Computer Law & Security Review 53 (2024) 105968

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

Evaluation of trust service and software product regimes for zero-knowledge proof development under eIDAS 2.0

Raül Ramos Fernández

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

ARTICLE INFO

Keywords:
ZKP
eIDAS 2.0
EUDIW
Electronic attestation of attributes
SSI
Data privacy

ABSTRACT

This paper delves into two legal models for zero-knowledge proof protocols in the context of the eIDAS 2.0 Regulation: a trust service or a software product. The ARIES: reliAble euRopean Identity EcoSystem EU project highlighted the need for a legal framework for stakeholders to accept proof of the existence of user data with legal certainty, while Hyperledger Indy shows that ZKP solutions are currently commercialized, stressing deficiencies in the eIDAS 2.0. An overview of ZKP applied to identity, its relationship to the European Digital Identity Wallet and the electronic attestations of attributes, both introduced by the eIDAS 2.0, and Self-Sovereign Identity systems, leads to the central question of proof of the existence of user-held data as a trust service or as a software product and its data privacy implications for each approach. Finally, we outline a possible solution based on the product approach for future work. Our findings reveal that ZKP technology must have legal value and a presumption system to be effective. However, the path we take could lead us either to develop a system of surveillance and control in electronic environments or to build an environment where we share not the data itself but proof of its existence.

1. Introduction

The general purpose of a zero-knowledge proof (ZKP) protocol is to prove the knowledge or possession of some information without revealing anything beyond the fact that the prover knows or possesses that information[1]. These cryptographic protocols introduce a paradigm shift by moving away from traditional identity models where data is shared to a new model where we instead share proof of the existence of that data. Such a model preserves user privacy and provides control over what type of data is shared and with whom. In addition, it reduces the liability of the data controller by removing the need to store large amounts of data.

The transition towards the model of sharing identity-related proofs almost came to fruition on the European stage with the European Parliament's legislative resolution on the eIDAS 2.0 Regulation[2], adopted on 29 February 2024 and voted positively by the Council of the EU on 26 March 2024. The resolution followed the European Parliament's agreement[3] on the final version of the Regulation on 8 November 2023. In turn, the final version was published on 16 November 2023, following the report of the ITRE Committee[4] on 2 March 2023, based on the initial[5] proposal of the Regulation on 3 June 2021. The next step will be the publication of the eIDAS 2.0 in the Official Journal of the European Union.

The eIDAS 2.0 introduces two new legal objects related to identity among its new features. On the one hand, the European Identity Wallet (EUDIW), defined as *an electronic identification means which allows the*

E-mail address: raulramos@icasbd.org.

[1] Shafi Goldwasser, Silvio Micali and Charles Rackoff, 'Knowledge Complexity of Interactive Proof-Systems.' [1985] Conference Proceedings of the Annual ACM Symposium on Theory of Computing 291.

[2] European Parliament legislative resolution of 29 February 2024 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)).

[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651.

[4] REPORT on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.2.3.2023 - (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD)).

[5] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity {SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final} Brussels, 3.6.2021 COM(2021) 281 final.

https://doi.org/10.1016/j.clsr.2024.105968

Available online 30 April 2024

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. On the other hand, the electronic attestation of attributes (EAA), a new trust service defined as *an attestation in electronic form that allows attributes to be authenticated*. Despite the vagueness of the EAA's definition, these are no less than credentials and certifying acts issued by public or private authorities, such as a library card, a university degree, a driver's license, a power of attorney, a certificate of extended family, or a bank credit score.

The goal is to make users the stewards of their data through decentralization. Instead of sharing identity-related data from third-party repositories that require their intervention each time validation is needed, the data will be given to the user. This approach differs from the self-sovereign identity (SSI) model, which aims to remove user dependency on third parties. In contrast, the decentralized vision of eIDAS 2.0 is based on the sovereignty of member states and focuses on user privacy and data security. As a result, repositories and records will not disappear, but the issuer's intervention will do so when the user wants to share the data. Decentralization takes place in the user's environment when they decide with whom they want to share the data provided by the issuer and for what purpose, without the issuer knowing. In addition, the eIDAS 2.0 envisions that the user's sharing could be done through selective disclosure of partial credentials. For example, in the case of a request for proof of age, it would be sufficient to disclose only the date of birth without disclosing all the data contained in the certificate, which is what happens in the current Public Key Infrastructure, PKI, supported by traditional X.509 certificates.

To achieve a common approach to the design of the EUDIW, the European Commission adopted a Recommendation[6] on 3 June 2021, calling on Member States to work towards the development of a toolbox including a technical architecture and reference framework (ARF), a set of common standards, technical specifications, and a set of common guidelines and best practices to translate the legal specifications contained in the normative part of the Regulation, which excludes the recitals, into technical requirements.

However, while the system design is a significant step forward from a data protection perspective, it is not fully aligned with the General Data Protection Regulation[7] (GDPR), as advanced cryptographic techniques, such as the zero-knowledge proof mentioned in eIDAS 2.0 recital 14, have not been legally developed within its framework. As a result, there is no legal certainty when issuing, validating, or accepting a ZKP for relying parties - those who receive the user's credentials - when they need to prove compliance with their tax or KYC obligations to regulators, for example. Decisions related to exercising the Union's competencies, including the market and the area of freedom, security, and justice, as outlined in Article 4 of the TFEU[8], are subject to the principle of legality under Article 288 of the TFEU. This principle means that public action must be legally enabled by the principles of subsidiarity and proportionality of Article 5 TFEU through adopting regulations, directives, decisions, recommendations, and opinions. Even if there are no technical concerns about the performance of ZKPs, the main obstacles to encouraging development and investment in zero-knowledge systems are the lack of legal certainty for relying parties and developers that they will not be exposed to significant risks and the lack of enabling legislation to harmonize the use of ZKPs under eIDAS 2.0 across all Member States.

Recital 14 of eIDAS 2.0 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 user's privacy. Thus, it is left to the Member States how to integrate ZKP into the EUDIW regarding its personal identification data and the electronic attestations of the attributes stored in it. The recital becomes a recommendation bound to be ineffective, just like what happened with the notification of electronic identification schemes by the Member States and their lack of interoperability under the eIDAS Regulation of 2014, which is one of the reasons given for the launch of the EUDIW in the explanatory memorandum of the eIDAS amendment published on 3 June 2021.

Consequently, the eIDAS 2.0 has to contain explicit provisions for the use of zero-knowledge proofs that, on the one hand, may be tied to the electronic attestations of attributes and, on the other hand, may be included in the EUDIW or used standalone for the sole effect of electronic attestations if the Member State decides that its EUDIW does not allow the issuance of ZKP. However, before discussing the possible outcomes, we need to determine how a ZKP generation should be delivered within the logic of the Regulation, as a software product or as a trust service.

The preceding is significant because, as a service, only a licensed provider can supply proof of the existence of the user's wallet data, imposing a dependency on a third party with the associated privacy concerns that the eIDAS 2.0 seeks to address through decentralization. In contrast, the logic of a product regime seems more appropriate, as it would mean addressing the guarantees of software as a product, from which the user can generate a ZKP without the assistance of a provider. Despite these differences, the fundamentals remain the same: to ensure confidence in the security of ZKP software issuance among users, wallet providers, and relying parties a legal regime is required. Such a regime should certify the product's quality through technology control rather than activity control. Activity control would suggest that someone other than the user generates the ZKP and have access to their data.

We argue that we have the tools to build ZKP systems related to identity management supported by theoretical cases studied within the European Union and actual commercial implementations. Those cases raise the question of how a technological approach regarding ZKPs should be handled legally. The question is whether zero-knowledge proof techniques are more privacy-friendly rather than through selective disclosure as envisaged by the eIDAS 2.0.

Therefore, this paper highlights the differences between the issuance of a ZKP as a trust service or as a software product to discuss if any regime simultaneously satisfies privacy, public security, and legal certainty in the EU context for a future revision of the eIDAS 2.0 according to its Article 49. We conclude that the model that satisfies the above properties is the product one.

Our findings outline a feasible legal scenario within the logic of a software product as a basis for future research. We point out a rule of equivalence between a proof of existence and the data it represents. Furthermore, we suggest that the acceptance of ZKPs by relying parties could be linked to Article 5f of eIDAS 2.0, which defines the cross-border effects of the EUDIW and imposes its acceptance on very large online providers. In this way, legal certainty can be provided to the risk-bearing party, the relying parties, when they need to provide evidence of their compliance with regulatory requirements, such as tax obligations. Finally, we consider that through technical certification by the conformity assessment bodies of the Member States and the definition of standards by the European Standardization Bodies, it is possible to establish a governance system that allows the safe technical and legal use of ZKP software with full guarantees before it is launched on the

[6] https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline.

[7] 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) (Text with EEA relevance).

[8] Consolidated version of the Treaty on the Functioning of the European Union. Official Journal C 326, 26/10/2012 P. 0001 – 0390.

market.

The remainder of the paper is structured as follows: Section 2 shows how ZKP protocols have been researched within the EU framework for digital identities and how a legal rule of equivalence with the data they refer to has previously been proposed. We also introduce a commercial identity management system that combines ZKPs with most of the features of the Self-Sovereign Identity movement, highlighting what lies beyond the eIDAS 2.0. In addition, we show the parallels of both projects with the Software-as-a-Service and Software-as-a-Product models. Section 3 introduces zero-knowledge proofs, discusses current barriers to using ZKP in the eIDAS 2.0 metasystem and its relationship to the SSI movement. Section 4 examines ZKP in the context of eIDAS 2.0 to determine what it means when ZKP is provided as a trust service or a product. Section 5 reports our findings, discusses them, outlines a software-as-a-product approach as the best privacy approach, and presents a possible legal design. Section 6 concludes the paper and suggests future research.

2. Related work

2.1. ARIES: ReliAble euRopean identity EcoSystem

An earlier work that researched the suitability of using zero-knowledge proof properties for digital identity was the ReliAble euRopean Identity EcoSystem[9] (ARIES) project under the EU Horizon 2020 Program. The aim was to provide more robust and reliable authentication in an efficient and user-friendly way while fully safeguarding subjects' rights to their data and privacy. The research concluded that a new trust service consisting of privacy-protected accreditation of the possession of personal attributes while maintaining legal certainty could be achieved by establishing an equivalence principle between the legal document and the derived self-created partial identities. This equivalence principle would effectively enhance privacy while reducing compliance costs for data controllers[10].

An in-depth study[11] showed how some ZKP protocols, such as IBM Idemix, ABC4trust credentials, or Camenisch-Lysyanskaya (CL) signatures, could be used to create identity proofs in which no credentials are sent, but only an attestation that the user possesses some identity attribute stored in a secure element. Later, a further description of how such a system could work once the user had performed the issuance protocol was conducted[12]. As a result, the user could create different proofs of possession to comply with attributes the service provider requires to access a service. This presentation protocol was based on ZKP by relying on the CL signature scheme to ensure the GDPR principle of minimal disclosure, allowing to demonstrate the possession of an attribute without disclosing the value itself to prove complex predicates about attributes, e.g., the date of birth is greater than a specific year (to check age). The authors emphasized that the primary constraint of such systems was a lack of legal certainty for relying parties and users.

To test the theoretical results of the ARIES anonymous credential system, a real use case[13] was conducted at Leeds International Airport (UK) to demonstrate how a user could deduct VAT on purchase through the system designed by the ARIES ecosystem by providing proof of the existence of a valid boarding pass generated from a digital wallet. An overview of the ARIES ecosystem is shown in Fig. 1.

A report[15] commissioned by the European Commission highlighted the main contributions of the ARIES project, namely the use of zero-knowledge proofs for identity management systems and the need for a legal presumption to provide legal certainty to these protocols. The report showed how eIDAS could legally support SSI systems and trustworthy DLT-based transactions in the Digital Single Market. It also highlighted other constraints, such as the need to define algorithms, using validated or certified software, sound operational practices, or liability to third parties for potential damages.

However, the ARIES project's main inherent limitation was its approach as a service, where a centralized identity provider generates the derived identifiers on behalf of the user and is not interoperable. While theoretically feasible, such a system was neither scalable nor economically efficient, as it would require an agreement between the ARIES provider and each airport where the system was to be implemented for it to operate appropriately.

2.2. Hyperledger Indy

A commercial identity management system that enhances the ARIES H2020 project is Hyperledger Indy[16], a technological solution regarded by ENISA as the most advanced SSI solution blockchain-based that "*should be considered as one of the technologies for the implementation of a European electronic identity wallet*" [17]. The solution not only complies with the eIDAS 2.0 proposal but also goes a step further in the properties desired by the new European digital identity system with the use of ZKP protocols. Thus, the framework introduced by Hyperledger Indy provides a vision of privacy aligned with the RGPD that neither eIDAS 2.0 nor the European Blockchain Services Infrastructure[18] (EBSI), an initiative of the European Commission, provide for.

Through the combination of blockchain technology with the widely accepted international recommendation of the World Wide Web Consortium (W3C), decentralized identifiers[19] (DIDs) and verifiable credentials[20] (VCs), Hyperledger Indy enables the core principles of SSI[21]. It

[9] 'ReliAble EuRopean Identity EcoSystem | ARIES Project | Fact Sheet | H2020 | CORDIS | European Commission' <https://cordis.europa.eu/project/id/700085> accessed 18 January 2023.

[10] D Alamillo Domingo, I., Valero Torrijos, J., Fortune, D., & Martin, '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>.

[11] Jorge Bernal Bernabe and others, 'Towards a Privacy-Preserving Reliable European Identity Ecosystem' (2017) 10518 LNCS Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 19.

[12] Jorge Bernal Bernabe and others, 'An Overview on ARIES: Reliable European Identity Ecosystem' [2019] Challenges in Cybersecurity and Privacy: the European Research Landscape 231.

[13] Jorge Bernal Bernabe and others, 'ARIES: Evaluation of a Reliable and Privacy-Preserving European Identity Management Framework' (2020) 102 Future Generation Computer Systems 409 <https://doi.org/10.1016/j.future.2019.08.017>.

[14] Bernabe and others, 'An Overview on ARIES: Reliable European Identity Ecosystem' (n 17).

[15] Ignacio Alamillo Domingo, 'SSI EIDAS Legal Report' [2020] European Comission <https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf>.

[16] Hyperledger White Paper Working Group, 'An Introduction to Hyperledger' <https://www.hyperledger.org/learn/white-papers>.

[17] European Union Agency for Cybersecurity -ENISA-, 'Digital Identity. Leveraging the Self-Sovereignty Identity (SSI) Concept to Build Trust' [2022] Publications Office of the European Union 15.

[18] «What is EBSI - EBSI -» <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/What+is+EBSI> accessed 18 January 2023.

[19] W3C, 'Decentralized Identifiers (DIDs) v1.0 Core Architecture, Data Model, and Representations' (2022) <https://www.w3.org/TR/did-core/> accessed 18 January 2023.

[20] W3C, 'Verifiable Credentials Data Model v1.1' (2022) <https://www.w3.org/TR/vc-data-model/> accessed 12 March 2023. accessed 18 January 2023.

[21] Christopher Allen, «The Path to Self-Sovereign Identity» (*Coin Desk*, 2016) <https://www.coindesk.com/path-self-sovereign-identity> accessed 21 January 2023.

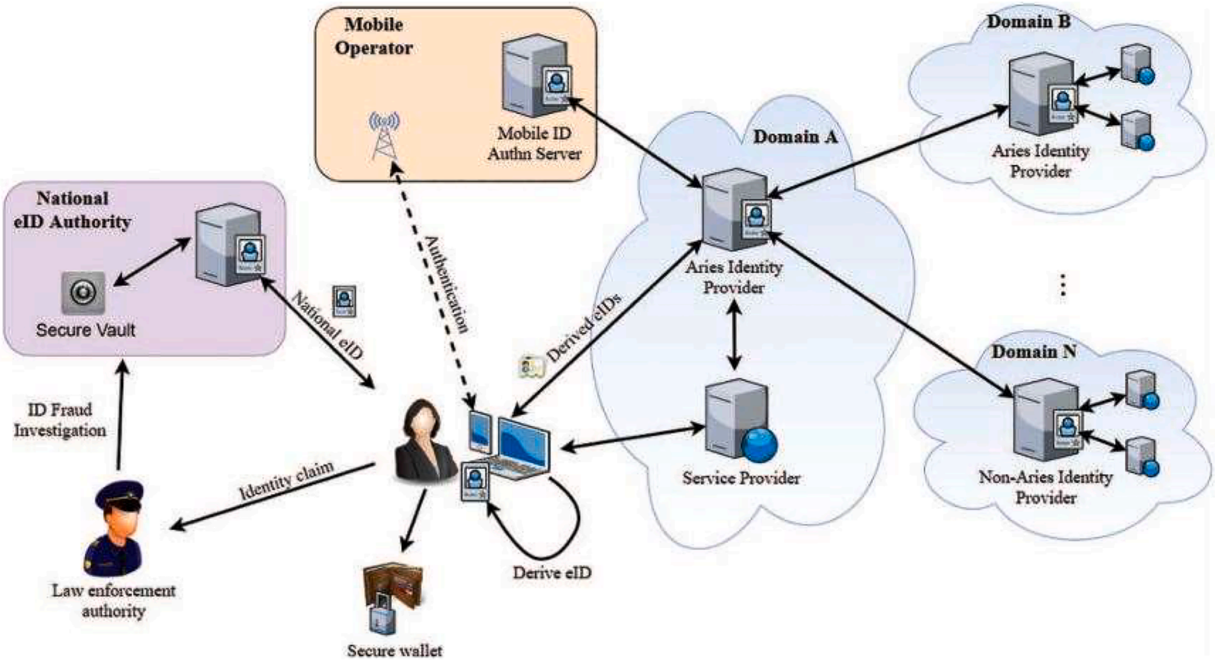

Fig. 1. Overview of the ARIES ecosystem. Once a person's identity has been provided, an ARIES provider provides a service that allows that person to self-create partial, derived identities that trustworthily assert a particular personal attribute (e.g., possessing a personal, valid boarding pass to shop at the airport or being older than a certain age)[14].

does so by removing the need for intermediaries and incorporating the ability to issue ZKPs, as the VCs are designed to do so. At the same time the Verifiable Credentials recommendation enables selective disclosure and multi-credential proofing, as proofs can be generated for any combination of credentials in a holder's wallet[22]. Therefore, anti-correlation is prevented by generating a unique proof for each transaction, preventing linkage issues. Thus, Hyperledger Indy is an example of a pre-existing system to eIDAS 2.0, conceived as a software product scheme where the user generates their identifiers from their wallet, interacts with blockchain networks, and can make selective disclosures or generate ZKPs.

While Hyperledger Indy presents a product approach model in which users themselves perform the cryptographic derivation of data stored in a wallet in a zero-knowledge format in a closed environment, without any third party participating in this operation and thus having access to the original data, the eIDAS 2.0 does not provide a minimum legal framework for a secure approach to the issuance of ZKP. In this sense, the lack of legal value of this type of cryptographic operation, although technically secure, prevents ZKP protocols from addressing the privacy tensions that concur when data is anchored in a network that is inherently decentralized and immutable. For example, the use of a distributed ledger technology (DLT), whose legal value is recognized in the eIDAS 2.0 under the legal object of electronic ledgers, *a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records,* as defined in Article 3 (52), for the dissemination of the cryptographic material necessary for the correct construction of a ZKP, if it is decided to use a DLT or an electronic ledger for that purpose.

3. Background

3.1. Zero-knowledge proof protocols

Zero-knowledge proofs are critical in enhancing the privacy and security of online user identity verification processes. They provide a high level of assurance that an individual possesses specific credentials or attributes required for verification without directly revealing the underlying information. This approach not only preserves user privacy but also ensures the integrity of the verification process, protecting consumers' data from theft or compromise. Additionally, zero-knowledge proofs can meet legal requirements, such as those outlined in the eIDAS and GDPR, allowing organizations to remain compliant and avoid liability.

The purpose of a ZKP is to prove knowledge of some information known or possessed by the claimant without disclosing the actual data. The cryptographic operation is done through "extractability assumptions" [23], which refers to the ability to verify that the proof is well constructed without revealing any information about the proof itself.

Thus, protocols are zero-knowledge if an efficient algorithm exists that could produce an interaction with the verifier that is indistinguishable from an honest interaction without knowing the secret value[24]. In other words, a protocol is zero-knowledge if the interaction transcript is indistinguishable from something that could have been produced without knowing the secret value.

ZKP protocols enable the verification of a wide range of statements about secret values, whether these values are hashed, committed,

[22] Drummond Reed and Alex Preukschat, *Self-Sovereign Identity* (Manning 2021) 122.

[23] Nir Bitansky and others, 'From Extractable Collision Resistance to Succinct Non-Interactive Arguments of Knowledge, and Back Again' [2012] ITCS 2012 - Innovations in Theoretical Computer Science Conference 326, 2.

[24] Amos Fiat and Adi Shamir, 'How to Prove Yourself: Practical Solutions to Identification and Signature Problems' (1987) 263 LNCS Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 186, 187.

encrypted, or signed[25]. In many application scenarios of blockchain and cloud computing, it is necessary to generate proofs without revealing the message preimage[26], so the zero-knowledge proof of the hash preimage is of great significance. Since a hash value can be generated from an input message of arbitrary length, in some application scenarios, proving that the preimage of a given hash value is known is proof that the corresponding message is possessed.

The versatility of ZKP and its application in distributed ledger technologies has led to a new field of study on cryptocurrencies with the development of many ZKP protocols, such as zkSNARK[27], Bulletproof,[28] and zkSTARK[29], to conceal transactions with the certainty of their correct execution. Such a use case attracted the attention of the SSI community to explore the use of blockchain as a critical piece to develop a decentralized public key infrastructure[30], leveraging on ZKP to avoid data correlation from multiple interactions with a single user by producing a unique proof for each transaction, thus opening lines of research for the alignment of GDPR and blockchain technologies.

Nevertheless, not all implementations that contain verified assertions without disclosing specific information are proof systems. An example is the PACE (Password Authenticated Connection Establishment) protocol used in the ICAO 9303 (International Civil Aviation Organization) standard for passports, which later led to the development of the eIDAS token set of technical specifications published in TR-03110 as a contribution to the interoperability framework for electronic identification[31].

The PACE protocol used by ICAO 9303 is not a proof system since no computation or mathematical calculation is performed within the travel instrument. What is contained is the overage or underage. Although the purpose of PACE is comparable to ZKP regarding privacy and security, it focuses specifically on secure authentication and the establishment of a secure channel. In contrast, ZKP is focused on proving the knowledge of a secret without revealing any information about that secret.

In this sense, the PACE protocol provides similar properties to a zero-knowledge proof protocol, allowing the passport chip and the chip reader to establish a secure channel without revealing the access key (PIN, password, or biometric data) in clear text. However, it is essential to distinguish that PACE focuses on establishing a secure connection through password authentication without revealing the password, rather than performing a zero-knowledge proof where one party proves to another that it knows a value without revealing any information about the value itself.

Regarding its applicability in the European Union, ICAO 9303 is an international standard that has been widely adopted worldwide since the adoption of the Chicago Convention, which entered into force for the signatory states in 1947 and whose application within the European Union is addressed by Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and residence documents issued to Union citizens and their family members exercising their right to free movement.

Therefore, although it can be argued that there are examples of specific use cases with similar characteristics similar to those of ZKP that do not have a particular regulation because they are standardized, it is also true that to harmonize their use on the territory of the European Union for market and common security purposes in the Member States, an enabling rule is necessary under the principle of legality stemming from Article 288 TFEU.

Another example that can be cited, more in the context of the ecosystem established by the EUDIW and the EAA, is the one developed by Hyperledger Indy together with the development of the Verifiable Credentials Data Model by the W3C, which precisely describes a data model for the issuance of ZKP. However, considering the impact of ZKPs on legal certainty within the European Union, public intervention becomes fully justified to prevent any compromise to legal certainty and avoid market fragmentation. Such action represents the utmost exercise of sovereignty by Member States, given that the EUDIW serves as a public good for which they are the legal guarantors.

3.2. Overview of the eIDAS 2.0 Regulation

Since its adoption in 2014, the original eIDAS Regulation established a federation of digital identities of EU citizens to enable interoperability of the Member States' identification systems for cross-border access to public services[32]. The eIDAS Cooperation Network[33] was developed to build such a system, and its development is currently governed by the Interoperability Framework Regulation[34], in line with the technological neutrality of eIDAS Article 12, allowing for the adoption of any solution as long as it complies with the eIDAS principles.

To adapt and evolve the eIDAS Regulation to new technological approaches emerging in the context of decentralization, a proposal to amend the Regulation, the eIDAS 2.0 draft, was published in June 2021, introducing a new means of identification, the European Digital Identity Wallet, and the introduction of two new trust services, the electronic attestation of attributes and the electronic ledgers. As shown in Fig. 2, the proposal aimed to broaden the framework for granting legal assurance of disruptive technical solutions, therefore granting legal value to paradigms such as SSI-like systems. On the other hand, it addressed the critical assessment and identified areas for improvement in eIDAS, such as the residual use of national identification systems due to their complexity, the willingness of the Member States to extend their identity solutions beyond their territory, and the exclusion of the private sector as an actor[35].

The main innovation of the final eIDAS 2.0 agreed on 29 February 2024, is the creation of a European Digital Identity Wallet, the EUDIW,

[25] Yang Yang and others, 'Implementation and Optimization of Zero-Knowledge Proof' [2022] Sensors 2022, 1, 6.

[26] In cryptography, we refer to the preimage as the original input used. A preimage resistance is a security property: given the digest produced by a hash function, it is impossible (or technically so hard we assume it will never happen) to reverse it and find the original input used. David Wong, *Real-World Cryptography* (Manning 2021) 21.

[27] Bitansky and others (n 33).

[28] Benedikt Bunz and others, 'Bulletproofs: Short Proofs for Confidential Transactions and More' (2018) 2018-May Proceedings - IEEE Symposium on Security and Privacy 315.

[29] Eli Ben-Sasson and others, 'Scalable, Transparent, and Post-Quantum Secure Computational Integrity' [2018] Eprint.Iacr.Org 1 <https://eprint.iacr.org/2018/046.pdf>.

[30] Reed and Preukschat (n 30) 89.

[31] European Union Agency for Cybersecurity -ENISA-, 'Digital Identity Standards. Analysis of Standardisation Requirements in Support of Cybersecurity Policy' (2023).

[32] Paloma Llaneza González, *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 edn, Bosch 2021) 142.

[33] 'Cooperation Network Resources - EID User Community -' <https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Cooperation+Network+Resources> accessed 18 January 2023.

[34] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (Text with EEA relevance).

[35] Steffen Schwalm and Ignacio Alamillo Domingo, 'Self-Sovereign-Identity & EIDAS: A Contradiction? Challenges and Chances of EIDAS 2.0' (2021) 2 European Review of Digital Administration & Law - Erdal 89, 98.

[36] Steffen Schwalm, Daria Albrecht and Ignacio Alamillo, 'EIDAS 2.0: Challenges, Perspectives and Proposals to Avoid Contradictions between EIDAS 2.0 and SSI' (2022) P-325 Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI) 63, 17.

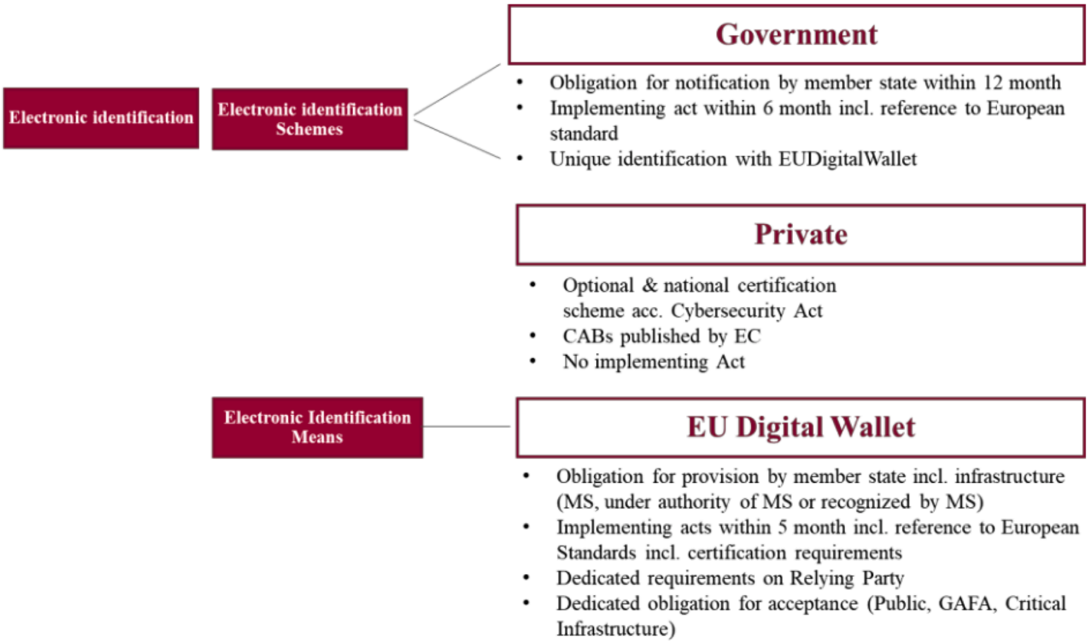
Electronic identification
Electronic identification Schemes
Government
Obligation for notification by member state within 12 month
Implementing act within 6 month incl. reference to European standard
Unique identification with EUDigitalWallet
Private
Optional & national certification scheme acc. Cybersecurity Act
CABs published by EC
No implementing Act
Electronic Identification Means
EU Digital Wallet
Obligation for provision by member state incl. infrastructure (MS, under authority of MS or recognized by MS)
Implementing acts within 5 month incl. reference to European Standards incl. certification requirements
Dedicated requirements on Relying Party
Dedicated obligation for acceptance (Public, GAFA, Critical Infrastructure)

Fig. 2. Proposal on eIDAS 2.0: Main changes on electronic identification and European Digital Identity Wallet[36].

to be issued by a Member State, on a mandate from a Member State or independently but recognized by a Member State according to Article 5a. This wallet will be optional for citizens and will be used as a means of identification through the personal identification data, PID, stored in it. It will also be used as a container for electronic certifications, known as electronic attestation of attributes. At the same time, the EUDIW should allow the selective disclosure of data and the creation of pseudonyms. Likewise, nothing prevents private sector providers from developing their wallets, different from the EUDIW, that can store electronic attestations of attributes and allow functionalities that the EUDIW does not offer, but without the effect of identifying the user from the wallet, since such a possibility is exclusive for the EUDIW.

As far as trust services are concerned, the eIDAS 2.0 creates two new ones. First, one related to the broad identity, the electronic attestation of attributes, the EAA, defined in Article 3 (44) as *means an attestation in electronic form that allows attributes to be authenticated*, which are certifying acts usually issued by public administrations or other private providers, such as a power of attorney, a driver's license, a payroll or an invoice, for example. Secondly, other one related to the assurance of electronic transactions, the electronic ledgers, defined in Article 3 (52) as *means a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records*, which is the distributed ledger technology, DLT, from the legal understanding of the European Union.

The above legal objects, the EUDIW, the EAA, and the electronic ledgers, are the legal categorization of existing elements, as seen in the Hyperledger Indy ecosystem. However, the legal definition made within the framework of the European Union answers two main reasons: first, to adapt the technology to the needs defined by the Member States through stringent controls and legal presumptions; second, to ensure that the legal certainty and public order of the Union will not be affected by a flawed implementation of the technology.

The EAA, regulated in Article 45b of eIDAS 2.0, introduces two legal effects that its Hyperledger Indy counterpart, the verifiable credential, does not enjoy, namely that *an electronic attestation of attributes shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that it is in electronic form or that it does not meet the requirements for qualified electronic attestations of attributes* and that *a qualified electronic attestation of attributes and attestations of attributes issued by, or on behalf of, a public sector body responsible for an authentic source shall have the same legal effect as lawfully issued attestations in paper form.* The latter means a rule of equivalence between the paper power of attorney or university degree with its electronic version and their admissibility in legal proceedings across the European Union.

For electronic ledgers covered by Article 45k, their legal effects, and which DLT technology such as blockchain does not enjoy, is that *an electronic ledger shall not be denied legal effect or admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers. Data records contained in a qualified electronic ledger shall enjoy the presumption of their unique and accurate sequential chronological ordering and of their integrity.* In other words, if the service meets a set of requirements, the ledger's uniqueness, integrity, and chronological sequence will be legally presumed. The aforementioned has profound effects in legal proceedings because, while blockchain technology inherently provides these properties, it will still be necessary for anyone seeking to enforce a blockchain-backed transaction to provide some evidence in court. In contrast, the legal presumption of qualified electronic ledgers reverses the burden of proof onto anyone who denies the transaction's validity. This scenario paves the way for possibilities such as designing the digital euro based on electronic ledgers or recording EUDIW transactions.

3.3. Current barriers to using ZKP in the scope of the eIDAS 2.0

Despite what has been said so far about the purpose of codifying in legal instruments the elements seen in the Hyperledger ecosystem, the eIDAS 2.0 leaves ZKPs out of the normative part of the text, in contrast to the draft of the ITRE commission of 2 March 2023, which foresaw in Article 6a(4) that *Digital Identity Wallets shall, in particular: (6) for EDIW users or relying parties, when available, to perform a zero knowledge proof inferred from person identification data or electronic attestation of attributes.*

Recital 14 of the final eIDAS 2.0 introduces that the 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 user's privacy. So, regardless of the definition given to ZKP in the Regulation, the truth is that their use is not mandatory. It is a recommendation to Member States that will imply the development of national legal regimes for ZKP that may not happen, may not be interoperable, or may not have cross-border recognition.

The fact that the ZKP protocols are mentioned in the recitals means that their mandatory application by the Member States is excluded from the normative part of the Regulation and the technical architecture and reference framework, the ARF document, which is being developed by the eIDAS group of experts from the Member States to develop a set of common standards, technical specifications, common guidelines, and best practices to translate the legal specifications contained in the normative part of the Regulation into technical requirements. Since the ARF document is non-binding, an implementing act will be required, thus recalling the subordination of the European Union's public action to the principle of legality.

With the approved eIDAS 2.0, the legal regime for ZKP will be the one developed by each Member State without cross-border effects. The reason lies in the significant differences between the private and public sectors in their contractual relationships. In the private sector, the parties can agree on terms and conditions as they wish, allowing flexibility. In contrast, the public sector is subject to a stringent regulatory framework under the principle of legality. Every action must be authorized and regulated by law to ensure transparency and efficiency in using public resources within the scope of EU competences. Therefore, the eIDAS 2.0 proposal identified Article 114 TFEU as the relevant legal basis to avoid fragmentation of the digital single market. Consequently, even though ZKP techniques are GDPR-compliant, the lack of legal certainty becomes a barrier to encouraging its use.

Indeed, according to ENISA[37], zero-knowledge proof protocols offer a unique opportunity to advance privacy and data security, which aligns with the principle of privacy by design and by default set out in Article 25 of the GDPR. The ability to minimize the exposure of personal data while facilitating rigorous verification processes is consistent with the GDPR's mandate to minimize privacy risks. It highlights the potential of ZKPs to significantly improve privacy management and data security in the digital age. However, the fact that ZKP approaches are GDPR-compliant does not automatically imply compliance with its requirements; it will be necessary to be able to evidence it, which may be difficult in a scenario where there are no specific rules to provide legal certainty to stakeholders and where cross-checking is not possible. Nevertheless, following the provisions of Article 42 of the GDPR, Member States, supervisory authorities, the Committee, and the Commission are mandated to promote the creation of data protection certification mechanisms to demonstrate compliance with the provisions of the Regulation. Thereafter, the question boils down to justifying the lack of legal guarantees for adopting technological approaches implementing ZKP protocols, which have characteristics that allow them to comply with the GDPR to a greater extent than the selective disclosure techniques envisaged for the EUDIW.

Without guarantees that their use is safe, that the market will not fragment, that there are incentives for their use, and that the investment required for their development can be recovered, neither Member States nor private sector providers will want to support these techniques. If their use is not mandatory, or if no incentive architecture is designed, the same situation will occur as with eIDAS 2014 regarding the voluntariness of Member States to notify identification systems for cross-border purposes. As stated in the explanatory memorandum of the proposal to amend eIDAS 2.0, a significant percentage of citizens have no means to access public resources across the European Union due to the lack of notified national systems, which is one of the reasons for the creation of the EUDIW.

Even with the existence of standards and formal proof methods that can be used to provide robust proof of compliance, an enabling rule is needed to give them legal enforceability, with the risk that the competent authority may consider that the technology used, however robust, does not meet a particular legal parameter, and therefore may result in a fine or economic loss for the company or Member State using such technology. It is a matter of having a legal framework that says that once the competent authority has verified that the system is working properly, there is a guarantee of compliance. Ultimately, the goal is to protect the assets and investments of those who deploy technologies in their environment with inherent risks and no defined guarantees for their use.

Regarding market fragmentation, the lack of common protocols across the Union is a significant constraint on developing ZKP functionality for the EUDIW and the EAA, even for developing additional systems outside of them. There is a risk that Member States' ZKP approaches will become isolated, undermining their usefulness in an environment moving towards seamless digital transactions across national borders. The eIDAS Regulation, emphasizing cross-border compatibility, should include mechanisms to develop at least European guidelines supported by official EU bodies, such as the approach taken with the ARF document, to provide at least a common framework for the EUDIW. In the current scenario, each Member State must design its own guidelines, develop its own systems, entrust them to the private sector, or decide not to support them, leading to an uneven provision of digital services.

The technical complexity for non-experts is also an obstacle. It is mainly why it is left to the convenience of each Member State to decide whether to implement ZKP protocols for the EUDIW and the EAA. Some Member States may be reluctant to implement technologies that rely on mathematical proof that is not human-readable and cannot be verified with the original data, where cross-checking is not possible. Without a proper framework to ensure the soundness of the technology across the EU, Member States may refuse to accept a mandatory regime for ZKP in the EU landscape or even develop a national regime. This knowledge gap may also lead to reluctance to adopt ZKP, as organizations and regulators may be unsure how to effectively implement or govern ZKP-based systems.

The absence of guarantees of legal certainty is another barrier to the generalization of ZKP techniques throughout the Union. Without prior checks to ensure the security of the technology, there is a risk that a ZKP considered valid could be manipulated, with severe consequences for the public security of the European Union. Furthermore, as the EUDIW is a public instrument, under the liability of Member States according to Article 5a(2) of the eIDAS 2.0, any new element introduced into it, whether by itself or by a third party, requires a prior administrative act to ensure the transparency and legality of the process, unlike what happens in the private sector.

From the perspective of private wallet providers, the State may decide not to allow the EUDIW the possibility to process ZKP data. Nevertheless, the eIDAS Regulation does not ban the existence of private wallets. It just means they do not have the same recognition as the EUDIW because they are not regulated. However, a private provider's wallet could issue ZKP from an EAA. Still, in the absence of a legal regime that even specifies the protocols that could be used for its use to be considered secure, the provider would have to take the risk or not offer this type of service at all.

If the competent authority were to consider that the technology used, no matter how robust, does not comply with specific legal parameters, this could lead to a fine or financial loss. It would also not be possible to comply with the law in situations of enhanced identification, as

[37] European Union Agency for Cybersecurity -ENISA-, 'Data Protection Engineering from Theory to Practice' [2022] Publications Office of the European Union 40.

provided for in Article 13 of the Fifth Anti-Money Laundering Directive[38] regarding the burden of "*identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council or any other secure, remote or electronic identification process regulated, recognized, approved or accepted by the relevant national authorities*". If no specific legal effects are provided for ZKP, its use would be deemed residual, as no provider would risk incurring a fine or, even worse, a tax crime.

Therefore, without a clear rule providing legal certainty to all stakeholders that there is no risk in exchanging or accepting a ZKP, this type of technology will not be encouraged. On the contrary, the existence of a legal provision giving EUDIW identification data and electronic attestations of attributes, qualified or not, the same legal value as their ZKP version and establishing the obligation to accept them would imply a scenario of legal certainty to know when it is mandatory to accept a ZKP and when it is not.

For users, a rule of equivalence between the ZKP data and the original data it represents would mean that they would know in which situations service providers cannot force them to provide data other than in the ZKP format. For relying parties, it would mean that supervisory authorities cannot require them to provide the original data held by the user; otherwise, relying parties would breach the minimization principle and the purpose of data processing under Article 5(1)(c) of the GDPR. For Member States, this would mean a harmonized legal regime and strict controls to ensure market cohesion and legal certainty within the scope of their national systems.

Therefore, the brake on using ZKP in the context of the eIDAS Regulation does not lie in its technical definition. Still, in the way it is to be implemented, whether the choice is left to the Member States, as is currently the case, or whether a common basis is created to encourage its use, since the investment and deployment costs may be one of the main obstacles for States or private providers to explore such techniques if they do not have the guarantee that their investments will be protected.

3.4. Zero-knowledge proof on Self-Sovereign Identity frameworks

Self-Sovereign Identity is an identity management system in which individuals manage their identity information[39]. The goal is to remove the dependency on Internet Identity Providers (IdPs) and Service Providers (SPs) that act as gatekeepers to the existence of users in electronic environments. To remove the risk of these providers arbitrarily excluding users based on the contract they entered into when accessing the service, the SSI community viewed blockchain technology as a component, but not critical or mandatory, to globally distribute databases that can serve as a trusted source of public keys without being vulnerable to single point of failure attacks. As a result, SSI is seen as the natural evolution of user-centric systems such as OpenID or OAuth, which still rely on a third party between the user and the end service provider; federated systems such as SAML, which differ from the above in that there is no lack of trust between the SP and the IdP; and centralized systems where each SP has its own IdP (Fig. 3):

In SSI systems, unlike authentication delegation systems such as the eIDAS node, where an identity provider is involved in every authentication, this role disappears. In a decentralized identity system, the subject already owns the identity data and other attributes authenticated by issuers and can share them with third parties, allowing offline verification of credentials. This scenario is more respectful of user privacy, as it reduces the risk of identity theft and prevents the identity provider from monitoring user behavior since the metadata of authentication transactions allows for the creation of user profiles[41].

For example, SSI blockchain-based systems decentralize identity by leveraging two widely used W3C standards: verifiable credentials (VC) and decentralized identifiers (DID). The latter are entity-specific URL-based identifiers that are portable[42]. VC, on the other hand, conveys an issuer's assertions in a tamper-proof and privacy-preserving manner[43]. ZKP helps achieve true privacy when decentralizing identity: for DIDs, ZKP can anchor a proof of its existence in a verifiable data registry; for VC, selective disclosure schemes using zero-knowledge proofs can use claims to prove additional statements about those claims, as described in Section 5.8 of the VC recommendation regarding zero-knowledge proofs. Fig. 4 shows how a blockchain-based SSI architecture works:

Analyzed within the context of the EU, the eIDAS prevents complete decentralization since a trusted third party is always required by the Regulation, as well as to satisfy the burden of proof in any regulated industry. The apparent disadvantage, however, is one of the most significant added benefits of eIDAS 2.0, as for the first time, a lightened version of SSI gains legal trust and becomes functional in regulated environments with their burden of proof and documentation requirements that must be proven in a non-repudiating manner against trusted third parties[45]. In addition, while SSI is primarily focused on authentication, it does not engage in identity proofing, the crucial process of verifying someone's claimed identity[46]. The eIDAS 2.0 fulfills this role and cumulatively provides the essential infrastructure to make SSI-based solutions possible.

The EUDIW is the equivalent of an SSI identity server that stores declarative identity documents. Instead of having a large central repository of identities, as in centralized and federated systems, citizens have control over their identity documents. This is a decentralized identity with SSI properties. Instead of all the information being on a government server, for example, and then shared by the user with third parties, it is given directly to the user.

Legalizing DLTs as electronic ledgers under eIDAS 2.0 is valuable because it addresses the oversight problem. For instance, when a provider needs to verify a university degree, it is not required to connect directly with the issuing university to confirm the credentials' legitimacy. This approach ensures that the issuer does not have to be involved in verifying the credential when the user wants to share it with a third party. Such verification can be accomplished by recording specific non-personal information in a distributed ledger. This is one of the use cases that the EUDIW technical infrastructure can support. Still, it will be up to each State to decide how to organize it once the common reference framework for interoperability developed in the ARF document is available.

The advantage of distributed ledger technologies lies in the absence of a central provider, which significantly reduces the risk of massive identity theft. By removing the identity provider from the verification

[38] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance). PE/72/2017/REV/1. *OJ L 156, 19.6.2018, p. 43–74.*

[39] Allen (n 29).

[40] Reed and Preukschat (n 30).

[41] Ignacio Alamillo Domingo, 'El Uso de Los Sistemas de Identidad Auto-Soberana En El Sector Público Español y En La Unión Europea' (*Blockchain Intelligence*, 2019) 5 <https://blockchainintelligence.es/articulo-el-uso-de-los-sistemas-de-identidad-auto-soberana-en-el-sector-publico-espanol-y-en-la-union-europea-por-ignacio-alamillo/> accessed 18 January 2023.

[42] W3C (n 27).

[43] W3C (n 28).

[44] Alexander Mühle and others, 'A Survey on Essential Components of a Self-Sovereign Identity' (2018) 30 Computer Science Review 80 <https://doi.org/10.1016/j.cosrev.2018.10.002>.

[45] Schwalm, Albrecht and Alamillo (n 47).

[46] Jérémie Grandsenne, 'Workshop Report E-Identity' [2018] EU Blockchain Observatory and Forum <https://www.eublockchainforum.eu/sites/default/files/reports/workshop_5_report_-_e-identity.pdf>.

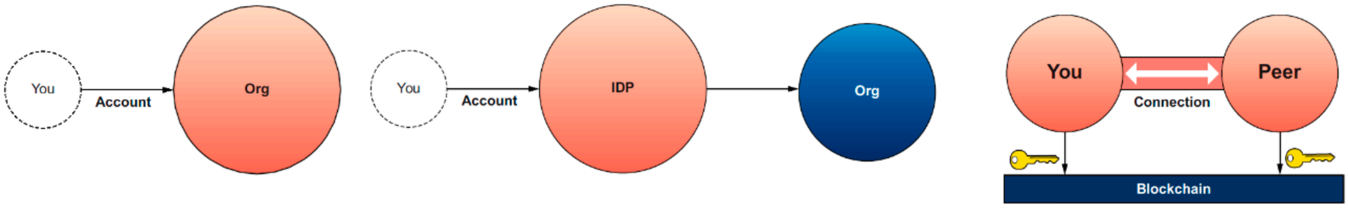

Fig. 3. Centralized, federated/user-centric, and Self-Sovereign Identity models based on blockchain [40].

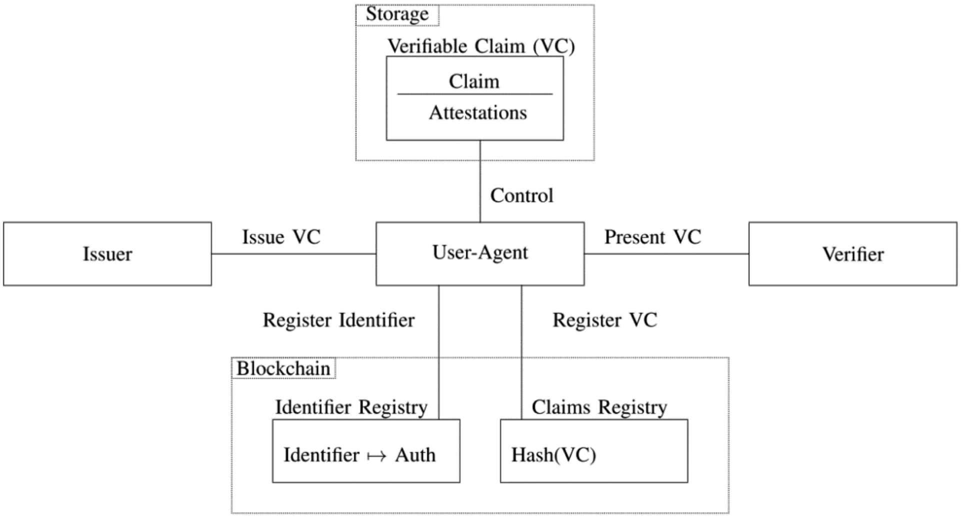

Fig. 4. Blockchain-based self-sovereign identity architecture[44]. Other trust registries, such as centralized ones, can be used.

process, the system relies on verifying information against the ledger.

In addition, it is a system that allows the sharing of proof of data existence. Instead of a university degree or part of it through selective disclosure, a cryptographic proof of existence can be recorded on the ledger. Therefore, if it is necessary to share this information for job applications, or if it needs to be provided to multiple parties, there are no problems with potential cybersecurity risks or privacy violations, as correlation is not possible. In turn, such proofs of existence do not contain the data to which they refer since no encryption technique is used, nor is it feasible to obtain the original data through the mathematical proof[47], so they would not be rendered as personal data, allowing the use of electronic ledgers as ZKP repositories.

However, how Member States integrate the use of ZKPs into the EUDIW, how it could be developed into a standalone wallet, or how it is addressed in a future revision of eIDAS 2.0 will have significant privacy and security implications depending on the technological approach taken, whether it is a user-managed functionality or a service provided by a third party that performs the cryptographic derivation for the user. Nevertheless, the legal regime for the approved eIDAS 2.0 will be the one developed by each Member State.

4. Zero-knowledge proof protocols regime models in the context of eIDAS 2.0 Regulation

Drawing from the related work and the background provided, we are positioned to analyze the two principal models in which zero-knowledge proofs can be implemented within the context of eIDAS 2.0: through software under the control and environment of the user or through a third-party service that generates the test in an environment external to the user. The difference between the two models lies in the impact on the user's privacy. Before analyzing these models, it is pertinent to briefly outline the EUDIW legal regime as the groundwork for discussing how ZKPs could be harmonized across all member states.

4.1. The legal regime of the European Digital Identity Wallet

The eIDAS 2.0 comprises two distinguishable parts. One is related to the EUDIW as a means of identification and container of electronic attestations of attributes, and the other is related to trust services, among them the electronic attestations of attributes.

According to Article 3(42) of the eIDAS 2.0, the EUDIW is 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. In other words, the EUDIW aims to guarantee access to trusted digital identities that enable users to take control of their online interactions and presence.

On the other hand, according to Article 5a (2) of eIDAS 2.0, the EUDIW shall be issued by a Member State, on behalf of a Member State, or by independent entities recognized by a Member State. However, since the EUDIW cannot be independent of any third-party system, as this would mean that even the hardware would have to be provided by or on behalf of the State, some of the provisions of Article 24(2) regarding the trust service will apply. Article 24(2)(e) specifies the requirement to use trustworthy systems and products protected against modification and ensure the technical security and reliability of the operations they support. Therefore, a pseudo-regime for qualified trust services will apply to the issuance of the wallet, which makes sense for

[47] Liz George and Jubilant J. Kizhakkethottam, 'A Comparative Study of Zero Knowledge Proof and Homomorphic Encryption in Guaranteeing Data Privacy in Blockchain Applications' (2021) 9 International Journal of Advanced Research 359.

the liability regime of Article 13 for trust service providers to apply to the EUDIW development in case of damage caused by non-compliance with Article 5a (20).

Article 5c establishes cybersecurity requirements for wallets. It introduces the presumption that certification or a declaration of conformity made in accordance with a cybersecurity scheme under the ENISA[48] Regulation meets the cybersecurity requirements from Article 5a, including the "high" security level requirements for accreditation and verification. Regarding compliance with data processing operations, the certification must be carried out under the provisions of the GDPR.

4.2. *The issuance of ZKP as a trust service*

Following the outline described for the EUDIW, the cryptographic derivation in ZKP format of the credentials or personal identification data contained therein could be understood under the concept of a trust service, which refers to a regulated market for the generation of electronic evidence. A ZKP generation service would, therefore, enjoy legal effects such as the integrity, certainty, and non-repudiation presumption of the ZKP when issued by a qualified trust service.

The development of a new trust service in eIDAS 2.0, focused on issuing zero-knowledge proofs for electronic attestation of attributes or identification data from the European Digital Identity Wallet, would require a service provider to offer users technological infrastructure—either cloud-based or through software connected to the provider's servers. This infrastructure would enable the creation and issuance of a proof of existence within a monitored environment, while also maintaining a record of the issued proofs. Such an approach closely mirrors the model of the ARIES project discussed in related work.

Trust services are trustworthy because they are legally enforced, and their providers must meet specific requirements. In this way, the consumer of trust services is protected by a liability structure that holds these service providers accountable for their actions. The reason for the existence of *ex-ante* controls in the case of qualified services and *ex-post* controls in the case of unqualified services is determined by the evidential value of these services and the legally binding effects given to them. The public interest in legal certainty, effective judicial protection, and the presumption of innocence as fundamental principles of the EU justifies all these controls. Notwithstanding, such a model is interesting because of the legal effects associated with trust services. This adds an extra layer of protection against any attempt at manipulation or fraud since the trust service provider would be the one to generate the ZKP after validating the identity of the user and the data to be processed. In this way, a qualified ZKP generation service would provide integrity and non-repudiation by verifying the correct data processing used to generate the proof.

From a technical point of view, ZKP as an activity is the traditional "Software as a Service" (SaaS) model, where a provider makes its expertise, resources, and infrastructure available to a customer for a fee[49]. Instead of buying software, the customer rents a service, which is essentially the right to use the software. By licensing the user on a subscription basis, the provider maintains the system, creates backups, and guarantees that the software runs properly. While this approach is preferable to the Software as a Product (SaaP) model in many areas because the vendor always controls the system with its security measures, it has one major drawback: a high degree of dependency on the vendor.

SaaS typically refers to an on-demand software delivery model that is part of the cloud computing phenomenon[50]. It provides network access to a collection of customizable computing resources that can be delivered with minimal management and commitment from the service provider. In other words, SaaS is the user's ability to use the provider's applications running on a cloud architecture. It allows access to the service from any device, frees the user from the limitations of keeping their data on a single device, and offers great scalability by not requiring the expensive hardware and security requirements of physical devices, such as smartphones, to access the service. It is also possible to analyze which users are logging in to applications, how often, and to which modules, enabling the creation of access logs as a security requirement.

Regarding the liability and supervision regime applicable to a trust service for creating a ZKP, this would be the one contained in Sections 1 to 2 of Chapter III of the eIDAS Regulation. In contrast, Section 3 contains specific provisions for qualified trust services, including the standards to be met by the products and systems on which trust service providers wish to rely. Therefore, several horizontal standards must be met for quality, cybersecurity, and certification requirements when referring to software as a product without changing the service's nature or the full application of the eIDAS Regulation.

Since trust services are those defined as such in the eIDAS, the issuance of a ZKP under this view must be defined explicitly in the Regulation. Moreover, additional provisions would have to be added for each trust service that determines whether a proof of existence can be bound to it, e.g., for EAAs and electronic ledgers. It would also be necessary to specify for the EUDIW part that the ZKP-issuing trust service can be used for the identity data associated with it. In this way, only qualified services could benefit from the presumption that the original data is equivalent to its proof of existence. The technical standards, application rules, and cryptographic requirements to be considered by the service provider when issuing the proof should also be specified. This can be done through implementing acts or a mandate for the European standardization bodies, ETSI, ESI, CEN, and CENELEC. However, activity regulation only introduces third parties, which defeats the purpose of disintermediation and the user's control over his digital identity.

According to this scheme, only qualified trust service providers would be authorized to issue a ZKP. As such, the liability and technical obligations regime for trust service providers would be the current one, with no need for further changes. Thus, the service approach has the least impact on the approved eIDAS 2.0, which means building on the framework established since eIDAS 2014. Therefore, to develop the creation, issuance and validation of ZKP as a trust service, a new Section 11 should be added to eIDAS Chapter III.

4.3. *The issuance of ZKP as a product*

Another approach that can be developed within eIDAS 2.0 is a model akin to 'Software as a Product' (SaaP), which facilitates the creation of zero-knowledge proofs by the user independently, without the need for third-party involvement. This is different from the SaaS model, where the provider oversees the maintenance of the system, manages the user's data, processes it, and performs any operations that need to be performed on that data. Unlike the SaaS model, the user pays a license fee to download and host the software on their device, becoming the host and controlling all the tools and functionalities of the application without the need to access the environment or the developer's servers to generate the ZKP. This option requires a deeper revision in eIDAS 2.0

[48] 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) (Text with EEA relevance).

[49] Yingwei Wang and David LeBlanc, 'Integrating SaaS and SaaP with Dew Computing' [2016] 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.

[50] Alexander Benlian and Thomas Hess, 'Opportunities and Risks of Software-as-a-Service: Findings from a Survey of IT Executives' (2011) 52 Decision Support Systems 232 <https://doi.org/10.1016/j.dss.2011.07.007>.

than the one proposed in the current service model.

One current product model is Hyperledger Indy and its wallet, which are discussed in the related work section. It is offered as standalone software, where cryptographic operations are performed within the user's device environment, with no external provider accessing the data. However, the disadvantage compared to trust services is the lack of legal certainty and specific legal effects. Although these shortcomings translate into a burden of proof for the claimant asserting the soundness of the product or technology, the product approach, unlike trust services, does not require legal recognition for use in the private sector. In contrast, the principle of legality requires legal approval for use in the public sector.

The main disadvantage of the SaaP model is that the user must maintain the software according to the developer's instructions, update the application, and maintain the hardware's security[51]. It is a static design as each update requires user intervention, but it provides more control over the software since activities are performed on the device. In brief, it requires a great deal of autonomy and expertise on the user since the maintenance of basic cybersecurity and its risks are no longer transferred to a third party but are assumed from the moment the software is used.

From a legal standpoint, software, as a computer product, is subject to the law since liability can always be traced to a natural or legal person who can control the risk of such technology being harmful[52], such as the developer, the seller, or the provider. Thus, software for creating ZKP is governed by a consolidated set of dispersed horizontal rules that provide a legal reference framework. However, the risk taken by the receiver of a ZKP (e.g., a seller of alcohol) to prove compliance with his obligations (e.g., the ZKP shows that the buyer was of legal age) is the same for a ZKP software product as for ZKP as a service. The eIDAS 2.0 could solve this problem by adding a specific or generic provision for scenarios where the issuance of proof of existence may benefit from legal presumptions.

As mentioned, the relevant Union legislation has taken the form of several sets of horizontal rules addressing software products from different viewpoints, such as general product liability and safety, specific rules for products with digital components, horizontal cybersecurity requirements and data protection. Regardless of the chosen legal instrument, the current system of product certification and technical standardization is not affected.

4.3.1. General regulation of the digital product

European law in force on digital products comprises Regulation (EU) 2023/998 on general product safety[53]. Moreover, three Directives deal with the scope of controls on the delivery of digital content, product safety in general, and product liability.

First, 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 applies. This Directive sets a high level of consumer protection by establishing common rules on specific requirements for contracts between businesses and consumers for the supply of digital content or services. These rules include the conformity of digital content or services with the contract, remedies for non-conformity or non-performance of the supply and how to enforce them, and the modification of digital content or services.

Second, Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety creates an obligation to ensure that products placed on the market are safe. Articles 1 and 3 apply to anything not covered by Directive (EU) 2019/770.

Third, Directive 85/374/EEC of the Council of 25 July 1985 on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products. It establishes the notion that a producer is liable, irrespective of fault, for damage caused by the lack of safety of his product. Finally, there is a proposal for the adoption of the Product Liability Directive repealing Directive 85/374/EEC[54].

4.3.2. Cybersecurity requirements

Current legislation does not directly address specific cybersecurity requirements for products with digital content; the Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements[55] faces this issue. This Regulation sets new cybersecurity criteria for all digital products on the EU market, exceeding existing legislation. According to Recital 2, it sets boundary conditions to enable the development of secure digital products, ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufacturers take security seriously throughout the product life cycle. Recital 16 states that it complements Directive 85/374/EEC.

In addition, the Regulation proposal assigns specific tasks to ENISA, in line with its current mandate and with Article 3(2) of the Cybersecurity Act[56], which states that ENISA shall carry out the tasks conferred upon it by Union acts, laying down measures for the harmonization of laws, regulations, and administrative provisions of the Member States in the field of cybersecurity. The Regulation proposal entrusts ENISA with the development of evaluation procedures in the candidate European Cybersecurity Certification Scheme based on Common Criteria[57] (EUCC) to ensure an adequate level of cybersecurity of ICT products, services, and processes in the EU and to avoid fragmentation of the internal market around cybersecurity certification schemes. For example, a ZKP product could be certified by the EUCC following the Cybersecurity Act and the data protection certification requirements of the GDPR. In addition, the NIS 2 Directive[58], which delegates the functions of the market surveillance authority to the cybersecurity bodies of the member states, is fully applicable.

Until the entry into force of the Cyber Resilience Act[59], which mandates the creation of technical standards for the establishment of

[51] Wang and LeBlanc (n 62).

[52] Susana Navas Navarro, 'Responsabilidad Civil Del Fabricante y Tecnología Inteligente. Una Mirada Al Futuro' [2019] Diario La Ley Sección Ciberderecho.

[53] 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 (Text with EEA relevance). PE/79/2022/REV/1. *OJ L 135, 23.5.2023, p. 1–51.*

[54] 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).

[55] 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 (COM/2022/454 final).

[56] 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) (Text with EEA relevance). PE/86/2018/REV/1. *OJ L 151, 7.6.2019, p. 15–69.*

[57] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1.

[58] 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) (Text with EEA relevance). PE/32/2022/REV/2. *OJ L 333, 27.12.2022, p. 80–152.*

[59] 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).

requirements for a platform for a data exchange space for software and hardware products to be commercialized in Europe, the assessment of the level of cybersecurity to be met by the software product is governed by the international standard ISO/IEC 15408[60], also known as the Common Criteria (CC) specification, which provides a basis for evaluating the security of IT products, including software, hardware, and firmware, by ensuring that the product meets a set of security requirements. It specifies the evaluations and procedures that must be followed to ensure the reliability, integrity, and availability of the system. The six evaluated parameters are (i) functional requirements to ensure adequate protection of the information system; (ii) technical security requirements, such as authentication, encryption, authorization or auditing; (iii) implementation of the functional and security requirements; (iv) system security configuration, including devices and security parameters; (v) assessment of risks, threats, vulnerabilities, and security mechanisms implemented; and (vi) security acceptance of the criteria reflecting the security requirements.

4.3.3. *Software quality issues*

Furthermore, industry self-regulation plays an essential role in shaping the marketplace and promoting the competitiveness of companies through certification, which not only assures the end user that the product has undergone evaluation but also promotes interoperability of products by ensuring that all vendors adhere to the same guidelines. This is the case with the ISO/IEC 25000[61] family, also known as SQuaRE (Software Product Quality Requirements and Evaluation), which assesses the quality of software development processes and their characteristics. The goal is to create a single framework for evaluating the quality of the processes used in software development and the quality of the resulting products, replacing the existing ISO/IEC 9126[62] and ISO/IEC 14598[63] to become the standard for evaluating software product quality[64].

The fact that the original data to which the proof refers cannot be cross-checked justifies public intervention since confidence in the proper performance of the software used to create the ZKP rests on all the prior controls established at the product level. Consequently, there is a need for certifications regarding the approved ZKP protocols, the life cycle of the proof, and the distribution of the cryptographic material required to verify the proof, including whether these resources can access a DLT and how the proof can be verified in an offline P2P environment. These concerns need to be addressed under Article 10 of the European Standardization Regulation[65], which allows for the delegation to the European standardization bodies CEN, CENELEC, and ETSI of the definition of technical specifications and technology control to ensure the cohesion of the digital single market.

Finally, Regulation (EC) 765/2008[66] assigns to the Conformity Assessment Bodies of each Member State the responsibility for market surveillance of the products placed on the market and for certifying their conformity with the existing requirements, rules, and standards in force. This ensures a complete system of confidence in the generation, derivation, and creation of software products used with the EUDIW or on a standalone basis.

In short, this whole system of specific certifications related to European cybersecurity, quality of processes, features, performance, and GDPR compliance can guarantee trust in a ZKP. Still, it cannot guarantee the quality of the original data, which is why there are trust services such as the electronic attestation of attributes or the electronic ledgers to which a ZKP software product can be linked.

5. Discussion

The regulation of zero-knowledge proofs emerges as a primary need to ensure their proper and secure application, especially in identity services and the handling of private data. Secondly, the legal definition and the scenarios in which a ZKP can be used for public services are mandatory due to the principle of legality. Then, whether the product or the trust service approach completely satisfies public security, user privacy, and market cohesion arises.

The product model, characteristic of the common law approach, is based on self-regulation by digital service providers. These companies operate their digital identity services based on private contracts without the intervention of a specific regulatory framework. This model raises challenges in continental European law, where the civil law view predominates. The main concern is the acceptance of the regulatory practices of one Member State in another, which translates into a reluctance to adopt a system of self-regulation in the European Union, given the legal diversity and the need to ensure legal consistency among its Member States.

The service model on which the EU states are based approaches regulation from a state perspective, recognizing the existence of mistrust between Member States and resistance to creating a single market. Because of this mistrust, the construction of the Digital Single Market requires harmonization of national legislation to allow cooperation and cross-border exchange. The pursuit of two main objectives characterizes this vision: first, to establish rules that have a clear and compelling legal effect within the territory of implementation; second, to ensure that these rules have a positive impact on relations and operations between different countries, thus addressing the substantive and cross-border dimensions of regulation.

Within the Europeanist vision, the regulation of ZKP as a product is possible. However, regulatory action is necessary as EU administration decisions must have a legal basis according to the principle of legality. Moreover, both options have significant privacy implications.

The service approach implies that only an authorized provider can generate a ZKP for the user, creating a dependency on a third party that is unacceptable from a privacy perspective. The product vision, on the other hand, assumes that it is the user who, in a controlled environment, outside of the supervision of third parties, generates from a credential or the EUDIW identification data a ZKP whose quality, security, and safety are predetermined by law.

In summary, current general rules are sufficient to deal with the misconduct or liability of trust service providers and product developers.

[60] ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model.

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

[62] ISO/IEC 9126-1:2001 Software engineering — Product quality — Part 1: Quality model.

[63] ISO/IEC 14598-1:1999 Information technology — Software product evaluation — Part 1: General overview.

[64] Moisés Rodríguez and Mario Piattini, 'Experiencias En La Industria Del Software: Certificación Del Producto Con ISO/IEC 25000' [2015] CIBSE 2015 - XVIII Ibero-American Conference on Software Engineering 814.

[65] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance.

[66] 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 (Text with EEA relevance) Text with EEA relevance (OJ L 218 13.8.2008, p. 30).

For products, we have a legal body conformed to regulations, directives, and specific national rules, updated to digital elements without regard to those in the proposal phase. Trust services need legal development in the eIDAS because they are legal objects. Nevertheless, once defined, the general liability rules for trust service providers will apply according to the Regulation. Thus, the foundations for developing a legal regime for creating, processing, and validating ZKPs are currently in place, providing a solid basis for creating either a product-oriented or service-oriented approach. The question is how such systems can be built.

In the context of the product as a service (a mobile application connected to the provider's servers) or as a pure service (browser access), understood as those activities performed by third parties in exchange for remuneration, such categorization would have to be considered as a trust service for the purposes of eIDAS 2.0. This implies the application of the general product regime, by mandate of eIDAS Article 24.2, which refers to the obligation to use trustworthy products for qualified trust service providers, but without changing the service regime. However, it would be necessary to develop an additional regulation for a new ZKP service, like what happened with electronic ledgers, which are to be identified in eIDAS 2.0 as a similar equivalent to distributed ledger technologies.

On the contrary, in a pure product regime, it would be necessary to make explicit: what the legal effects are; when a ZKP is mandatory for the acceptance of relying parties, which could be linked to the cross-border trust and the mandatory acceptance of the EUDIW for very large online platform providers imposed in Article 5f of eIDAS 2.0; and to which legal instruments and trust services it can be related, mainly the EUDIW, the EAA and the electronic ledgers. For each of them, it will be essential to describe its legal value, i.e., that the data to which the ZKP refers are equivalent to the data it represents and that it could not be denied in legal proceedings on the grounds that it is provided in electronic or zero-knowledge format.

Therefore, there is already a product liability regime, and if the product does not work properly, there is a whole set of safety, industrial quality, and product certification standards. Consequently, the argument that the issuance and validation of a ZKP should be treated as a matter of product regulation fits better into the current framework alongside the existing rules. It is about the guarantees of an IT product that must work in a specific way. Even if the product is based on existing trust services, such as EAA or distributed ledgers, or can be linked to EUDIW, it would still be a product. However, to generate a ZKP or link it to these trust services, specific and standardized data schemas must be established for them. The responsibility for the technical development of these schemas could be entrusted to European standardization organizations: the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI).

Relevant privacy issues must also be resolved in favor of a pure product regime. An activity scenario means that a third party performs the cryptographic derivation of the user's data in ZKP format, with privacy issues involved in the data transfer and dependency on the provider. Moreover, an activity view re-centralizes data to a third-party endpoint when relying on them for issuing a ZKP, as they must be given the data that the user has collected from multiple issuers. Consequently, this third-party ZKP issuing service could become a potencial source for profiling and a target for cybersecurity attacks.

Hence, in a pure product scenario of ZKP generation and validation, all aspects, including liability, cybersecurity, software quality, privacy, and market surveillance, are effectively addressed. This leaves us with the remaining discussion on the legal implications and certification of ZKP generation and creation software.

It should be emphasized that a zero-knowledge proof by itself should not carry any specific legal effect. Instead, the legal significance lies in the original data the ZKP represents. In essence, establishing an equivalence between the ZKP and the personal identification data of the EUDIW or electronic attestations of attributes, whether qualified or unqualified, would be sufficient for linking the legal significance of the data to its proof of existence. Thus, the legal value lies in the trust service from which the ZKP will be issued. In other words, the value of the electronic representation of a paper credential is given by the electronic attestation of attributes trust service. Nevertheless, what eIDAS 2.0 does not foresee is the legal rule that a ZKP of the EAA is also equivalent to either the paper credential or the electronic credential. Therefore, once an issuer has provided an EAA to a user, an equivalence rule between the EAA and the ZKP is required for the user to prove its possession, or some attribute contained in it in ZKP format.

Building on this concept, it would be essential within eIDAS 2.0 to clarify how a ZKP is issued based on the EUDIW identification data and to establish that the cryptographic proof is equivalent to the identification data it represents.

For trust services, it would be necessary to specify that for each service, mainly the EAA and the electronic ledgers, its version in ZKP format retains the same validity as the original data. For instance, a paper diploma digitized and issued in a qualified EAA, its cryptographic derivation in the ZKP would retain the same value. It would be equivalent to the original paper. In turn, proof of the existence of these data could be recorded on an electronic ledger with a full guarantee of privacy since the ZKP does not contain the data it represents since it is not an encryption technique. It would open the door to the digitalization and legal security of the traditional systems of the states of the old regime, which are based on the registrar tradition by means of documentary settlements on paper that are perpetuated today.

Following the same scheme as with the ARF document, where the legal requirements of the eIDAS 2.0 normative text are translated into technical format, the same should happen with ZKPs. The legal development of ZKPs in eIDAS 2.0 could lead to the European standardization bodies ETSI, CEN, and CENELEC being entrusted with the task of developing European standards to be followed by the Member States, including the ZKP protocols to be used, their semantic rules and their interoperability with other systems. In turn, it would be necessary to review the final framework to be approved under the ARF document (which is not mandatory; it will be the implementing act that decides on its implementation) to harmonize a data model for the EUDIW identification data, the EAA and other trust services that can be linked for the issuance, generation, and validation of ZKP.

Once the protocols to be used have been standardized and the semantic structure has been defined, together with the creation and cryptographic verification of the data in the ZKP format, the next step is for the certification and accreditation bodies of each Member State, previously authorized by the respective national accreditation body, to certify the conformity of the ZKP software products. These products may be incorporated into the EUDIW, be pluggable into it, or used as standalone products to manage EEAs and issue proofs of their existence. This incorporation should be done following the certification schemes established for cybersecurity, privacy, software quality, protocols, and semantics for zero-knowledge proof data.

Subsequently, the list of approved products in each Member State could be notified to ENISA to maintain a European registry with a dual purpose. First, to provide software with a legal presumption that the cryptographic zero-knowledge proofs derived from that software are equivalent to the original data; thus, a relying party that has accepted a ZKP from a valid boarding pass and proceeded to the VAT refund will fulfill its tax obligations by presenting the proof of the transaction issued by the verification module. Secondly, to promote the free market and the cohesion of the digital single market by enabling the free competitiveness of companies in the European Union, allowing, for example, a French consumer to purchase the product of a Belgian company.

6. Conclusions

Cryptographic zero-knowledge proof protocols allow for sharing proofs of the existence of identity-related data, introducing a paradigm shift in how identity management has been understood. It is not about doing something more efficiently but about doing things that were not possible before. The ability to share proof-of-identity data allows the tension between privacy and security presented by traditional identity management models to be bridged. However, once the technology is available, legislation is needed to make its use secure, reliable, and legally binding.

This paper aimed to critically analyze the legal framework for implementing zero-knowledge proof protocols within the eIDAS 2.0 Regulation, focusing on two potential models: ZKP as a trust service or a software product. The objectives included evaluating the implications of each model on user privacy, legal certainty, and feasibility of their application in the context of the European Digital Identity Wallet and electronic attestation of attributes while also considering the broader impact on the digital identity ecosystem in Europe.

Our contribution lies in the comprehensive analysis of both product and service models to pave the way for future integration of ZKP technologies into EU digital identity systems within the scope of the eIDAS 2.0 review that is to take place 24 months after the date of its entry into force according to Article 49 of the Regulation. By addressing both the potential benefits and challenges associated with ZKPs, we aim to set the stage for their effective and legally sound deployment in enhancing the privacy and security of digital identities across Europe.

We have highlighted the reasons that lead to the need for legal recognition of ZKPs by providing Relying Parties with legal certainty in fulfilling their legal obligations towards supervisory authorities. In addition, the legality principle governing the European Union and its Member States requires legal habilitation for using ZKP techniques. Therefore, to have a harmonized framework throughout the European Union that guarantees the security of these tools, it is necessary to develop them in eIDAS 2.0. Currently, the Regulation leaves the development of legal frameworks for ZKP to the initiative of the Member States. It means that there is no obligation to regulate ZKP in the Member States, that these frameworks are not interoperable, and that potentially different regimes may emerge, thus fragmenting the Digital Single Market.

Our study has led us to conclude that the product approach is the most suitable since there is no third-party access to the user information to generate a ZKP from it, as opposed to the service view, where a third party has access to the user's data.

A Software as a Product model, where users produce proof of the existence of the data they have been provided with, is crucial to developing a decentralized identification system where users maintain and utilize their data while ensuring high security. Since the ZKPs do not contain the data they refer to, they also reveal nothing more than the claimant's knowledge or possession. Such a characteristic overcomes two security issues: sharing information over an insecure channel like the Internet and prevent the legitimate receiver of the ZKP attempt to use it for purposes other than authorized processing.

However, giving value to the use of ZKP protocols requires answers to fundamental questions such as the attribution of the legal validity of a credential to its transformation into proof of zero knowledge, the services to which it can be linked, and the governance model for their supervision and certification; in short, to determine the participation of the public administration in the configuration of a public-legal regime that will support the use of ZKP protocols.

To address the issues raised, we outline as future work the analysis of a scenario involving the ruling of ZKP software products through preliminary technology controls before their market launch under the supervision of Member States. In such a framework, only ZKPs issued by certified products would be acknowledged as equivalent to the data they represent. Subsequently, the European Standardization Organizations could establish mandatory technical standards for national conformity accreditation bodies to implement in software approval processes. Additionally, ENISA could compile and maintain a list of products approved throughout the Union. Adopting this approach would ensure that Relying Parties, required to accept ZKPs on par with the EUDIW, could demonstrate compliance when required by the supervisory authority. Moreover, a unified perspective on ZKP throughout the EU would facilitate market liberalization, enhance the public security of Member States, and ensure real privacy for users.

Based on a product-oriented approach, the sketch outlined should reveal that the apparent tension between security and privacy is a false dichotomy resulting from the absence of an appropriate regulatory framework.

Author information

Raül Ramos Fernández is a PhD student at the Autonomous University of Barcelona and a lawyer at the Sabadell Bar Association (Catalonia, Spain). His academic research focuses on digital identity, DLT technologies, and zero-knowledge proof for the generation of electronic evidence.

Data availability

No data was used for the research described in the article.

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.

Data availability

No data was used for the research described in the article.

Acknowledgment

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