D7.2

Validation of DLT and GDPR compliance legal rules

SUMMARY

This document details technology to enhance user control, privacy, and maintain compliance with EU regulations.

Impressum

Internal Reference

Deliverable No.	D 7.2
Deliverable Name	Validation of DLT and GDPR compliance legal rules
Lead Participant	PROSUME
Work Package No.	7
Task No. & Name	T 7.2 Determination of cryptographic techniques for data encryption, storage and sharing. Definition of data protection in legal terms
Document (File)	GENTE-D7.2-Validation_of_DLT_and_GDPR_compliance-PU-P_R1
Issue (Save) Date	R0: 2024-08-06 R1: 2025-01-24

Document status

	Date	Person(s)	Organisation
Authors	2024-05-24	Alessia Borge, Alex D'Elia	PROSUME
Verification by	R0: 2024-07-19 R1: 2025-01-24	Laura Zabala Josephine Harris	R2M HSLU
Approval by	R0: 2024-07-25 R1: 2025-01-24	Alex D'Elia Roman Lötscher	PROSUME HSLU

Versions

	Date	Changes
Version R0	2024-02-15	First release version - consortium only
Version R1	2025-01-24	Removed *Guidelines and Requirements* chapter as content was consortium-only confidentiality level

Document sensitivity

☐	**Not Sensitive**	Contains only factual or background information; contains no new or additional analysis, recommendations or policy-relevant statements
☐	**Moderately Sensitive**	Contains some analysis or interpretation of results; contains no recommendations or policy-relevant statements
x	**Sensitive**	Contains analysis or interpretation of results with policy-relevance and/or recommendations or policy-relevant statements
☐	**Highly Sensitive Confidential**	Contains significant analysis or interpretation of results with major policy-relevance or implications, contains extensive recommendations or policy-relevant statements, and/or contain policy-prescriptive statements. This sensitivity requires SB decision.

Disclaimer

About ERA-Net Smart Energy Systems

ERA-Net Smart Energy Systems (ERA-Net SES) is a transnational joint programming platform of 30 national and regional funding partners for initiating co-creation and promoting energy system innovation. The network of owners and managers of national and regional public funding programs along the innovation chain provides a sustainable and service oriented joint programming platform to finance projects in thematic areas like Smart Power Grids, Regional and Local Energy Systems, Heating and Cooling Networks, Digital Energy and Smart Services, etc.

Co-creating with partners that help to understand the needs of relevant stakeholders, we team up with intermediaries to provide an innovation ecosystem supporting consortia for research, innovation, technical development, piloting and demonstration activities. These co-operations pave the way towards implementation in real-life environments and market introduction.

Beyond that, ERA-Net SES provides a Knowledge Community, involving key demo projects and experts from all over Europe, to facilitate learning between projects and programs from the local level up to the European level.

www.eranet-smartenergysystems.eu

Abstract

With the EUDI Digital Wallet, the main perspectives of the regulatory framework are set to improve digital inclusivity, security, and seamless integration among member states. The integration of Zero-Knowledge Proof (ZKP) technology into digital wallets significantly enhances user control and privacy while maintaining compliance with regulatory frameworks such as eIDAS and GDPR. This document details the technical and operational aspects of the EuDI Wallets, including how they can leverage ZKP technology to enhance user control, privacy, and maintain compliance with EU regulations.

Table of Contents

Impressum **2**
Abstract **4**
List of Abbreviations **6**
1. Introduction **7**
2. EuDI and ARF **10**
3. Cryptographic techniques **12**
Enhanced User Privacy 12
Increased User Control 12
Compliance with eIDAS and GDPR 13
Security and Efficiency 13
Conclusion **14**
References **15**

List of Abbreviations

CELL	Collaborative Energy Living Lab
DSO	Distribution System Operator
ER	Exploitable Results
EV	Electric Vehicle
HSLU	Lucerne University of Applied Sciences and Arts
IoT	Internet of Things
KPI	Key Performance Indicators
LEC	Local Energy Community
PV	Photovoltaics
UC	Use case

1. Introduction

On March 26, 2024, the European Council laid the groundwork for a new phase in the digitalization process of society. With the EUDI Digital Wallet, the main perspectives of the regulatory framework are set to improve digital inclusivity, security, and seamless integration among member states.

Digital Wallets based on Zero-Knowledge Proof can provide a higher level of user control and privacy by allowing users to authenticate and prove their identity without revealing sensitive information. This aligns with the eIDAS and GDPR directives by ensuring secure, private, and user-controlled digital interactions within the EU. The EUDI Wallets are designed to be interoperable and compliant with these regulations, fostering trust and adoption across the European digital landscape.

The integration of Zero-Knowledge Proof (ZKP) technology into digital wallets significantly enhances user control and privacy while maintaining compliance with regulatory frameworks such as eIDAS and GDPR. This is achieved through several key mechanisms and features inherent to ZKPs, as outlined in the following chapter.

One of the biggest challenges in managing distributed platforms built on diverse services and apps written in different languages is running on different devices (clients, servers, web browsers and mobile) while granting data integrity and the consistency of cryptographic transformations.

Despite a good level of homogeneity among cryptographic algorithms and implementations, determinism can hardly be taken for granted in this domain. The severity issue is directly proportional with the amount of different software platforms and components present in the cryptographic flow: the implementation of algorithms can differ between multiple applications and libraries, or even executing the same library function on a different OS can produce a non deterministic output, making the data unusable.

The General Data Protection Regulation (GDPR) represents a significant shift in how personal data is handled within the European Union (EU). Enacted in May 2018, the GDPR aims to give individuals greater control over their personal data while imposing stringent obligations on organizations that process this data. Key challenges include

ensuring compliance with complex requirements, such as obtaining explicit consent, enabling data portability, and implementing the right to be forgotten.

One of the primary challenges organizations face is ensuring that their databases are compliant with these regulations. Key issues include obtaining explicit consent for data collection and processing, maintaining accurate and up-to-date records of personal data, and implementing robust security measures to protect data from breaches.

Organizations must also provide mechanisms for individuals to exercise their rights under the GDPR, such as the right to access their data, rectify inaccuracies, request deletion (the right to be forgotten), and obtain data portability. These requirements necessitate comprehensive changes in database management practices, including enhanced data audit trails, encryption, and anonymization techniques.

Blockchain technology, renowned for its decentralized and immutable nature, presents unique challenges when striving for GDPR compliance. While blockchain offers enhanced security and transparency, its fundamental characteristics, such as immutability and distributed ledger architecture, conflict with GDPR principles, particularly regarding the right to erasure (right to be forgotten) and data rectification. The irreversible nature of blockchain transactions makes it challenging to amend or delete personal data, as mandated by GDPR. Additionally, the pseudonymous nature of blockchain data poses difficulties in identifying data subjects and obtaining their consent, a cornerstone of GDPR compliance. Smart contracts, integral to blockchain applications, may also introduce complexities in fulfilling GDPR requirements, especially in terms of lawful data processing and ensuring data minimization. Striking a balance between the transparency and immutability of blockchain and the data protection rights enshrined in GDPR necessitates innovative solutions and careful consideration of privacy implications. As organizations explore the potential of blockchain technology, navigating these legal and technical complexities is essential to establish GDPR-compliant blockchain ecosystems.

Utilizing blockchain technology within a GDPR-compliant framework offers several distinct advantages. Blockchain's immutable and decentralized nature inherently enhances data security and integrity, aligning with GDPR's emphasis on protecting personal data. The distributed ledger architecture of blockchain ensures transparency and accountability, facilitating compliance with GDPR's principles of accountability and transparency. Smart contracts, integral to blockchain ecosystems, can automate and

enforce GDPR compliance measures, streamlining processes such as consent management and data access requests. Blockchain's cryptographic techniques enable pseudonymization, safeguarding individuals' privacy rights while still allowing for data analysis and processing. Furthermore, blockchain's tamper-resistant nature ensures the integrity of data transactions, enhancing trust between data subjects and data controllers, a key aspect of GDPR compliance. Leveraging blockchain technology in a GDPR-compliant environment not only enhances data protection but also fosters innovation in data management practices, paving the way for more secure and transparent data ecosystems.

Our architecture satisfies the GDPR requirements by using a blend of blockchain and relational database management system (RDBMS) technology. The core strategy is to store user personal data on a standard relational database and create a unique anonymous user ID that's used to store user information on the blockchain. The blockchain does not store any user personal data; all user data on the blockchain is related to the database-stored user personal data by the anonymous ID. When a user requests to delete their information, the system deletes the user's personal data from the database, and the blockchain user information will no longer be related to the user. Blockchain data remains usable as a historical record for statistical purposes, without any relation to the individual. The user’s consent process can be managed by the system using smart contracts, and all user communications are certified by anonymous cryptographic values on the blockchain. User personal data can still be stored on the blockchain using cryptographic techniques, with keys kept by the user, or stored on the relational database.

2. EuDI and ARF

The official documents that outline the new European Digital Identity (EuDI) Architecture and Reference Framework (ARF) are provided by the European Commission and other related organizations. These documents detail the technical and operational aspects of the EuDI Wallets, including how they can leverage Zero-Knowledge Proof (ZKP) technology to enhance user control and privacy while maintaining compliance with the eIDAS regulation and the General Data Protection Regulation (GDPR).

Several key points emerge regarding the use of ZKP in Digital Wallets:

1. **Enhanced Privacy with Zero-Knowledge Proofs**:
    a. ZKP technology allows users to prove the validity of their claims, such as identity attributes, without revealing the underlying data[1].
    b. This approach minimizes data exposure and ensures that only necessary information is relayed to the main chain or verifying parties, thus preserving transaction details' privacy[1].
2. **User Control**:
    a. The EUDI Wallets give users "full control" and "sole control" over their personal data, meaning they can decide when and how their information is shared.
    b. Users have sovereignty over their data, including encryption keys and the management of data within the wallet, which may include secure hardware solutions like Secure Elements (SE) or Trusted Execution Environments (TEE)[2].
3. **Compliance with eIDAS and GDPR**:
    a. The EUDI Wallets are designed to be compliant with the eIDAS regulation, which sets the framework for electronic identification and trust services in the EU.
    b. The wallets adhere to GDPR principles, ensuring data protection by design and by default, and providing transparency and control to users over their personal data[3,4].

4. **Interoperability and Security**:
    a. The EUDI Wallets are intended to be interoperable across EU Member States, allowing users to access services both domestically and across borders with a high level of security[5].
    b. The use of ZKP within the wallets contributes to a secure authentication process, as it does not require the sharing of personal data beyond the proof of its validity[6,7].
5. **Qualified and Non-Qualified Electronic Attestations**:
    a. The EUDI Wallets can contain both qualified electronic attestations (QEA) provided by Qualified Trust Service Providers (QTSPs) and non-qualified electronic attestations (NQEAA) provided by other trust service providers.
    b. While QEA are government-backed and have a high assurance level, NQEAA can be issued for a variety of use cases, expanding the wallet's utility while still being supervised under eIDAS.

Digital Wallets based on Zero-Knowledge Proof can provide a higher level of user control and privacy by allowing users to authenticate and prove their identity without revealing sensitive information. This aligns with the eIDAS and GDPR directives by ensuring secure, private, and user-controlled digital interactions within the EU. The EUDI Wallets are designed to be interoperable and compliant with these regulations, fostering trust and adoption across the European digital landscape.

Considering that EUDI Wallets are under development in Europe, no real products exist on the market. Within the GENTE project, PROSUME developed her own Android APP as a demo only solution. The APP has to be further extended to include ZKP and Key management tools. This specific evolution will be further developed by PROSUME in the next phase after completion of the GENTE Project.

3. Cryptographic techniques

One of the challenges in managing a platform built on services and apps, running on different hardware and software environments, is the integrity of the cryptographic data: current state-of-the-art cryptography is not fully deterministic and can't ensure consistent results in a multiplatform setup. To be compliant with the European regulation framework and to maintain a good level of interoperability and compliance, we have focused on technologies that enable a high level of security and privacy for the end user. Zero-Knowledge Proof is definitely the most suitable choice because it allows to provide:

- Enhanced User Privacy
- Increased User Control
- Compliance with eIDAS and GDPR
- Security and Efficiency

Enhanced User Privacy

ZKP allows for the verification of transactions or identity claims without revealing any underlying personal information. This means that users can prove their identity, or that they have certain attributes or permissions, without disclosing the actual data. For instance, a user could prove they are of legal age to access a service without revealing their exact birth date. This significantly reduces the amount of personal data that is exposed during digital interactions, thereby enhancing privacy.

Increased User Control

Digital wallets based on ZKP technology give users unprecedented control over their personal data. Users can selectively disclose information, choosing exactly what to share and with whom. This selective disclosure is a departure from traditional digital interactions where users often have to provide more information than necessary, leading to potential privacy risks. With ZKP, users can manage their digital identities more securely and efficiently, deciding on a case-by-case basis what information is necessary for each transaction or verification process.

Compliance with eIDAS and GDPR

ZKP-based digital wallets are designed to be compliant with the eIDAS regulation and GDPR. eIDAS provides a regulatory framework for electronic identification and trust services for electronic transactions in the European Union's internal market. By enabling secure and private verification of identities and transactions, ZKP-based wallets align with eIDAS requirements for trust and security in digital services. Furthermore, the GDPR emphasizes data protection and privacy for individuals within the European Union. ZKP contributes to GDPR compliance by minimizing the amount of personal data processed, thus adhering to the data minimization principle.

Security and Efficiency

ZKP enhances the security of digital wallets by ensuring that sensitive information is not exposed during transactions or identity verifications. This reduces the risk of data breaches and identity theft. Additionally, ZKP can improve the efficiency of digital transactions by reducing the need for extensive data verification processes, thereby speeding up transactions and reducing costs.

Conclusion

The European Council has introduced the EUDI Digital Wallet, aiming to improve digital inclusivity, security, and seamless integration among member states. Zero-Knowledge Proof (ZKP) technology is integrated into digital wallets to enhance user control and privacy while complying with eIDAS and GDPR directives. The project aims to address challenges in managing distributed platforms with diverse services and apps, such as data integrity and consistency. The GENTE consortium is committed to adhering to ethical, fundamental rights, privacy, and data protection regulations, as well as national and local regulations.

The project involves engaging with end-users and conducting an ethics self-assessment to ensure compliance with international, European, and national laws. Two areas of concern are "Humans" and "Personal data." Procedures are adopted to protect the privacy of involved users, with access to sensitive information controlled with restriction policies. GENTE partners are committed to adhering to European ethical and fundamental rights standards, ensuring participants' dignity and fundamental rights are respected.

The European Digital Identity (EuDI) Architecture and Reference Framework (ARF) outlines the use of Zero-Knowledge Proof (ZKP) technology in digital wallets. ZKP allows users to prove the validity of their claims without revealing underlying data, preserving transaction details' privacy. Users have full control over their personal data, including encryption keys and data management within the wallet. EUDI Wallets are designed to be compliant with eIDAS and GDPR, ensuring data protection by design and default. They are designed to be interoperable across EU Member States, contributing to secure authentication processes. ZKP technology also offers enhanced user privacy, increased user control, compliance with eIDAS and GDPR, and enhanced security and efficiency. This aligns with the European Union's digital landscape and promotes trust and adoption.

References

European Commission's Digital Strategy:

https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation

https://www.identity.com/eidas-2-0-redefining-digital-identity-in-the-eu/

https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI%282022%29699491_EN.pdf

European Digital Identity Regulation Website:

https://www.european-digital-identity-regulation.com/

Secure Elements (SE) or Trusted Execution Environments (TEE):

https://www.eurosmart.com/eidas-2-0-architecture-and-reference-framework-eurosmarts-feedback/

EUR-Lex - The official site for accessing the legal text of Regulation (EU) 2016/679 (General Data Protection Regulation):

https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Digital Identity (EUDI) Wallet Architecture and Reference Framework (ARF):

https://identyum.com/unlocking-the-potential-of-eidas-2-0-what-the-new-digital-id-wallet-means-for-citizens-and-businesses/

European Commission's Digital Strategy Page:

https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

ZKProof Community Reference - This document provides a comprehensive reference for the development and standardization of zero-knowledge proof technology:

https://docs.zkproof.org/reference.pdf

More information regarding Zero Knowledge Proofs:

https://www.identity.com/what-are-zk-rollups-scalability-and-privacy-in-blockchain/

https://www.eurosmart.com/eidas-2-0-architecture-and-reference-framework-eurosmarts-feedback/

https://arxiv.org/pdf/2301.00823.pdf

FUNDING

This project has received funding in the framework of the joint programming initiative ERA-Net Smart Energy Systems' focus initiative Digital Transformation for the Energy Transition, with support from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883973.