 25000²² can be relied on for quality assessment, Regulation (EU) 1025/2012²³ can be used to harmonise specific ZKP protocols, and the GDPR is applicable to guarantee user rights and fair data processing.

Finally, Regulation (EC) 765/2008²⁴ gives the Conformity Assessment Bodies of each Member State the responsibility for market surveillance of products put into circulation and certifying their conformity with existing requirements, rules, and standards in force. This ensures a complete system of trust in the ZKP generation, derivation, and creation of software products used with the EUDIW or on a standalone basis.

Hence, when considering ZKP issuance software as a product, there is currently a consolidated set of liability rules for its individualisation on a case-by-case basis according to the dispersed rules discussed above. On the other hand, considering a trust service scenario, in the sense of the digital signature or the (Q)EAA, would require its development within the eIDAS service catalogue. Thus, liability, supervision, applicable security requirements including the use of secure products (Article 24 eIDAS) and the possible qualification of trust service providers would be governed by Chapter III of eIDAS on trust services.

In summary, the main difference in choosing between the product or service regime for software development is the perspective of privacy and control of data: whether the user in the product model or the user's dependence on a third party to manage

²² ISO/IEC 25000:2014 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE.

²³ Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation. OJ L 316, 14.11.2012, p. 12–33.

²⁴ Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93 (OJ L 218 13.8.2008, p. 30).

his data. Therefore, according to the logic of eIDAS 2.0, the product model should be chosen to guarantee the user's independence when sharing their data.

4.2. Creation software as a component by default

One possibility outlined is that the ZKP processing software is conceived as a component of the EUDIW architecture and is, therefore, included by default for issuing the personally identifiable data of the EUDIW or the (Q)EAA stored therein in ZKP format. This scenario is the starting point for eIDAS 2.0.

According to Recital 14, *Member States should integrate different privacy-preserving technologies, such as ZKP, into the EUDIW*. On the other hand, Recital 21 allows for additional functionalities that do not undermine the provision of the core functionalities of the EUDIW but with the restriction that they do not benefit from cross-border effects. Therefore, the current eIDAS 2.0 framework encourages the development of additional functionalities for the EUDIW, but with three major drawbacks: the voluntariness of the Member States, the lack of cross-border effects and the exclusion of the private sector in free competition.

Firstly, the voluntariness of the Member States is one of the reasons for the introduction of the EUDIW in eIDAS 2.0, as there are States that have decided not to extend their national solutions for cross-border use, thus depriving their citizens of the possibility to use their national identification means to access public services in other Member States. This same situation may arise with the implementation of optional additional functionalities for the EUDIW, with States limiting themselves to only what is mandated by eIDAS 2.0 and its implementing acts.

Secondly, additional EUDIW functionalities would be governed according to the general rules of EUDIW (Article 5a), their certification rules (Article 5c), and the security breach rules (Article 5e). However, when using EUDIW for cross-border purposes, non-mandatory additional functionalities will not be automatically acknowledged. Voluntary mutual recognition between States will be necessary for cross-border effects and interoperability. Moreover, if each State develops its own functionalities rather than adopting a harmonised framework, there could be 27 national systems with different data structures and semantics for ZKPs.

Thirdly, the interoperability issue leads to the exclusion of the private sector in open tendering. In the vision of additional functionality as an internal component of the EUDIW, the State controls the technology to be used, so there are two options: either the State develops the additional functionality, or it outsources it to the private sector. Outsourcing requires the State to determine which vendor(s) can participate in the development and what type of technology must be used. This idea contradicts the principle of market fostering, as it constrains innovation and private capital investment by restricting the development of solutions at the national level and making it more difficult for suppliers established in another Member State to access them, as different national rules may apply.

Nevertheless, even though ZKP functionality is optional in the current eIDAS 2.0, according to the assessment under Article 49 of eIDAS 2.0 to be conducted in 2026 the mandatory implementation of ZKP in the EUDIW could be envisaged, which would imply both cross-border effects and interoperability of these techniques if entrusted the their standardisation to the European bodies ETSI, CEN and CENELEC. Notwithstanding, this does not change the legal status of ZKP as a feature design of the EUDIW nor that it is the State that has the mandate to issue them and, therefore, the

accountability for their performance. It is an integral part of the EUDIW, so the applicable regime is the same as any other EUDIW functionality.

The EUDIW legal framework comprises three dimensions: the EUDIW regime set out in Section 1 of eIDAS 2.0, the reference in Article 5a(20) to the trust services aspects envisaged in Article 24(2)(b) and (d) to (h), and the remission to the product regime discussed in Section 4.1 of this paper through Article 24(2) letter (e).

According to Article 5a (2), the EUDIW must be provided by the Member State. Therefore, even if the State outsources the software or sets specific requirements for access to the EUDIW for software extensions, such as protocol type or enabling technologies, the State remains accountable for its technological choice. Consequently, whether Member States develop their software, outsource it, or support it as an external module to the EUDIW, they remain responsible for their technological choice. In that regard, the State becomes a provider of the EUDIW; even though the EUDIW is a product, the legal regime is a service one, but under the particular regime developed for the wallet.

As far as the rules laid down in Article 5a (20) of eIDAS 2.0 are concerned, this provision imposes on the EUDIW provider similar obligations to those imposed on trust service providers, such as having specially trained personnel, using trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes they support. This, in turn, leads to the application of the product rules discussed above. In this way, legal control can be exercised over the entire technology lifecycle, and concurrent liability can be established at each stage, from development to implementation. Still, the state will always be accountable as the issuer of the EUDIW.

In summary, the regime of the EUDIW architecture is the most conservative among the ones we discuss as it implies a strong vision of technology control by the Member States. In return, even if it is possible to trace responsibility over the technology's life cycle, the State will be held accountable for using its chosen technology. In addition, the State would largely bear development and investment costs without prejudice to outsourcing the software development through public tendering, thus shifting part of the costs to the private sector. Therefore, the option of a future reform considering the mandatory introduction of ZKP as a core component of the EUDIW is unlikely due to the risk that Member States would take. Developing and implementing ZKP systems is technically challenging and prone to potential vulnerabilities due to the complexity of the underlying cryptographic algorithms. It requires specialised knowledge of cryptography and a deep understanding of the underlying protocols, which may limit widespread adoption. In addition, user experience challenges require user-friendly interfaces that are costly to develop and operate. From the point of view of Member States, a system overseen by them, which shifts both the responsibility and the investment costs to the private sector, would be more beneficial.

Thus, the current wording of eIDAS 2.0 provides the legal regime for the direct implementation of ZKP processing software as a component of the EUDIW architecture. For this purpose, Member States wishing to integrate ZKP into their EUDIW must develop internal rules on technological, governance issues, and legal effects of ZKP as the eIDAS 2.0 does not define any for them. Moreover, additional functionalities will not have cross-border effects if there is no agreement between States, and there is also a risk that different national rules and standards will prevent interoperability of ZKP validation systems. A harmonised framework within eIDAS 2.0, making it mandatory for Member States to integrate ZKP into their EUDIW and defining the legal value of ZKP could solve

those problems. Still, this option is unlikely when evaluating other options to avoid State liability, such as external additional functions that are not part of the EUDIW architecture but, once a set of requirements are met, can be integrated with it. This makes it easier for additional functionalities to exist for EUDIW so that the burden of responsibility and investment is shifted to the private sector.

4.3. Creation software as an additional extension

A second way of integrating ZKP protocols into the EUDIW is through an external software module. This approach is particularly attractive from a Member State perspective as it shifts investment costs and liability to the private sector while stimulating the Digital Single Market by allowing the commercialisation of additional EUDIW elements on a competitive basis. In addition, the Member State may be unwilling to take the risk of developing its software, may lack the technical capacity or may wish to reduce production costs.

The additional component approach offers the closest market opening, allowing for public-private partnerships. In this regard, industry self-regulation with product pre-certification according to the body of rules outlined in Section 4.1 provides the necessary guarantees that the single market will not fragment and that the legal certainty of the Union and the Member States will not be jeopardised. Governance controls and the pan-European definition of the technical rules to be followed fully justify public intervention while shifting the liability for the product regime to the private sector.

When considering liability arising from the placement of a ZKP software product on the market, the concepts of producer and finished product come into play, as defined in Article 3 of Directive 85/374/EEC, as well as the concept of putting into circulation, as defined in Articles 6 and 7 of the same Directive. The finished product is one which is

placed on the market without the need for subsequent modification and without prejudice to subsequent updating. In contrast, the placing on the market is when the manufacturer no longer has to intervene. From this point onwards, the manufacturer's liability is limited. Thus, reconditioned products will exonerate the manufacturer when the intervention has been carried out by a third party (Izquierdo Grau 2023).

On the other hand, the Proposal for a Directive on liability for damage caused by defective products²⁵ devotes Article 7.1 to determining the liable parties. From its literal wording, we can extract the premises on which the provision is based. Firstly, the Proposal concentrates liability for damage on the producer, in the same way as Directive 85/374/EEC. Additionally, the Article stresses that the producer is liable when a defective component causes damage. This is a provision with no clear precedent in Directive 85/374/EEC and is certainly consistent with the consideration of the vendor of the software system as a producer²⁶.

Consequently, in cases where the good has been made available on the market as a finished product, and it is the victim or a third party outside the organisation of the original product and outside its control who has installed software in the product, the exoneration of the liability of the original producer of the goodwill operate, as suggested in Article 10.2 of the Proposal for a Directive on liability for defective products (Izquierdo Grau, 2023).

²⁵ Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products COM/2022/495 final.

²⁶ Recital 12 of the Proposal for a Directive on liability for damage caused by defective products COM/2022/495 final.

What is at stake is the accountability for an add-on software module to the EUDIW as a finished product. In this case, the ZKP module is outside the organisation of the Member State issuing the EUDIW and is independent of its initial components. Even though the Member State would allow access to EUDIW for products that were not originally part of it, the fact that the ZKP cryptographic module would have to be certified or comply with a technical standards catalogue does not change the fact that the Member State no longer remains accountable.

Yet, the fact that the Member States are no longer responsible for the additional component does not mean that they lose control over it from a technical point of view. Whereas in the vision of the essential component the liability of the States was determined by the choice of the specific protocols and data structures to be implemented, in the case of the additional component these controls can be exercised indirectly, guaranteeing the exoneration of the State while ensuring that public security is not compromised. Within this approach, ZKP protocols could be harmonised across the Union, with cryptographic requirements for access to EUDIW defined by CEN, CENELEC, and ETSI. Their security could be certified by national accreditation bodies and lists of trusted products that can be used with the EUDIW could be published by ENISA.

In summary, the main advantage of this approach is that it strengthens the Digital Single Market while ensuring that Member States transfer product liability and costs to the private sector, while the main drawback is the legal changes needed to comply, including the governance framework or the scenarios in which a ZKP can be accepted or in which they should be mandatory. This framework should provide legal certainty for all stakeholders: for Member States to know that public security will not be compromised, for service providers to know when they are obliged to accept a ZKP, for users to know what kind of data they may be asked to provide, and for developers to comply with legal

requirements when developing their products and selling them across the EU. Despite these hurdles, the external software module approach offers the opportunity to create a common framework to ensure interoperability and cross-border acceptance, irrespective of the software manufacturer. With this approach, users could use the EUDIW means of identification, while seamlessly certifying (Q)EAA stored in a ZKP format.

The main drawbacks of the external software module approach relate to the shift of development, operational costs and liability to the private sector. This includes dealing with the complexity and computational overhead of ZKP modules, their scalability and network latency issues, user experience challenges and security risks. In return, participation in a regulated market will be opened to the private sector, giving legal value to ZKPs where interoperability and technical standardisation rules exist to release their products.

4.4. Creation software as a private standalone wallet

The two previous scenarios relied on either the voluntariness of Member States or an exercise of maximum harmonisation by imposing an obligation to accept the addition of ZKP software extensions to the EUDIW, both for the personally identifiable information of the EUDIW and for (Q)EAA that may be stored in the EUDIW.

A third scenario is where Member States decide not to support the use of ZKP protocols and they are not mandated to allow access to the EUDIW for additional extensions. In such cases, there is nothing to prevent private providers from commercialising their wallets. Even if the EUDIW enables the use of ZKP modules, private wallets could coexist if users decide to use unregulated wallets. The main difference between unregulated wallets and the EUDIW lies in the conception of the EUDIW as a means of identification. According to Article 45c of the eIDAS, the (Q)EAA

does not replace electronic identification unless specifically allowed by the Member State or public sector body. In this scenario, the possibility of issuing ZKPs refers only to the (Q)EAA due to the impossibility of using stand-alone wallets as a means of identification.

From a legal point of view, the standalone wallet scenario follows the same rules as ZKPs as an additional component of the EUDIW in terms of the product, but the technological aspect is not covered. In this regard, this approach represents the highest risk for the private sector. This is the case of the problems in the H2020 ARIES project described in Section 2 regarding the demonstration of compliance with legal requirements.

Even if technical self-regulatory guidelines for ZKP protocols were widely accepted by the industry, a relying party would still face challenges if a national authority required proof of compliance with legal requirements and the party was unable to comply. In such a case, the relying party might have to resort to legal proceedings if the validity of the ZKP was disputed by the national authority. The potential economic damage is significant, highlighting the need for a real commitment to developing ZKP systems. Without the proper incentives, the private sector might not be compelled to develop technologies that lack legal backing.

On the other hand, in private-to-private relations, the ZKP approach as a standalone wallet would not present any complications, as it would be based on the agreements and contracts entered into. This approach would be desirable for proving that an individual has powers of attorney to act on behalf of a company, for non-disclosure agreements, trade secrets, user access within a company, and many other use cases that do not involve the public sector or affect how the compliance of these entities is

evidenced. However, this approach is the most limited in terms of market opening and the development of technological innovation in the EU.

In summary, the standalone wallet approach encounters several significant challenges. The lack of standardization and interoperability can hinder smooth integration with existing systems. Additionally, regulatory uncertainties and potential security risks, especially related to the accurate implementation of cryptographic algorithms, raise further concerns. Moreover, high development and operational costs add to these difficulties, making widespread adoption of such wallets challenging in the current environment.

5. Discussion

Of the three options analysed, the most attractive scenario for Member States, the private sector, and individuals regarding ZKP data issuance from the EUDIW is an external software product extension. This approach offers several benefits: it shifts responsibility for IT product development from Member States to private sector entities, improves the competitiveness of the EU's Digital Single Market, and enhances user privacy by removing intermediaries, unlike a service approach. Additionally, it encourages innovation in new cryptographic methods by commercialising products in a free and competitive digital market. **Figure 2** provides an overview of the legal regimes analysed:

Legal regimes overview		
1.Component by default		
	Optional component of the EUDIW architecture (current situation)	Mandatory component of the EUDIW architecture (unlikely scenario)
Liability	Member State (liability as provider of a service) Developers (product liability)	Member State (liability as provider of a service) Developers (product liability)
Ease of implementation	HIGH. Direct implementation but need national rules with current eIDAS 2.0	MEDIUM. Need to modify eIDAS 2.0 for harmonisation at EU level
Cost	Assumed/shared with private sector by Member State	Assumed/shared with the private sector by Member State
User experience	Allow for ZKP identification and credential sharing	Allow for ZKP identification and credential sharing
Interoperability	Risk of non-interoperability	Could be entrusted to the European Standardisation Bodies
Cross-border effects	Need for agreement with other Member States	Recognised across EU
Legal effects of ZKP	The ones each Member State rule	The one eIDAS 2.0 would define
Market opening	LOW	MEDIUM
Legal regimes overview		
	2.Additional extension (desirable scenario)	3.Feature of a private wallet (current situation)
Liability	Developers (product liability) LOW. Need a framework in eIDAS 2.0	Developers (product liability) HIGH. No need of legal changes
Ease of implementation	for the product approach	
Cost	Assumed by developers	Assumed by developers
User experience	Allow for ZKP identification and credential sharing	Allow only for ZKP credential sharing Needs private self-regulation for ZKP standards
Interoperability	Interoperable with other EUDIW	
Cross-border effects	Recognised across EU	Lack cross-border effects
Legal effects of ZKP	The one eIDAS 2.0 would define	None
Market opening	HIGH	LOW

Figure 2. Overview of possibilities for integrating ZKPs into the EUDIW. Own elaboration.

Entrusting the development of ZKP software to the market does not compromise the security of the EUDIW or obscure liability if vulnerabilities are discovered. There are two specific regimes for assessing liability in the event of risk: the EUDIW regime if the fault originates in the EUDIW and the product regime if the vulnerability is found in the ZKP module.

Since a ZKP is a mathematical object unintelligible to humans, confidence in its security relies on prior technology control. Public intervention and stringent controls are fully justified due to the risk to legal certainty and public security posed by relying on cryptographic protocols that cannot be checked and validated against the original data. This ensures that the right to effective judicial protection is not jeopardised. Therefore, legal mechanisms must be in place to ensure the secure use of products implementing

ZKP protocols and to provide developers and relying parties with legal certainty when designing or accepting such protocols.

The mechanisms that could be implemented include software product certification schemes for quality products, as defined by the ISO 25000 family, and European cybersecurity certification schemes. These schemes guarantee, as stated in Recital 75 of the Cybersecurity Act, that ICT products comply with minimum requirements regarding the availability, authenticity, integrity, and confidentiality of the data stored, transmitted, or processed. According to Article 56 of the Cybersecurity Act, ZKP processing software intended to be connected to the EUDIW could be required to be certified against the ENISA candidate scheme based on common criteria, thus giving the product a presumption of conformity. The implementation and supervision of this scheme could be carried out by national cybersecurity certification authorities, ensuring that certificates issued under this scheme are fully valid and recognised throughout the Union, as outlined in Recital 73 of the Cybersecurity Act.

In line with the NIS 2 Directive, which aims to provide ENISA with more competencies, the Agency could be tasked with creating lists of software whose cybersecurity has been certified by the competent authorities of the Member States. This approach is similar to the mandate in Article 12.3 of the Cybersecurity Act, where ENISA is responsible for creating a European database of vulnerabilities. This would result in a presumption of conformity, as Member States' conformity assessment bodies would certify that the product is safe and complies with all security and cybersecurity standards set by the General Product Regulation, the future Cyber Resilience Act, the EUCC candidate scheme, and the GDPR. This would justify the intervention of Member States

in their market surveillance functions under Regulation (EC) 765/2008 to ensure that ZKP generation software products used in the EUDIW are secure.

Moreover, given the rapidly evolving nature of technology and cryptographic techniques, European standardisation bodies should develop the applicable technical rules and cryptographic suites for ZKP software intended to be linked to the EUDIW, in accordance with Regulation (EU) 1025/2012.

Consequently, there is already a consolidated body of law that, through stringent prior controls, offers an adaptable framework to guarantee the security of the technology as a precondition for granting it legal presumptions and obtaining subsequent legal value. This presents an opportunity for future work based on the benefits that ZKPs offer in defining the European digital identity.

In this regard, a substantive equivalence rule, similar to Article 45b(2) of eIDAS 2.0—which equates lawfully issued declarations in paper format with the qualified EAA—could extend such effects to mathematical derivation in the form of ZKPs, ensuring their use is sound and secure. Such an equivalence rule should provide legal certainty to parties relying on ZKPs, as the risk lies with the final recipient, who must demonstrate compliance with their obligations. For example, a recipient of a VAT discount must prove they fulfilled specific requirements. Without such guarantees, final recipients, typically information society and e-commerce services, may refuse to accept these credentials.

Additionally, it would be necessary to foresee cases where cryptographic derivations may be mandatory for final recipients. This would ensure their legal certainty

when receiving ZKP attestations and inform users when they can demand that such attestations be accepted.

The stringent system design we draft as future work is necessary due to the inherent risks of using ZKPs. These risks arise from the probabilistic and non-absolute nature of ZKPs, meaning there will always be a gap between the theoretical concept and practical application. In a ZKP scenario, risks to rights and freedoms stem from discrepancies between algorithmic and procedural approaches and their actual application in specific technical, organisational, and legal contexts.

However, modifying eIDAS 2.0 may not be necessary if Member States choose to integrate ZKPs into their respective EUDIW systems. Such functionality would fall under the EUDIW regulation and be the responsibility of Member States. This is the least likely scenario, though, as issues such as interoperability and cross-border acceptance would still need to be addressed as a major drawback.

Another argument against changing eIDAS 2.0 is the interaction between ZKPs and the GDPR, which we also highlight as future work. ZKPs offer a level of privacy previously unattainable and help comply with the principles of data minimisation and privacy by design and by default, as outlined in Article 25 of the GDPR. Additionally, Articles 5a (16) and (17) of eIDAS 2.0 impose high privacy standards consistent with the GDPR and declare the GDPR fully applicable.

In summary, while integrating ZKPs into the EUDIW framework without modifying eIDAS 2.0 is possible, addressing interoperability and cross-border acceptance remains a challenge. The future work should focus on leveraging ZKPs to enhance

privacy compliance and exploring their full potential within the existing regulatory framework.

Thus, the consideration of ZKPs as a benchmark for implementation in the EUDIW could be inferred if, during an impact assessment, it is determined that no other techniques meet the privacy and unlinkability standards outlined in Article 5a of eIDAS 2.0 and the requirements in Article 25 of the GDPR. Practically, this interpretation would mean that any privacy impact assessment must consider and justify the choice of technology over ZKP. This interpretation would make ZKPs legally binding in cases where no other techniques offer similar data protection. However, the legal effects of ZKPs still need to be clearly defined.

For this reason, we conclude that the ZKP regulatory option, as an extension of the EUDIW, allows for the legal development necessary to provide maximum legal certainty. This ensures that Member States know public security will not be compromised, market providers know their investments are secure, relying parties know they will not face significant risks by accepting ZKPs, and users understand what data may be required of them.

Ultimately, the legal development of ZKPs under eIDAS 2.0 should address how these technologies intersect with the trust service of electronic ledgers in a broader context, beyond just supporting identity management systems. There is a tension between GDPR and blockchain, where data can only be aggregated, raising issues of data limitation and the right to be forgotten. Therefore, exploring ZKPs in the context of the EU identity metasystem should aim to achieve an unprecedented level of data protection in the EU and stimulate debate in other use cases. This includes addressing the interplay

between ZKPs, GDPR, and the electronic ledgers' trust service to tackle the challenges posed by blockchain networks and how EU public administrations can benefit from them.

6. Conclusions

The eIDAS 2.0 Regulation allows for the use of ZKP protocols to support the European digital identity metasystem. However, the legal framework for these tools is not yet defined. Therefore, we analysed how ZKPs could be integrated into EUDIW through three mutually compatible regulatory options.

Our study finds that there is a consolidated and evolving regulatory framework that ensures security and trust in issuing ZKPs for personally identifiable information within the EUDIW and the EAA. This framework applies to both the EUDIW and unregulated wallets through a software product regime.

Of the three regulatory options analysed, the additional software product, with strict ex-ante controls and competitive participation of private sector providers, is the most balanced. It supports the cohesion of the Digital Single Market and reassures Member States that the financial and liability risks will be borne by the private sector. This provides an incentive for Member States to accept regulatory developments and encourages private-sector investment. However, a clear legal and governance framework is needed to provide certainty to all stakeholders.

ZKPs offer unique advantages that other privacy-enhancing mechanisms do not, such as the ability to prove the existence of data without revealing the original source. This is in line with the design and default principles of Article 25 of the GDPR, as well as the minimisation and consent principles of Articles 5.1 (c) and 7 of the GDPR. However, the implementation of ZKPs in current environments is limited due to the lack

of research on their use in identity management systems. However, interest in ZKPs is growing, which should lead to their adoption as a reference standard for privacy impact assessments, providing a benchmark to justify the use of other techniques that do not offer the same level of privacy.

Our study suggests that once we have the enabling technologies to allow new use cases, the next step is to extract value from these innovations. Legal value could be attached to zero-knowledge cryptographic derivation through a set of presumptions. Under the current eIDAS framework, a service provider implementing a ZKP solution faces significant risks in the choice of protocols and underlying technologies, such as electronic ledgers. Similarly, accepting a ZKP carries the risk of not being able to demonstrate compliance with regulatory obligations. As a result, unregulated technologies lack adequate oversight and security, making it difficult to implement many initiatives with regulatory safeguards. Therefore, future work should consider the feasibility of establishing a substantive legal effect between the EUDIW data and the EAA with its derivation in ZKP format, the cases where acceptance of a ZKP could be mandatory, and the governance and legal controls for ZKP products.

In summary, the product regime we have analysed provides the proper legal basis to give legal value to using cryptographic ZKP protocols and stimulates the debate on the value that ZKPs bring to distributed ledger technologies as a supporting tool for digital identity.

Acknowledgements

This work has been carried out within the scope of the Doctoral Program in Law of the Autonomous University of Barcelona.

Declaration of Competing Interest

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Bibliography

Alamillo Domingo, I., Valero Torrijos, J., Fortune, D., & Martin, D. 2017. 'ARIES H2020 D2.3 - Legal Requirements and Analysis of ID Legislation and Law Enforcement Aspects'. <https://www.aries-project.eu/content/legal-requirements-and-analysis-id-legislation-and-law-enforcement-aspects-0>.

Alamillo Domingo, Ignacio. 2019. *Identificación, Firma y Otras Pruebas Electrónicas*. Aranzadi.

———. 2020. 'SSI EIDAS Legal Report'. *European Comission*. https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf.

Allen, Christopher. 2016. 'The Path to Self-Sovereign Identity'. Coin Desk. 2016. <https://www.coindesk.com/path-self-sovereign-identity>.

Babel, Matthias, and Johannes Sedlmeir. 2023. 'Bringing Data Minimization to Digital Wallets at Scale with General-Purpose Zero-Knowledge Proofs'. <http://arxiv.org/abs/2301.00823>.

Bamberger, Kenneth A, Ran Canetti, Shafi Goldwasser, Rebecca Wexler, and Evan Zimmerman. 2021. 'Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs'. *Berkeley Technology Law Journal* 37 (1): 55. <https://doi.org/http://dx.doi.org/10.2139/ssrn.3781082>.

Bandara, Eranga, Xueping Liang, Peter Foytik, Sachin Shetty, and Kasun De Zoysa.

2021. 'A Blockchain and Self-Sovereign Identity Empowered Digital Identity Platform'. *Proceedings - International Conference on Computer Communications and Networks, ICCCN* 2021-July: 1–7.
<https://doi.org/10.1109/ICCCN52240.2021.9522184>.

Ben-Sasson, Eli, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. 2014. 'Zerocash: Decentralized Anonymous Payments from Bitcoin'. *Proceedings - IEEE Symposium on Security and Privacy*, 459–74.
<https://doi.org/10.1109/SP.2014.36>.

Bernabe, Jorge Bernal, Martin David, Rafael Torres Moreno, Javier Presa Cordero, Sébastien Bahloul, and Antonio Skarmeta. 2020. 'ARIES: Evaluation of a Reliable and Privacy-Preserving European Identity Management Framework'. *Future Generation Computer Systems* 102 (700085): 409–25.
<https://doi.org/10.1016/j.future.2019.08.017>.

Camenisch, Jan, and Anna Lysyanskaya. 2001. 'An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation'. *Advances in Cryptology—EUROCRYPT 2001, Springer, 2001*, 93–118.

Delignat-Lavaud, Antoine, Cedric Fournet, Markulf Kohlweiss, and Bryan Parno. 2016. 'Cinderella: Turning Shabby X.509 Certificates into Elegant Anonymous Credentials with the Magic of Verifiable Computation'. *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 235–54.
<https://doi.org/10.1109/SP.2016.22>.

EBSI. 2022. 'EBSI Verifiable Credentials Explained'. <https://ec.europa.eu/digital->

building-

blocks/wikis/display/EBSI/EBSI+Verifiable+Credentials#:~:text=EBSI%27s

Verifiable Credentials Framework is, the blockchain to establish trust.

Emami, Ashkan, Habib Yajam, Mohammad Ali Akhaee, and Rahim Asghari. 2023. 'A Scalable Decentralized Privacy-Preserving e-Voting System Based on Zero-Knowledge off-Chain Computations'. *Journal of Information Security and Applications* 79 (October): 103645. <https://doi.org/10.1016/j.jisa.2023.103645>.

European Union Agency for Cybersecurity -ENISA-. 2020. 'EIDAS Compliant EID Solutions Security Considerations and the Role of ENISA', no. March: 0–60. <https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions>.

———. 2022. 'Data Protection Engineering from Theory to Practice'. *Publications Office of the European Union*, 40. <https://doi.org/10.2824/09079>.

Flamini, Andrea, Giada Sciarretta, Mario Scuro, Amir Sharif, Alessandro Tomasi, and Silvio Ranise. 2024. 'On Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials'. *Journal of Information Security and Applications* 83 (May): 103789. <https://doi.org/10.1016/j.jisa.2024.103789>.

Goldwasser, Shafi, Silvio Micali, and Charles Rackoff. 1985. 'Knowledge Complexity of Interactive Proof-Systems.' *Conference Proceedings of the Annual ACM Symposium on Theory of Computing*, 291–304. <https://doi.org/10.1145/22145.22178>.

Izquierdo Grau, Guillem. 2023. 'Software y Algoritmos Defectuosos: Algunas Consideraciones Sobre La Responsabilidad Del Desarrollador de Software o de Sistemas de Inteligencia Artificial'. *IDP Revista de Internet Derecho y Política*, no. 38: 1–12. <https://doi.org/http://dx.doi.org/10.7238/idp.v0i38.406131>.

- Kafhali, Said El. 2024. 'Blockchain-Based Electronic Voting System: Significance and Requirements'. *Mathematical Problems in Engineering* 2024 (3).
<https://doi.org/10.1155/2024/5591147>.
- Lee, Jeonghyuk, Jungyeon Hwang, Jaekyung Choi, Hyunok Oh, and Jihye Kim. 2020. 'SIMS : Self-Sovereign Identity Management System with Preserving Privacy in Blockchain'. *IACR Cryptol. EPrint Arch*, 1–13.
<https://eprint.iacr.org/2019/1241.pdf>.
- Llaneza González, Paloma. 2021. *Identidad Digital. Actualizado a La Orden ETD/465/2021, de 6 de Mayo (Sobre Métodos de Identificación Remota) y a La Propuesta de Reglamento EIDAS2*. 1st ed. Bosch.
- Ramos Fernández, Raül. 2022. 'Reflexions Sobre El Projecte d'Identitat Digital Europea a La Llum Del Certificat COVID Digital i El Moviment Sobre La Self-Sovereign Identity'. *Revista Catalana de Dret Public* 2022 (65): 179–93.
- . 2023. 'A La Recerca Del Règim Jurídic de Les Proves de Coneixement Nul En La Construcció de La Identitat Digital Europea'. *IDP. Revista de Internet, Derecho y Política* 38: 1–12. <https://doi.org/10.7238/idp.v0i38.406015>.
- . 2024. 'Evaluation of Trust Service and Software Product Regimes for Zero-Knowledge Proof Development under EIDAS 2.0'. *Computer Law and Security Review* 53 (910). <https://doi.org/10.1016/j.clsr.2024.105968>.
- Reed, Drummond, and Alex Preukschat. 2021. *Self-Sovereign Identity*. Manning.
- Saher, GTO, Atos, UMU, ERTZ, OPCC, BFP, Sonae. 2017. 'ARIES H2020 D4.2 - Prototype Demonstration and Evaluation Plan'.

- Schwalm, Steffen, Daria Albrecht, and Ignacio Alamillo. 2022. 'EIDAS 2.0: Challenges, Perspectives and Proposals to Avoid Contradictions between EIDAS 2.0 and SSI'. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)* P-325 (July): 63–74. <https://doi.org/10.18420/OID2022>.
- Sedlmeir, Johannes, Reilly Smethurst, Alexander Rieger, and Gilbert Fridgen. 2021. 'Digital Identities and Verifiable Credentials'. *Business and Information Systems Engineering* 63 (5): 603–13. <https://doi.org/10.1007/s12599-021-00722-y>.
- Spanish Data Protection Agency -AEPD-. 2020. 'Encryption and Privacy IV: Zero-Knowledge Proofs | AEPD'. 2020. <https://www.aepd.es/en/prensa-y-comunicacion/blog/encryption-privacy-iv-zero-knowledge-proofs>.
- Vasconcelos Barros, Mauricio de, Frederico Schardong, and Ricardo Felipe Custódio. 2022. 'Leveraging Self-Sovereign Identity, Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass'. *SSRN Electronic Journal* 5694: 0–1. <https://doi.org/10.2139/ssrn.4036226>.
- W3C. 2022. 'Verifiable Credentials Data Model v1.1'. 2022. <https://www.w3.org/TR/vc-data-model/>.
- Wang, Yingwei, and David LeBlanc. 2016. 'Integrating SaaS and SaaS with Dew Computing'. *Proceedings - 2016 IEEE International Conferences on Big Data and Cloud Computing, BDCloud 2016, Social Computing and Networking, SocialCom 2016 and Sustainable Computing and Communications, SustainCom 2016*, 590–94. <https://doi.org/10.1109/BDCloud-SocialCom-SustainCom.2016.92>.