Smart Contracts for Privacy-Preserving Identity Management: Ethics, Regulatory and Technical Challenges

Carmela Occhipinti
R&D Department
CyberEthics Lab.
Rome, Italy
email:
c.occhipinti@cyberethicslab.com

Tetiana Vasylieva
R&D Department
CyberEthics Lab.
Rome, Italy
email:
t.vasylieva@cyberethicslab.com

Luigi Briguglio
R&D Department
CyberEthics Lab.
Rome, Italy
email:
l.briguglio@cyberethicslab.com

Alessio Bianchini
R&D Department
CyberEthics Lab.
Rome, Italy
email: a.bianchini@cyberethicslab.com

Sayonara Crestani
R&D Department
CyberEthics Lab.
Rome, Italy
email: s.crestani@cyberethicslab.com

***Abstract*— Access to online data and service is a fundamental human right recognized by the United Nations. The current digital era, characterized by a continuously evolving network infrastructure which allows broadband and ubiquitous communication, can ensure this fundamental right to a broader number of citizens. However, if not properly managed, this fundamental right may be threatened by cyber threats and related identity frauds. For this reason, Identity Management (IdM) systems lay the foundation to enable this fundamental right. In the context of the IMPULSE project, the research team is adopting an "ethics-by-conception" approach to embed ethics, regulatory, and technical perspectives into the development process of the IdM system. This paper describes the ethics and regulatory framework which identifies principles and regulations to be applied during the development of an IdM system and, based on this framework, the research team identifies potential concerns and measures. This approach allows to design, implement and validate an IdM by integrating blockchain technology and smart contracts mechanism. Moreover, this IdM proposes an iconic representation to simplify the comprehension of policies in the informed consent and, therefore, it empowers users to take better decisions on access and management of their own personal data.**

Keywords* — *Privacy-Preserving Technology; Identity Management; Ethics and Regulatory Framework; Smart Contract; Blockchain; Regulation; GDPR; eIDAS.

I. INTRODUCTION

Internet access is recognised as a human fundamental right by the United Nations [1] and the implementation of broadband connection networks, including wireless and mobile technologies, is enabling this fundamental right for a continuously growing global population. Certainly, Internet access and online activities have become integral to human life for millions of citizens.

Reliable Identity Management (IdM) and verification are crucial for various online services, ranging from blog and social media login to online banking and public administration services. Therefore, even though online IdM enables ubiquitous access to data and services to a broader number of users, however, online identity fraud and cyber threats pose significant risks, affecting millions of users and making their identities vulnerable to breaches.

Privacy concerns also arise due to the exchange of personal information and for this reason, when accessing online services, users have to deal with the provision of grant to manage their own personal data (i.e., informed consent), in compliance with the General Data Protection Regulation (GDPR) [2]. Therefore, in theory, for each service, users have to manage consents during their lifecycle. In practice, user often grant consent to personal data management and forget which data they are making available and to whom.

In response to these risks, threats and concerns, the European Commission, as well as academics, corporations, and public opinion are actively focusing on resolving the issues of IdM.

In this scenario, the IMPULSE project [3] and its multidisciplinary team are focusing on the multidimensional and user-centric analysis of the transformative impact of two disruptive technologies (i.e., blockchain and artificial intelligence) on electronic IDentities (eID) for the improvement of digital public services.

This paper aims at presenting an IdM, based on blockchain and smart contracts, and its impacts from ethics, regulatory and technical perspectives. The paper is structured in four main sections representing the steps during the research process. After the introduction, Section 2 deals with the analysis of "Identity Management" and related ethics and regulatory framework. This section is relevant to better comprehend the underlying framework composed by ethics principles and regulations (i.e., General Data Protection Regulation – GDPR, electronic Identification, Authentication and Trust Services - eIDAS) which impact IdM. This framework establishes "privacy-preserving" requirements and guidelines to be embedded into the development process and outputs. Section 3 describes the "Design Approach" which is built on top of the framework and benefits from a decentralisation model enabled by distributed ledgers (i.e., blockchain technology) and the smart contracts. This section provides an analysis from the legal perspective and describes the innovative approach proposed for an easier comprehension and management of informed consents, which are fundamental elements to legally binding data access to personal data according to the GDPR. Finally, Section 4 provides conclusions on the work in progress of the IMPULSE project and the next steps.

II. IDENTITY MANAGEMENT

A. Literature Review

In literature, there are multiple definitions of Identity Management, each stressing one or more facets of IdM.

“Identity Management system provides the tools for managing all partial identities of an individual in digital world. A partial identity may or may not uniquely identify an individual.” [4]

“Identity Management is a set of functions and capabilities, for administration, management, maintenance, discovery, information exchange, policy enforcement and authentication. This is used to ensure identity information and security. It provides tools for managing individual identities in a digital environment.” [5]

“Identity Management seeks to solve the problem of remembering different user names and passwords for accessing organizations. It includes fair and lawful processing, purpose specification, data participation and control, disclosure and information security.” [6]

“Identity Management systems are used to manage user identities across multiple systems and providing a way to user access in the organization. This is done for the whole life cycle of a user in the organization by single sign-on and keeping a check on user’s credentials.” [7]

These definitions are collectively summarising various aspects of IdM.

In order to better understand the concept of IdM, it is necessary to turn to its main component, namely the concept of identity. Examining it at the philosophical and legal levels becomes clear its complex nature. Throughout history, identity has been deeply connected to state control over individuals and people’s rights and the construction of the self through a set of relational structures.

A unique identity is needed to recognise individuals' rights and responsibilities. However, being associated with a specific identity can grant privileges or lead to exclusion and discrimination. Additionally, the question arises whether identity can remain constant as a person evolves and whether individuals have the right to an identity that aligns with their self-perception.

Manders-Huits [8] points out the risk of reducing an individual's identity to a simplified "administrative" notion of it, which fails to capture its true complexity. Ishmahev and Stokkink [9] emphasise the difficulty of overcoming the complexities of identity in a workable definition that can serve as the ethical foundation for an identity management system, whether digital or otherwise.

Attempts to simplify the approach to "identity" inevitably impact key moral aspects like autonomy, self-determination and self-identification (Manders-Huits and Hoven) [10]. Ishmahev and Stokkink's analysis reveals a tension between an approach to identity management focused on the individual and his/her rights and the society.

Ishmahev and Stokkink point to the tension between individual rights and societal interests in Identity Management, using the example of the Chinese "Social Credit System” (SCS) where social scoring aims to identify and isolate "bad elements," potentially favouring society over individual rights and well-being.

The above is true of any Identity Management System but Zwitter et al. [11] highlight the new set of problems brought by Digital Identity, including the fragmentation of identity. In the digital space, individuals possess multiple Digital Identities issued by different providers, each with distinct attributes. This raises the question of whether we should strive for a single persistent identity and impose it.

Digital identity has become a crucial infrastructure service with different rules and obligations for accessing various services. It is not neutral in its shaping and management, as each provider sets its own rules, leading to fragmentation.

This raises ethical considerations about how much an individual can be considered accountable over his/her action, and how much anonymity and freedom can be favoured over public responsibility and liability. Lessig [12] emphasises that these choices are political and moral decisions when designing network capabilities and participation rules.

There are three primary models of Identity Management: Centralised, Federated, and Decentralised. The IMPULSE solution aligns with the Decentralised model, following the Self-Sovereign Identity (SSI) model and is based on Blockchain (Blockchain-Based Identity Management System (B-Based IdM)). It is important to remark that the SSI model allows the users to fully control their own data, satisfying a fundamental right defined in the GDPR regulation [2], and for this reason the European Commission selected the SSI model to for its European Digital Wallet initiative.

B. Ethics and Regulatory Framework

Within the EU framework, there is no specific regulation for B-Based IdM, but the eIDAS regulation (910/2014) [13] addresses Identity Management in general. While only one standard directly focuses on B-Based IdM, other standards cover general IdM or distributed ledgers. Consequently, there is an urgent need for EU regulation and standardisation for B-Based IdM Systems. In terms of relevant regulation law framework, the GDPR's [2] applicability to IdM systems based on Blockchain is a subject of debate. Limited scientific literature systematically addresses this issue, necessitating further understanding. Many scholars have identified several challenges to blockchain's GDPR compliance. Among them are:

The immutability of Blockchain poses difficulties in fulfilling the "right to erasure" (Article 17 [2]) and the "right of rectification" (Article 16 [2]) since blocks cannot be deleted or modified without compromising the chain's integrity. Similarly, “withdrawing consent” (Article 7 [2]) and “defining data controllers” (Article 4 [2]) become complex due to Blockchain's replication and peer-to-peer nature.

Additionally, the classification of hashed identifiers on the Blockchain as anonymised or pseudonymised data raises questions. While some argue that hashed personal data is pseudonymised, others consider it personal data subject to GDPR. The issue of pseudonymity or anonymity of hashing remains unresolved, creating a grey area.

Moreover, Self-Sovereign IdM, Kondova & Erbguth [14] state that:

“Self-Sovereign Identity (SSI) involves personal data. A detailed analysis of the system used and the use-case is required to determine what data components of the SSI constitute personal data, how the GDPR applies and who is considered to be a controller and what justifications exist. When storing some data on an immutable blockchain, it has to be ensured, that either the data stored on a blockchain will not or no longer constitute personal data, that the data subject is considered to be the controller, that the household exemption applies or a permanent justification for continuous storage on the blockchain exists. In many cases, according to Art. 35 GDPR [2], a data protection impact analysis (DPIA) will be required."

Concerning eIDAS (electronic Identification, Authentication and Trust Services) Regulation, it aims to establish trustable and reliable Digital Identities, replacing physical devices like smart cards with other authentication methods. eIDAS provides a common framework in Europe for e-signature and e-identity authentication. The Regulation distinguishes three assurance levels for electronic identification means, varying based on the degree of confidence in asserted identities.

Although the literature on Blockchain's compliance with e-IDAS is limited, integrating Blockchain into existing eIDAS standards does not seem contradictory. Blockchain can enhance security and enable the signing of various object types. Immutability remains a significant concern, also in the case of digital seals and signatures, but it does not seem to go against any part of eIDAS. Further analysis is needed to ensure compliance between B-Based IdM systems and eIDAS regulation, considering the crucial role of digital signatures and certificates in identity management.

Aiming to deliver a secure and trusted digital identity for all EU citizens, The European Commission (EC) on 3 June 2021 proposed a framework for a European Digital Identity, which builds on the revision of the current eIDAS Regulation. The EU Proposal [15], which is commonly named eIDAS 2, is currently under trilogue negotiations.

Among many amendments and changes to eIDAS, the Proposal has introduced a novel element, European Digital Identity (EUDI) Wallet which will be issued by every Member State and will be available to all EU citizens, residents, and businesses in the EU. The Wallet promotes social inclusion and fundamental rights, complying with the Charter of Fundamental Rights of the European Union. It emphasises personal data protection, security, reduced risk of ID theft, equality, solidarity, inclusion, engagement, freedom of movement, and residence. The EUDI Wallet aligns with the aims of the European Union, particularly regarding the protection and promotion of individual rights, personal data, access to services, and freedom of movement. Another innovative aspect presented by the European Commission in the Proposal concerns Article 45 (Section 11) regarding Electronic Ledgers which are effective against cyberattacks and they are present in Blockchain and Distributed Ledger Technologies (DLT). However, the European Parliament's vote on the electronic identification Regulation removed electronic ledgers as trust services, potentially impacting blockchain companies' business opportunities in providing e-identity solutions. The European DIGITAL SME Alliance, together with major IT and Blockchain associations, has sent a letter [16] to the members of the European Parliament's ITRE Committee, expressing concerns and calling for reinstating the provisions to ensure a future-proof eIDAS 2 Regulation supporting innovation and economic development.

III. Design Approach

The IMPULSE project design approach to IdM is built on top of the established ethics and regulatory framework. This approach aims at maximising benefits from decentralisation model enabled by distributed ledgers taking into consideration ethics guidelines and principles, regulatory constraints, and the impact of blockchain for electronic IDentities (eIDs) in public services from diverse standpoints, including legal, ethical, socio-economic and socio-political, technical and operational.

Indeed, decentralised model of the blockchain guarantees:

i) **Tamper-resistance and data integrity** - by design, the blockchain is a permanent and immutable storage of data blocks, therefore data added on the ledger cannot be intentionally or accidentally changed, altered or deleted by anyone. This maintains data integrity.

ii) **Data transparency and auditability** - data in the blockchain can be traced and verified by everyone in the network belonging to the blockchain, as well as data blocks constitute themselves an auditable trail of data.

iii) **Data protection** - the use of cryptography to process and store data in the blockchain protects from unauthorised accesses.

iv) **Data sharing and availability** – each node of the distributed network replicates and shares a copy of data. This network of nodes ensures high availability infrastructure.

These benefits lay the foundation for an effective IdM system [17].

Moreover, to ensure compliance with the ethics and regulatory framework, IMPULSE enables data subjects to full control sharing of and access to their own personal data through informed consent. This means that the IMPULSE system has to provide a "Consent Management" feature allowing a user to consult policies, grant consents, show the history of provided consents, and modify (when feasible) provided consents. Moreover, by considering access to public services, the IMPULSE system has to provide a "Policy Management" feature allowing a public administration (PA) to create policies, modify existing policies and retrieve the status of the users' granted consents. These two fundamental features derive from the consent mechanism defined in the GDPR regulation and for this reason the service is called GDPR Service. The use case diagram representing interactions among user, PA and GDPR Service is shown in Figure 1.

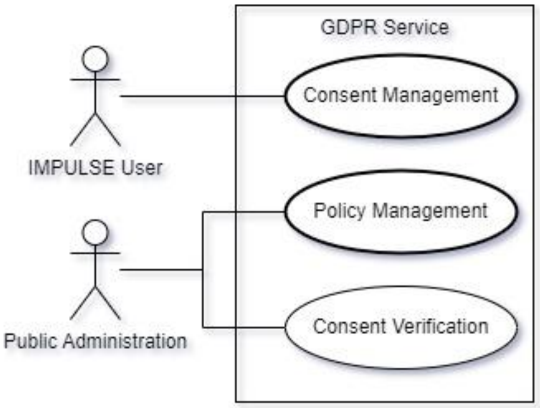


Figure 1. IMPULSE GDPR Service - use case diagram.

The GDPR Service is implemented by combining the usage of blockchain and smart contracts.

For the sake of clarity, usually, informed consents are too complicated to be fully interpreted and managed by users. For this reason, IMPULSE aims at simplifying this mechanism through the implementation of a more understandable and intuitive instance of informed consents, including a set of user-friendly meaningful icons. These icons allow user to understand what kind of personal data is going to be shared in a quick and simple way.

A. *Smart Contracts: Legal Perspectives*

The nature of a smart contract is subject to numerous conflicting viewpoints.

Legally, a "smart contract" refers to a contract represented and executed by software. Programmers instead view smart contracts as algorithmic code that performs tasks when certain conditions are met, often on a distributed ledger.

Nick Szabo was the first who proposed the concept of a smart contract in the late 1990s, defining it as a "computerised transaction protocol that executes the terms of a contract" [18]. Although not particularly innovative, Szabo argues that this idea distinguishes smart contracts by being purely digital and involving complex calculations, multipart deals, rights transfers, and encryption. It is crucial to acknowledge that a smart contract is not equivalent to a legal contract. In fact, it is often claimed that the term "smart contract" is misleading since, in many cases, smart contracts are neither intelligent nor contracts. Scholars aligned with the programmer's viewpoint contend that smart contracts do not meet the legal definition of contracts. Geiregat, instead, describes smart contracts as hardware or software “that initiates, controls, and/or documents legally relevant acts, depending on predetermined and digitally proven events, and by means of which legally binding contracts may be concluded, depending on the circumstances” [19].

Regarding the notion of smart contracts and their legal nature, there are two exact antipodes of opinion in the scientific community. Each perspective offers different solutions to the scientific challenge of establishing the legal force and effect of smart contracts. From the programmer's standpoint, a smart contract is a code designed to perform various tasks when specific conditions are satisfied. In contrast, another group of scholars supporting both traditional and eclectic views see a smart contract as a dual phenomenon that encompasses both technical and legal components. These two aspects do not merge into a unified whole.

B. *Implementation based on Smart Contracts*

Smart contracts are considered and used since the “onboarding” process, i.e., when users grant consent to a third party to access a set of predefined data, and applied during the “usage” process, i.e., when users can decide to or not to grant consent, or when necessary, to modify it according to specific needs and conditions. For these processes, users need to view and accept terms of usage of a given service and the IdM system provides them with a comprehensive view of required consents. To manage the informed consents, the IdM system defines a Consent Object which can assume two main states:

- Denied: when users want to deny access to their data to an entity, that, in the specific case of IMPULSE project, is represented by a Public Administration Service (PAS);
- Allowed: when users agree to a certain policy that enables a PAS to process data according to specific rules.

At the beginning of its lifecycle, a Consent Object is, obviously, not yet created. It is created when a user accepts or rejects a certain policy presented by the requested entity.

The Consent Object can change its own state, according to one of the following events: i) a user accepts the previously rejected policy; ii) a user rejects a previously accepted policy; iii) a user revokes the granted consent; iv) a policy change occurs; and v) a consent expires over time.

Development with smart contracts and blockchain requires to mind the “immutability” constraint which implies the unsuitability to add in the smart contract data model users’ identifiers. To prevent this concern, the GDPR service will replace users’ identifiers with pseudo-identifiers (pseudo-ids): these act as links among users and their consent objects stored on the smart contracts. Pseudo-ids are generated by using hash functions which ensure the following characteristics:

- **Deterministic**: a specific input message returns always the same output hash message. This allows the GDPR Service to process identifiers from input data without managing pseudo-ids;
- **Unique**: for each input message exists always a unique output message. This ensures security against brute force attacks and avoid collisions between pseudo-ids;
- **One-way**: hash functions cannot allow to derive the input message from the hash output message. This ensures that there is no way to directly or indirectly identify users and their data.

The GDPR service plans to make use of secure hash functions (e.g., SHA-256) to generate pseudo-ids. Pseudonymization mechanism can be enriched by combining other attributes (e.g., consent object data). The following schema in Figure 2 shows a possible approach where the pseudo-id is generated using as input the concatenation of user’s public key, pas id and policy id.

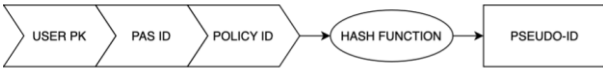


Figure 2. Pseudonymization approach.

By using the pseudo-ids, the GDPR Service works as an intermediary between personal data storages, which rely on traditional databases (such as PostgreSQL – see Figure 3), and third-party components, which need access to personal data to grant services.

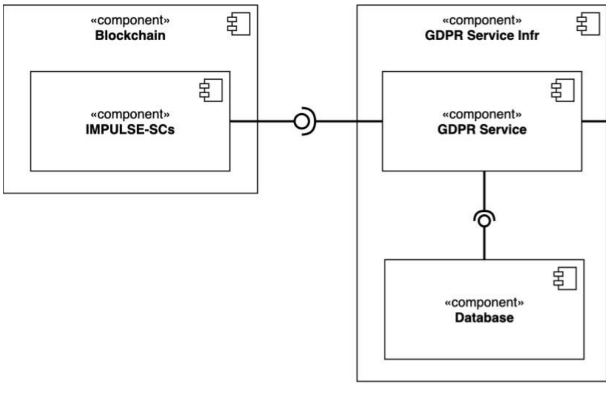


Figure 3. Component Diagram.

This approach ensures compliance with GDPR principles such as “right to modification” and “right to erasure”. Indeed, smart contracts are used to store transactions (i.e., consents) with references to data stored in the traditional database and by applying hashing functions. This ensures data integrity and auditability. To better clarify the typical use case scenario, it is considered the user requesting access to a public administration service through an application (e.g., IMPULSE app).

The GDPR Service acts as intermediary between the mobile app and the public administration service, managing the smart contracts to allow i) user registration and ii) request of the user to access. The registration phase allows users to read and understand the terms and conditions to use the system, and if they agree with the policy in place, they accept the consent. Policy acceptance enacts the GDPR Service to register metadata of the consent object, generate the pseudo-identifiers and create the smart contract.

When users want to access a public administration service, the GDPR Service checks the existence and status of the consent object, therefore based on this consent verifies its validity and enables/disables access to the public administration service. In case the consent object is “not valid” (e.g., policy expiration, revocation or modification) the application will have to show users with policy and perform appropriate rectification to the consent by involving the GDPR Service.

All these steps rely on actions performed by users which grant/revoke/modify consents based on policies defined with the Public Administration. Policies are described in the informed consents and therefore these have to be clearly understood to take the right decision.

C. *Icons for representing consent information*

To solve the long-standing problem of understanding often hard to grasp consent forms, the IMPULSE project proposes the use of a visual-based language, based on a selected and adapted set of icons from the Italian Data Protection Authority (see Figure 4) and integrated in the IdM system, with which citizens can make a complete decision about their data (e.g., who will have the permission of process their data, for which purpose, for how much time) in a fully informed, simpler and more comprehensible way.

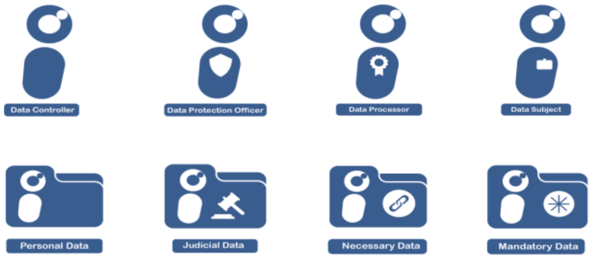
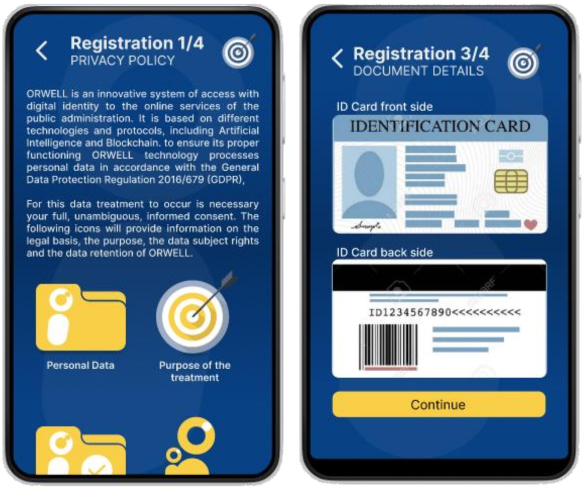


Figure 4. Set of icons to represent consent information.

This approach strengthens the comprehension of policies described in the consent, in compliance with the GDPR rules, and it represents a novelty in Identity Management systems.

This approach empowers users by respecting and protecting their fundamental rights (i.e., enabling full control of personal data), is used since the onboarding phase of the user (i.e., registration) as shown in Figure 5.



Registration 1/4
PRIVACY POLICY

ORWELL is an innovative system of access with digital identity to the online services of the public administration. It is based on different technologies and protocols, including Artificial Intelligence and Blockchain. to ensure its proper functioning ORWELL technology processes personal data in accordance with the General Data Protection Regulation 2016/679 (GDPR),

For this data treatment to occur is necessary your full, unambiguous, informed consent. The following icons will provide information on the legal basis, the purpose, the data subject rights and the data retention of ORWELL.

Registration 3/4
DOCUMENT DETAILS

Figure 5. Two phases of the user’ registration.

IV. Conclusion and Future work

This paper described a proposed solution to tackle the identified concerns of Identity Management (IdM) taking into considerations ethics, regulatory and technical perspectives. To achieve this goal, the research team of the IMPULSE project has established an “ethics-by-conception” approach starting from the identification of ethics principles, guidelines and regulation constraints impacting the IdM system.

Specifically, the IdM is expected to i) be compliant with current European regulations (i.e., GDPR and eIDAS); ii) be respectful of fundamental human rights (i.e., privacy and Internet access); iii) simplify user experience when dealing with full control of personal data and informed consents; iv) be built by adopting blockchain technology and smart contracts mechanisms.

While the current implementation in the IMPULSE project is demonstrating the feasibility and validity of design approach, as well as its compliance with the established ethics and regulatory framework, the research team is working for defining a mobile application (app) which, integrated with the GDPR Service, will allow users to full control their own personal data and informed consents.

A preliminary app is currently under development and the research team is working for finalizing and validating it.

The human-centred approach adopted in the IMPULSE project demonstrates that the integration of Social Science and Humanities (SSH) perspectives into technology development improves the comprehension of aspects and details that usually might be hidden and overlooked from the technical team, due to lack of competences. Therefore, an integrated and multidisciplinary team, as the IMPULSE project experienced, allows to understand and identify the multifaceted aspects belonging to a system to be adopted in the society, including inter-alia its impacts, and this contributes to identify potential social barriers and adopt appropriate countermeasures.

Adopting this approach since the beginning of the project and applying a continuous assessment allows a flawlessly development. Indeed, SSH experts and technology developers will be able to identify requirements and implement them since the beginning. Assuming that a single assessment will be able to ensure compliance with ethics and regulatory frameworks is practically unreasonable: new requirements will come up during the assessment, and the implemented system will risk the regulatory compliance, the acceptance from citizens and its business objectives.

ACKNOWLEDGMENT

This work is part of the IMPULSE project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101004459.

REFERENCES

[1] United Nations, "The promotion, protection and enjoyment of human rights on the Internet," July 2021. [Online] [Retrieved: August, 2023]. Available: https://documents-dds-ny.un.org/doc/UNDOC/LTD/G21/173/56/PDF/G2117356.pdf

[2] European Parliament and the Council, “The Regulation (EU) 2016/679 on 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),” [Online] [Retrieved: August, 2023]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[3] IMPULSE Project website, [Online] [Retrieved: August, 2023]. Available: https://www.impulse-h2020.eu/.

[4] S. Clauß and M. Köhntopp, "Identity management and its support of multilateral security," Computer Networks, vol. 37, no. 2, pp. 205-219, 2001.

[5] D. Chadwick, "Federated Identity Management," Foundations of Security Analysis and Design, Lecture Notes in Computer Science, vol. 5705, pp. 96-120, 2009.

[6] T. Olsen and T. Mahler, "Identity Management and Data Protection Law: Risk, Responsibility and Compliance," Circles of Trust. Computer Law & Security Report, vol. 23, no. 4, pp. 342-351, 2007.

[7] K. Tracy, "Identity management systems," IEEE Potentials, vol. 27, no. 6, pp. 34-37, 2008.

[8] N. Manders-Huits, "Practical versus moral identities in identity management," Ethics and Information Technology, vol. 12, p. 43–55, 2010.

[9] S. Q. Ishmaev Georgy, "Identity Management Systems: Singular Identities and Multiple Moral Issues, Frontiers in Blockchain," vol. 3, 2020. [Online] [Retrieved: August, 2023]. Available: https://doi.org/10.3389/fbloc.2020.00015

[10] N. Manders-Huits and J. van der Hoven, "The Need for a Value-Sensitive Design of Communication Infrastructures," Evaluating New Technologies. The International Library of Ethics, Law and Technology, vol. 3, pp. 51-60, 2009.

[11] A. Zwitter, O.J. Gstrein, and E. Yap, "Digital Identity and the Blockchain: Universal Identity Management and the Concept of the ‘Self-Sovereign’ Individual," 28 May 2020.

[12] L. Lessig, "Code and Other Laws of Cyberspace, Version 2.0," 2006. ISBN 978-0465039142.

[13] European Parliament and the Council, "The Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC," [Online] [Retrieved: August, 2023]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910.

[14] G. Kondova and J. Erbguth, “Self-Sovereign Identity on Public Blockchains and the GDPR”. Proceedings of ACM SAC Conference, Brno, Czech Republic, March 30- April 3, 2020 (SAC’20), pp. 342 – 345, 2020. DOI: 10.1145/3341105.3374066.

[15] The Commission of the European Union, "Proposal for a Regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity," [Online] [Retrieved: August, 2023]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281.

[16] "Open Letter for the preservation of the electronic ledger’s provisions in eIDAS 2," [Online] [Retrieved: August, 2023]. Available: https://inatba.org/news/savesection11-eidas2-trusted-electronic-ledgers-open-letter/.

[17] D. Augot, H. Chabanne, T. Chenevier, and W. George, "A user-centric system for verified identities on the bitcoin blockchain," Lecture Notes in Computer Science, vol. 10436 LNCS, p. 390–407, 2017.

[18] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," 1996.

[19] S. Geiregat, "Cryptocurrencies Are (Smart) Contracts,” Computer Law & Security Review, vol. 34, issue 5, pp. 1144-1149, 2018. ISSN 0267-3649.