Impulse

Identity Management in PUbLic SErvices

D3.1 EU Relevant Legal Framework

A Reconnaissance of Blockchain-Based Identity Management Systems

Lead Author: Piercosma Bisconti Lucidi (CEL)

With contributions from: Antonio Carnevale (CEL), Lydia Vogt (DIN), René Lindner (DIN), Alejandro Cuenca Parra (GRAD), Georgi Simeonov (MOP)

Reviewer: Alicia Jiménez (GRAD)

Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Delivery date:	30-06-2021
Version:	0.7
Total number of pages:	36
Keywords:	Identity Management Systems; Federated identity management; blockchain; SSO; Institutional identity management;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101004459

Executive summary

The aim of this document is making an exploration of the current EU regulatory and normative frameworks regarding the use and the impacts of the technologies of **Identity Management (IdM)** and **Blockchain-based Identity Management (B-Based IdM)** for providing trustworthy digital public services which, on the meantime, could also guarantee cybersecurity and privacy of citizens.

Accordingly, the present document has a twofold scope. As a public report, the document gives an account of the existing evidence-based practices and international legal guidelines on the field. Indeed, particularly for the B-Based IdMs, we are speaking about too much innovative and low-explored applications and, thus, their regulation and standardization often is affected by a sort of "*vacation legis*". For this reason, we think that such an operation of literature review and survey can serve to highlight the multi-disciplinary biases that will need to be implemented in the future from a juridical-normative and political point of view.

The second scope of the document is offering within the consortium a preliminary understanding of the state of the art about current risks, challenges, and opportunities of IdM and B-Based IdM, to support them to be compliant with the current and forthcoming normative and legal standpoint.

In order to perform these scopes, the document will be structured as follow:

Table 1 - Structure of D3.1

	Chapter title	Summary
1	***Introduction: The IdM***	Introduction to the basic concepts, uses and the need of identity management (IdM) systems in the digital domain.
2	***The IdM: Current Different Solutions***	Summary of the different existing approaches for IdM: centralized, federated, Single Sign On.
3	***The IdM: Open Issues***	Outline of the open issues regarding IdM: trust between entities of the federation, security of IdM and possible impacts of security breaches, proper design and user experience.
4	***National Governments and IdM Systems: A Landscape***	Summary of some of the relevant experience at the EU level for IdM systems, specific focus on the countries where the pilots will take place.
5	***B-Based IdM System***	Focus on blockchain-based identity management systems. Brief overview of the nature and functioning of a blockchain, list of some experiment of b-based IdM systems and specific focus on self-sovereign solutions
6	***EU Regulatory and Standardization Framework***	Discussion on the compliance of b-based IdM systems in the current and forthcoming regulatory framework, especially GDPR, EIDAS and the proposal of a European Identity Management regulation. Preliminary discussion on the existing standards.
7	***Conclusion***	Conclusions regarding the landscape given by this deliverable: main issues to attention are user-experience and user interfaces, compliance with GDPR.

Document information

Grant agreement No.	**687691**	**Acronym**	**IMPULSE**
Full title	**Identity Management in PUbLic SErvices**		
Call	DT-TRANSFORMATIONS-02-2020		
Project URL	www.IMPULSE-h2020.eu		
EU project officer	Giorgio CONSTANTINO		

Deliverable	**Number**	D3.1	**Title**	Blockchain-based Identity Management Systems: a Reconnaissance
Work package	**Number**	WP3	**Title**	Multidisciplinary analysis of standards, legal and ethical implications
Task	**Number**	T3.1	**Title**	Reconnaissance of the EU regulatory, legal and societal frameworks

Date of delivery	**Contractual**	M5	**Actual**	M5
Status	version 0.5		☒Final version	
Nature	☒Report ☐Demonstrator ☐Other ☐ORDP (Open Research Data Pilot)			
Dissemination level	☒Public ☐Confidential			

Authors (partners)	CEL; ISI; DIN			
Responsible author	**Name**	Piercosma Bisconti Lucidi/Riccardo Santilli/Antonio Carnevale		
	Partner	CEL	**E-mail**	p.bisconti@cyberethicslab.com

Summary (for dissemination)	The aim of this deliverable is to make an exploration of the current EU regulatory and legal frameworks, including a study on the scientific literature of current international and European regulatory framework regarding the impacts of the IMPULSE core disruptive technologies, specifically in terms of security and privacy.
Keywords	Identity Management Systems; Federated identity management; blockchain; SSO; Institutional identity management;

Version Log

Issue Date	Rev. No.	Author	Change
15/04/2021	v01	Piercosma Bisconti Lucidi (CEL)	ToC and most of the chapters
18/05/2021	v02	Antonio Carnevale (CEL)	Review and feedback on the entire document
03/06/2021	v03	Lydia Vogt & René Lindner (DIN),	Integrations on standardization
08/06/2021	v04	Piercosma Bisconti Lucidi (CEL)	Adding summary of chapters, various improvements
17/06/2021	v05	Alicia Jiménez González (GRAD)	Review and feedback on the entire document
22/06/2021	v06	Alejandro Cuenca Parra (GRAD), Georgi Simeonov (MOP) Janni Søvang (ARH)	Integration on technical sections and national identification services
28/06/2021	v07	Piercosma Bisconti Lucidi (CEL), Antonio Carnevale (CEL)	Final document for submission

Table of Contents

List of figures

List of tables

Abbreviations and acronyms

IdM: Identity Management
B-Based IdM: Blockchain-based Identity Management
IP: Identity Provider
RP: Relying Parties
SSO: Single Sign On
URI: Uniform Resource Identifier
FIdM: Federated Identity Management
B-Based IdM Systems: Blockchain Based Identity Management Systems
DL: Distributed Ledgers
BC: Blockchain
SSI: Self-Sovereign Identity
SSIdMS: Self-Sovereign Identity Management Systems
PoW: Proof of Work

1 Introduction: The IdM

While the world population exceeds 7 billion, an increasingly larger part gains internet access, now widely recognized as a human fundamental right. Meanwhile, a large part of human activities is now carried out on the web: from social media to online purchasing to public administrations, many rely on the internet for providing services and information. A large part of these activities involves the identification of the user by the provider, in order to guarantee the service. The importance of reliability of identity on the web varies depending on the type of service the user is seeking. It is of small importance in the blogs log-in, increasingly important in social media login, fundamental for online banking and public administration services.

Furthermore, the importance of a reliable and secure identification of the user is directly linked with the nature of the service and the information exchanged in the relation between the user and the provider. An urgent problem, in fact, are frauds of online identities, affecting millions of users worldwide and becoming one of the riskiest aspects of today's internet. The theft might regard emails, online banking, e-commerce, social media and countless type of services on which users rely (Kumar & Bhardwaj, 2018). While the anonymity granted by the web is one of the core of its diffusion, as Sherry Turkle reminds (Turkle, 1996), today we face multiple risks when logging on a web service. This problem involves multiple considerations.

First, every web site generally has its own log-in system, requiring the user to remember and manage an enormous number of passwords of increasing complexity. The shortcoming of this approach is that users often have few simple passwords to log in multiple web sites as highlighted by Dhamija in what he calls cognitive scalability of IdM (Dhamija & Dusseault, 2008). This implies that one single hacker's breach in one website put at risk the online identities of multiple users in multiple sites. Moreover, privacy issues are at stake: users create accounts exchanging important and sensible information with countless web sites, increasing the possibility of negative implications for privacy. On top of all, this bumbling and messy approach is highly inefficient in managing users' online identities, guaranteeing security, privacy, usability and reliability.

For all these reasons, academics, corporations, and the public opinion are increasingly focusing on resolving the issues of Identity Management (IdM). The OECD declared "the growing importance of digital identities" and they promised "to contribute to the development of the Internet Economy, we will strengthen confidence and security, through policies that ensure the protection of digital identities and personal data as well as the privacy of individuals online".

In this context, in June 2021 the European Commission proposed a framework for a European Digital Identity which will be available to all EU citizens, residents, and businesses in the EU. The new Regulation will aim to create a European Digital Identity "wallet" across all EU member states (more details in 6.2.3).

A fundamental challenge for an effective IdM is decentralizing the process. While surely the problem of identifying users is highly relevant, the *trustability* of service providers in acquiring, storing, sharing and managing users' identities is a crucial issue too. Nowadays, a small part of them is compliant with privacy safeguard, network and infrastructure security, and legal compliance. A forefront solution for IdM seems to come from the "blockchain", today at the core of the novel ideas to ensure privacy and security in identity management.

The next pages will provide an extensive reconnaissance of the existing IdM systems, the new paths of research and implementation, the institutional and corporate forerunners. Then, we will focus, in line with the IMPULSE project, on Blockchain-based Identity Management systems (B-Based IdM). Alongside, we will discuss the open issues, the privacy risks and the current regulation for this technology.

1.1 The conceptual framework of IdM

Before going deeper in analysing the different possible configuration of IdM systems it is useful to remind some basic concepts.

First, we should define what an "identity management system" is. In literature there are multiple definitions, 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." (Clauß & Köhntopp, 2001)

"Identity Management is the combination of business process and technology used to manage data on IT systems. Applications manage data for user objects, attributes, security entitlements and authentication factors" (Hitachi ID[1])

[1] Hitachi. (2014). Websso. Retrieved 22.12.2016 from http://hitachi-id.com/concepts/websso.html

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. (Chadwick, 2009)

"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" (Olsen & Mahler, 2007)

"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" (Tracy, 2008)

Those definitions, taken together, well summarize the multiplicity of aspects involved in IdM. The first definition stresses the difference between identity and individuals on the web.

The first account states that an individual may have different identities on the web, all of them legit, in respect to which attributes are shared, as we will see later. The second and third definitions focus on the fundamental functionalities and processes of IdM, which at the core have the exchange of information. Moreover, the fourth highlights the user-centeredness of IdM solving the relevant problem of countless passwords to remember, with the implications we discussed above. The last account introduces two fundamental concepts of IdM: first, the *centralization of IdM and federation of providers*; second, the most common IdM technology: *single sign-on* (SSO). These two concepts constitute the most widely used implementation of today's IdM not based on blockchain.

Before presenting the different possible solutions for identity management systems, we hereafter define the concept of identity.

1.2 The importance of managing the Internet identity

Identity management is a term that refers to administration of individual identities within a system, as a company, a country or even a network, used to manage the roles and access privileges of individual users of the network (Kumar & Bhardwaj, 2018). It enables the control of user access information and to be recognized inside the environment. The most important tasks are user creation, user deletion, lock user, unlock user, grant access, and revoke access (Zissis & Lekkas, 2012).

In the internet context the definition of identity is more troublesome than expected. If only regarding humans' online identities we may rely on Pfitzmann and Hansen's definition "An identity of an individual person may comprise many partial identities of which each represents the person in a specific context or role. A partial identity is a subset of attribute values of a complete identity, where a complete identity is the union of all attribute values of all identities of this person" (Pfitzmann & Hansen, 2010). While this definition is surely correct, in the ubiquitous web also objects, processes, and hardware may have an identity (Mead, 2003).

Maybe the most complete definition is given by Casassa (Casassa et al., 2003) defining

"identity information as a set of attributes (along with their values) describing relevant aspects and properties of an entity. This information is dynamic: the set of attributes and their values can change over time. Different views on an entity's identity information can be created, disclosed, accessed and used by multiple parties. A view consists of an aggregation of one or more attributes. Each attribute can assume different values, depending on the view it belongs to and the context where it is used. A digital identity (or identity) is itself a view on the identity information associated to an entity, at a specific point of time. Digital certificates, credentials, etc., are examples of digital identities. In general, views on identity information might include any meaningful aggregations of attributes that can be used for identification and profiling purposes, including e-mail addresses, credit card details, personal information, roles, rights, etc."

Therefore, what – technically – constitutes an identity on the internet are identifiers, credentials and attributes. Reporting from the seminal book "Identity Management Concepts, Technologies, and Systems":

- *Identifiers: A series of digits, characters, and symbols or any other form of data used to identify a subject. Identifiers can be scoped by time and/ or space. For example, a URI is globally unique over time. Pseudonyms can be temporal and effective only for a specific service. Some examples are user account names, passport numbers, mobile phone numbers, employee numbers, pseudonyms, and URI.*

- *Credentials: A set of data providing evidence for claims about parts of or entire identities. A credential can be generated based on one or more credentials. Some examples are passwords, digital certificates, fingerprints etc.*
- *Attributes: A set of data that describes the characteristics of a subject. The data includes the fundamental information for identifying a subject (e.g., full name, domicile, and date of birth), his/her preferences, and the information generated as a result of his/her activities. Some examples are given/family names, domiciles, ages, genders, roles, titles, affiliations, activity records, and reputations.* (Bertino & Takahashi, 2010)

2 The IdM: Current Different Solutions

After having clarified the key aspects of identity management on the web, and its importance for a reliable and secure internet, we proceed discussing the various solutions and implementations of IdM existing nowadays, before going deep into the implementation of blockchain-based IdM. The actual dominant solution, where every site has its own identity management system not linked with the others, in a totally unconnected way. As we discussed, this is not optimal. Therefore, different solutions are implemented. Here we discuss some solutions available on the market, highly relevant for Institutional IdM and therefore IMPULSE.

2.1 Centralised IdM

Centralized IdM are what usually users are offered. It means that a website – be it a bank, an e-commerce, a social network etc. – has its own login system, stores and verifies users' identities. There is no communication with other Identity Providers. This solution, as we discussed above, raises multiple problems both on the user side (no control over data, multiple passwords etc.) and on the provider side: the need of an IdM infrastructure, privacy and security issues, vast use of resources. The discussion among scholars and practitioners on IdM focuses precisely on how to overcome centralised and unconnected IdM systems.

2.2 Federated IdM

Federated IdM (FIdM) is probably the most promising solution today available. As Jensen (Jensen, 2012) states:

"Federated Identity Management (FIdM) is a concept that allows cooperation on identity processes, policies and technologies across company borders. It is considered a promising approach to facilitate secure resource sharing among collaborating partners in heterogeneous IT environments, and it has emerged with the recognition that individuals frequently move between corporate boundaries".

Total centralization of IdM is hardly feasible because of the massive consensus that this would require and the wide differences between countries in privacy policies and security requirements. FIdM is an association of providers where the identification of a user on one provider enables the verification of the identity on all the providers of the network. This means that a user can verify his/her identity on one provider and this authentication is valid inside all the networks, that is the number of credentials and accounts is massively reduced, improving users' experience.

Major benefits deriving from the implementation of FIdM are in fact the reduction of cost for companies because they can avoid the replication of users' data, relying on the interoperable federated login system. Another key benefit of FIdM is users experience: the reduction of accounts and the need to remember passwords. Fundamental element of the network of associated providers is a certain level of trust between each other (Chadwick 2009). In fact, the presence of only one non-trustable provider puts at risk the entire network of identity authentication. The trust inside the network is not only related to security issues, but also related to the safeguard of user's privacy and the use of their personal data. The decentralization of the network in part presupposes that all the providers will comply with certain standards in the collection, use and safeguard of the data. Related to trust there is also a problem of the increased relevance of identity thefts in FIdM: if the identity of one user is stolen in one provider the problem is widened throughout the federated network. As suggests Dhamija: "Federated identity systems that let users leverage one credential across many sites will only increase the value of the credential as a phishing target" (Dhamija & Dusseault, 2008). Therefore, the differences in security standards between the providers is a highly relevant issue for FIdM. Another problem for the presence of trust inside the network is also the dynamicity of the network: not all the identity providers know themselves but, when federated, they accept to be vulnerable to one another (Mayer et al., 1995). Interoperability, moreover, is a key goal for FIdM: lack of it would impede a smooth exchange of information between the federated providers. All these issues regard not only the technical level: management practices and standards must be produced in order to handle trust (Jensen, 2012), security/privacy and interoperability inside the network.

Federated identity management could, in the future, constitute the most effective solution to manage online identities. Given the wide increase of online-based services in the last ten years, also from the public administration, a solution will be required. This solution should have a user-centric design in order to guarantee usability and reduce privacy and security risks. Nowadays, the situation for the federation of IdM systems is well described by Bazarhanova & Smolander (2020):

"While the research on user-centric designs has attracted much attention from researchers and practitioners, many proprietary solutions are based on service-centric paradigms (e.g., services from Google, Facebook) and with only limited federation of identity data possible (i.e., Single Sign-On (SSO) is possible with e.g., Google, but limited user control on what data is shared). Existing and functioning networks of identity systems (in research, education, companies, countries, etc.) cannot be easily modified [5]. Thus, the digital identity landscape consists of many disintegrated silos of infrastructures and the real challenge is to "connect" them and allow the inter-federation of trust."

2.3 IdM as Single Sign On (SSO)

In order to overcome the issues emerging in FIdM, a solution widely used is the so-called SSO (Single Sign On) login. The most widely used protocol for SSO is OAuth 2.0, supported by all the major Identity Service providers as Google, Facebook etc (Sun & Beznosov, 2012). The functioning of SSO requires three main actors: the Identity Service Provider, the Relying Party, the user (Bazarhanova & Smolander, 2020). The first is the one who authenticates the digital identity, as for example Google or Facebook, the Relying Party is the site where the user is logging in. This solution has major benefits, and shortcomings, divisible in three groups: user experience, trustability, interoperability.

From the user's side, the process of logging in a site or online service is far easier and faster since s/he will not need to register. Moreover, the user will not need to remember many credentials since most of the sites today allow SSO login. Lastly, the use of a SSO enables an easier usability of double factor authentication systems (as for example notification or messages on the smartphone), a key element for reliable and robust IdM. A consequence is the fact that user's are not always able to verify/understand which data they are going to share through the SSO login. Privacy issues are at stake since user experience is nowadays not considered as important as it is necessary (Bazarhanova & Smolander, 2020) in the design of IdM systems.

The federated environment, with SSO, will not have a fully connected network of trust-bounded Identity Providers (IP): IPs will be only the Identity Service Providers of the SSO system, while all the other actors will be Relying Parties, managing identities but not verifying nor authorizing them. This system requires far less trust in the network maintaining the federation and the interoperability of the identities. While the reliance on trusted and security-aware companies as Google or Facebook, if the identity of a user is violated the user is actually alienated from her/his own identity tout-court, from all the services and sites. The value of phishing identities becomes even more attractive since a large part of the user's life would be at disposal. Sun & Beznosov (2012) raise concerns on the implementation of SSO :

"OAuth-based SSO systems are built upon the existing web infrastructure, but web application vulnerabilities (e.g., insufficient transport layer protection, cross-site scripting (XSS), cross-site request forgery (CSRF)) are prevalent and constantly being exploited. Moreover, as the protocol messages are passed between the RP and IdP via the browser, a vulnerability found in the browser could also lead to significant security breaches."

Moreover, other ploy can be put in practice as the SIM swapping (Jover, 2020). As this last, social engineering strategies are highly efficient in stealing identities. Therefore, while drastically reducing the probability of having the identity breached on one site, SSO also drastically increases the damage that one single identity theft may produce to the user.

Finally, while data interoperability is very high with SSO, the reliance on Google, Facebook or other popular social networks does not resolve entirely the problem of fragmented IdM: even if these providers have billion of users, nobody can be obliged to create a Google/Facebook account, therefore the Relying Parties must also have their own IdM system, to manage the identities of those users not logging through SSO. This produces useless data replication and identity conflicts between IP and RP.

3 The IdM: Open Issues

After this overview on the basic concepts and technical implementations of Identity Management Systems, in this chapter we summarize the open issues and challenges for today's IdM. In the next chapters we show how the implementation of the distributed ledger technology may help overcome these issues.

3.1 Trust

Trustability in IdM is the focal issue, especially for federated IdM. To be trustable all the identity providers (IPs) should comply and ensure the same standards on technical security and privacy. The federated environment can be more or less dynamic, still it is very unlikely that all the IPs will trust each other. OAuth SSO increases the trustability of the federation since the IPs are less and (supposedly) more secure and privacy compliant. The authentication of the user (the most trust-related element of IdM) will be a matter of few IPs, providing the service to multiple Relying Parties.

3.2 Security

Security in IdM is the key technical aspect. Security must be ensured in the three aspects of:

- Identification of the subject (to avoid false identities). More and more often biometrics systems are implemented.
- Authentication of the access (often with multiple checks as password, one time password, notification, message etc).
- Reliability and integrity of the data stored (identifiers, credentials, attributes etc).

3.3 Users' Experience

There is a delicate balance between the multiplication of authentication methods (password, captcha, one-time password, notification, messages, QR codes) and the users' experience, digital literacy and awareness about the functioning of the IdM, its risks and implications. As (Bazarhanova & Smolander, 2020) points out, the strongest system can be easily compromised if the user is not aware of how it works. A trivial example is that if users write their corporate password on a sticky note attached on the screen, the corporate rule to change password every two weeks is not only useless, but even harmful. In fact, to change the password too often will push unaware users to write it down somewhere, instead of storing it in the memory. Therefore, every technical solution must take into account the fundamental importance of the user experience in order to avoid design errors and shortcomings.

4 National Governments and IdM Systems: A Landscape

Reliable, trustable and univocal identities to identify people on the web is not only a matter of corporations or online marketing. States and institutional players increasingly rely on web services for citizens. They are far less expensive, faster and nearly paper-free. Moreover, users can interact with public administration from their homes, saving time and increasing satisfaction.

In this section we provide a landscape of Identity Management Systems in use by states and governments. Here we list all the state with a currently implemented IdM systems:

- Italy with the *Sistema Pubblico di Identità Digitale*,
- Austria with the *National Citizen Card*,
- France with *France Connect*,
- Spain with the *Documento Nacional de Identidad Electrónico*,
- Germany with the *German eID*,
- Luxembourg with the *Luxembourg National Identity Card*,
- Croatia with the *National Identification and Authentication System*,
- Belgium with the *FAS scheme*,
- Portugal with the *Cartão do Cidadão*.

4.1 IMPULSE Pilots

Against this backdrop, in the next sections, we discuss part of them, including the IdM systems of those countries in which IMPULSE pilots will take place. As we will see, most of them have the same type of functioning: a single identity with an SSO for a federated permissioned environment. First, we discuss the countries where Impulse pilots will take place, then we will give two other examples.

4.1.1 Italy

The Digital Identity system adopted by the Italian government is called SPID and stands for Sistema Pubblico di Identità Digitale (Public System for Digital Identity).

Together with Germany, Italy was the first country to notify the European Commission about the governmental Digital Identity Project. The program, that aims to implement electronic interactions between businesses, citizens and public authorities, was introduced and is managed by the Agency for Digital Italy (AGID), and is compliant with the eIDAS Regulation.

SPID is an open system that allows public and private agencies – as long as they are accredited by AGID – to offer services of electronic identification for citizens and businesses. Italy has been the only European country, so far, to adopt a system of accreditation with the participation of private companies, so not entirely regulated by governmental authorities.

Until now, the system has been used only for Public Administration's website, but the project foresees the utilization of SPID also for private companies' websites, as it may be useful when providing online bank or insurance services, for example.

Just a small number of projects for digital identity are based on authentication systems that do not involve the use of a Sim Card. Having a look at the projects so far notified, pre-notified and in development by European member states only Italy, France and Austria (with the mobile phone signature system) offer such an innovative solution.

4.1.2 Spain

The Spanish mechanism to identify a digital identity is called Documento Nacional de Identidad Electrónico (DNIe). It certificates the digital identity with two different mechanisms: the authentication certificate and the signature certificate.

The DNIe system is based on a Sim Card, which contains the same data appearing at the card (personal data such as name and surname, Spanish id card number, date of birth, e-mail address, public key linked to the citizen; photography; digitized signature and digitized fingerprint), the authentication certificate and the electronic signature. The digital identification system is accessible with the use of a computer and a card reader.

Both mechanisms, therefore, guarantee the subscriber's identity and data protection while using a government-issued document combined with a PIN[2]. The Spanish government affirms that the DNIe will assist users to easily connect with governmental authorities or public and private companies, preventing citizens from queuing or moving around to issue official documents.

Another mechanism, probably the most used one, is called Certificado Electrónico de la FNMT. This electronic certificate is a digital signature installed on the browser to accredit your identity online. It allows you to perform operations from your computer, mobile device or tablet on the online platforms of the institutions that have this system enabled.

Yet another mechanism complements the previous ones, it is called Cl@ve and provides a user/password mechanism for authentication, along with a SMS for 2-factor authentication. Cl@ve is connected to eIDAS, which allows cross-border recognition of electronic identities in accordance with European legislation and makes it possible to use European identification mechanisms in Spanish services.

4.1.3 Iceland

Also Iceland issued its own digital identity: the "electronic ID (rafræn skilríki)". The electronic identity can be verified through both smart cards and smartphone authentications. The latter requires an Iceland sim card. The password of the e-ID is obviously secured and uses Hash cryptography. To obtain an e-ID a citizen must go to banks, issuers of the e-ID, with a valid car licence, passport or physical ID. Only specific types of SIM cards are enabled for the e-ID.

With the e-ID also electronic certificates are issued: in the web page of the Iceland e-ID we can read that "Electronic certificates are based on the so-called Íslandsrót, which is owned and managed by the state. The state does not issue certificates to individuals, but sets strict conditions for the issue. Parties that issue or intend to issue certificates to individuals in Iceland are under the official supervision of the Consumer Agency. With strict requirements and its ownership of Íslandsrót, the state has full control over the environment of the documents and is responsible for the basic structure on which they are based."

With the e-ID a citizen can access banks and various types of public administration services.

4.1.4 Bulgaria

In Bulgaria a project for an electronic identity card is ongoing, and this e-ID card is expected to be introduced very soon – probably in 2022. However, at the moment, the IdM system is being implemented by the use of the so called "Qualified Electronic Signature". This is actually a digital equivalent of a handwritten signature. It ensures credibility and irrevocability of the signed electronic documents. The signed document remains signed no matter whether you store it on magnetic, optical or other media and whether you send it by an e-mail, or access it via the Internet. Signing by electronic signature means that a citizen or a legal entity:

- identifies him/her/itself as an author of the digital document;
- agrees with the contents of the document;
- protects the document from subsequent changes.

Qualified electronic signature is an electronic signature within the meaning of Art. 3, p. 12 of Regulation (EU) No 910/2014. "Qualified Electronic Signature" means an advanced electronic signature, created by a qualified electronic signature creation device, based on a Qualified Electronic Signature Certificate. "Qualified Electronic Signature Certificate" means an electronic signature certificate issued by a Qualified Certification Services Provider.

The Qualified Electronic Signature Certificate contains information about the Signatory (Holder) and/or the legal entity with which it is associated, such as:

- Name of citizen / name of company or organization
- Personal No (or Personal Identification Number of a Foreigner) – only for persons/citizens
- Unified Identification Code (UIC) – only for legal entities / organizations
- Address

[2] http://firmaelectronica.gob.es/Home/en/Ciudadanos/DNI-Electronico.html

- Other data

This e-ID solution is not free, and its subscription fee depends on its duration. It can be used by citizens in order to access various services of banks and public administrations. Citizens of Peshtera Municipality can take advantage of digital services of the municipality only if they have such e-signature.

4.1.5 Denmark

Since 2010 they are using a digital system called NemID, that is used for online authentication. NemID either requires that the citizen has installed the app, Nøgleapp, that generates the codes that are used for the authentication or that the citizen still uses NemID in paperform, Nøglekort.

NemID is used for such things as banking, access to public databases, as a public log-in, etc. Every citizen has a unique access that is validated with the citizen's national identification number, CPR-number. When the user log on, firstly enter their user ID and password and then code from the code card (or Nøgleapp).

NemID works as a multi-factor authenticator, that both allows the user to identify with several public documents, to sign documents digitally and to verify that changes has been made by the legal owner.

Further, the NemID solution is also available for companies, and works basically in the same way as the citizen solution. While NemID for citizens is free of charge, companies must pay a relatively small amount of money in order to use the solution.

4.2 Other interesting cases: France and Estonia

4.2.1 France

France is developing a holistic identification and authentication system, called France Connect, to allow citizens, businesses and civil servants to access online services and to control how their data are exchanged. These Service Providers can be the public central administration, agencies for social services, local and regional authorities, but also private organizations such as industries, business innovators or non-profit operators.

Nowadays, French citizens who use online services, as the ones provided by the Ministry of Economics, Finance and Industry (DGFiP) or the Post Office (La Poste), are asked to create a personal account for each service. The role of France Connect is to federate these separate online identities and make them secure.

The information of the user is collected by the ID Provider and then forwarded to France Connect, which creates a "Pivot ID" (Identité Pivot) that will be sent by France Connect to each Service Provider every time the user requests it.

Moreover, in a second step of the project, France has also the aim to exchange data between administrations. This means that administrations that have signed up to France Connect, with previous authorization by the user, will be able to transmit all the information needed for a particular administrative procedure without sending unnecessary data. In these cases, France Connect acts as a trusted intermediary, validating the user's ID before any data is exchanged[3].

4.2.2 Estonia

Estonia has developed an innovative and cutting-edge IdM system that, this is the main peculiarity, allows also foreigners to obtain the e-Estonia card. What Estonia did is not only an IdM but also an extension of some rights of citizenship to foreign people, asking for the Estonian E-citizenship.

This allows them to benefit from some services that Estonian institutions provide to e-citizens, mainly regarding business issues. Therefore, the case of e-Estonia is ground-breaking both for the technical effectiveness of the solution implemented, and for the fact that it enables new type of residency and citizenship in the digital world.

As Sarav & Kerikmäe (2016) state:

"Apparently, the country is aspiring to become as renowned for its e-services as Switzerland is for its banks.17 Accordingly, the Digital Agenda 2020 for Estonia puts down the intent to retain the image of a tech-savvy

[3] https://joinup.ec.europa.eu/document/france-connect-id-federation-system-simplify-administrative-processes

country, whereas the concept of e-residency is emphasised as being one of the key factors in achieving that goal.18 However, issuing digital identities is not only about Estonia's reputation, but it also has a multifaceted effect. In addition to marketing Estonian e-services, the legal foundation for the e residency—the Identity Documents Act of Estonia—introduces as the objective of the issuing of e-residencies the advancement of Estonian "economy, science, education or culture by providing access to e-services with the Estonian digital document"19; and thirdly, as laid down by the Concept, the e-residency programme further ought to contribute to the enhancement of the policy of the Estonian compatriots programme supporting Estonians and Estonian culture abroad.

The e-Identity for Estonian "real" citizens obviously allows more services than the e-residency. Sarav & Kerikmäe also point out various legal and privacy issues of e-residency in respect to European Regulation and Estonian regulation itself.

In November 2015, Estonia started a collaboration with Bitnation to integrate the E-ID with the Blockchain, in order to bypass traditional, national governance systems. This would allow it to manage authentication and identification without passing for intermediaries as governments or banks, as for Bitcoin transactions. In blockchain based identity management systems identity is established using a distributed ledger on a global open-source platform, rather than using traditional authentication sources like government records and authentication intermediaries like banks, for example. As the joint press statement points out, "via the international Bitnation Public Notary, e-Residents, regardless of where they live or do business, will be able to notarize their marriages, birth certificates, business contracts, and much more on the blockchain." (Sullivan & Burger, 2017)

Estonia is the first State nation starting a project to integrate distributed ledger (DL) technologies, as Blockchain, with Identity Management Systems. However, this solution could gain increasing attention since, as many scholars claim, DLs will probably become a disruptive technology for IdM. In the next chapter we discuss B-Based IdM systems.

5 B-Based IdM System

Since the explosion of interest toward the distributed ledgers (DL) in the last ten years - one for all Bitcoin -, also the IdM discussion nowadays includes distributed ledgers. Therefore, in line with the aim of the IMPULSE project, in this chapter we discuss the blockchain-based identity management systems, their benefits and shortcomings. First, we give a brief overlook on what a DL is, then we discuss Blockchain (BC) specifically. Moreover, we introduce the possible applications of BC in IdM, the main benefits of applying this technology and its shortcomings.

5.1 Distributed Ledger and Blockchain

Extensive attention has been given in recent years to distributed ledgers, as the Blockchain, mainly for the unforeseen success of Bitcoin, the digital coin created by Satoshi Nakamoto in 2008.

Bitcoin, as Ethereum or other types of cryptocurrencies, relies on a similar infrastructure: a ledger (as a storyboard of all the transactions made) is replicated on all the nodes of the network. Every new transaction, to be valid, must be registered in the distributed ledger. The registration, and therefore validation, of a new transaction is made by consensus between the nodes. The possibility to become a node of this network, and therefore to have a copy of the ledger, might be permissioned (only authorized nodes from a central authority) or permissionless (anyone can have a copy and therefore validate transactions).

Then, distributed ledgers are a decentralized peer-to-peer system that, without a central authority, validate transactions.

In the domain of distributed ledger, the Blockchain (BC) is today the most widely used technology. Specifically, is a chain of records, the "blocks", that increasingly grows every transaction. To ensure the validity of the new blocks, every block contains the cryptographic hash of the previous one: in this way, and with other types of security checks as the timestamp, the chain is secured: once a transaction is registered, no one in no way can modify the chain.

Here reported the explanation given by Lim et al. (2018) of the hash functioning:

Each block contains a record of transaction and is cryptographically hashed. A hash function takes in input value and creates an output value deterministic of the input value. Every input has a determined output. The process of applying the hash function to any data is called hashing and the output is called the hash value or simply the hash. One critical characteristic of a secure hash function is that it is only one way. This means that given the hash, it is impossible to determine what the input was. Hashing is extensively used with Blockchains. For example, a process of hashing public keys derives addresses on a Blockchain. An Ethereum account is computed by hashing a public key with keccak-256.

This brings us to the first important benefit of BC: it is tamper resistant.

Blockchain generally requires a "proof of work" in order to create a new block: this ensures that some computational effort was made to create the new block. The computational effort also serves to ensure the validity of the chain's new blocks, namely, to verify the hashes.

As we will discuss later in details, participants to the peer-to-peer networks (and the transactions themself) do not need to be "trusted" by the other peers. In fact, the trust in the actors is not needed since the cryptographic systems put in place by the Blockchain already ensure the trustability of the transactions/information registered in the chain. Since the system itself ensures trustability, actors of the chain can be anonymous. Moreover, every registered transaction is accessible to every node of the chain, therefore it is auditable.

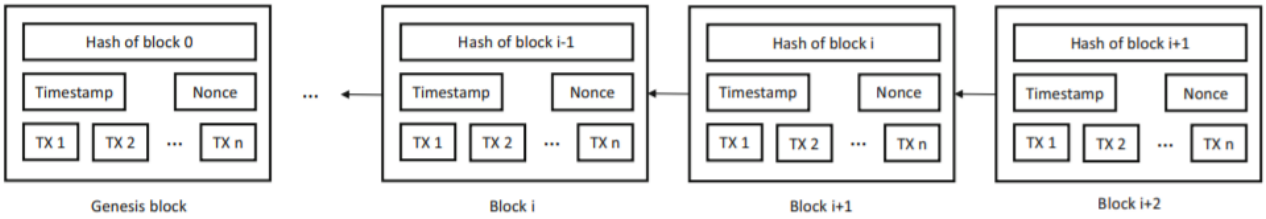

Figure 1 - The Structure of a Blockchain's Block, from Zheng (et al., 2018)

We can therefore summarize the main concepts of Blockchain in the following table.

Table 1 - Main Relevant Concepts of Blockchain

Decentralization	There is no central authority managing the information storage, accessibility, modifiability etc.
Immutability	Once a transaction is registered, it cannot be altered – BC is therefore tamper-resistant
Permission	BC might be permissioned or permissionless
Consensus	The validation and registration of new information/transaction is done through the consensus of the nodes

5.2 B-Based IdM System

All the benefits that we discussed above are key elements for an effective IdM system. The decentralization (ensured by the distributed ledgers) guarantees that the identity, the credentials etc. will not be deleted or altered in a malicious way, it is indelible as the blockchain itself (Augot et al., 2017). The fact that it is tamper-resistant ensures that past information transactions will not be altered, the permissioned/less nature of BC enables a choice between the two. Most important, the consensus is based on an algorithm assuring the validity of every transaction, whether is based on proof of work (Vukolić, 2016), proof of stake (Li et al., 2017) or on the Byzantine Fault Tolerance system (Gramoli, 2020). This means, but as we will see it is debated, that no trust is required in a B-Based IdM system. This, as many claim (Dunphy & Petitcolas, 2018; Zwitter et al., 2020), would be the most important benefit of applying DL technologies to IdM: in fact, as we thoroughly discussed above, trust between the IPs is the main issue affecting federated identity management. The application of BC to the IdM system is quite novel and only in the last few years we have seen a proliferation of tentative applications of this technology (see the table below).

5.2.1 Types of B-Based IdM system

What types of B-Based IdM are today available? The literature in this topic is today quite magmatic, due to the increasing hype of the topic and the totally missing standards (even from a linguistic point of view). As claimed by Dunphy & Petitcolas (2018) most "fall in two categories:

- Self-sovereign identity is owned and controlled by a user without the need to rely on any external administrative authority and without the possibility that this identity can be taken away. This can be enabled by an ecosystem that facilitates the acquisition and recording of attributes, and the propagation of trust among entities leveraging such identities. Examples include Sovrin, uPort, and OneName.
- Decentralized trusted identity is provided by a proprietary service that performs identity proofing of users based on existing trusted credentials (for instance, a passport) and records identity attestations on a DLT for later validation by third parties. Examples include ShoCard, BitID, ID.me, and IDchainZ."

5.2.2 Self-Sovereign IdM

Some space must be given to a completely new approach to IdM and discuss in detail its implications. The term ‘‘Self-Sovereign Identity’’ (SSI) is new-born in the realm of IdM and identifies an IdM system based on BC with peculiar characteristics. At the core of SSI is the fact that users are in full control of their online identities. The World Wide Web Consortium (W3C) working group on verifiable claims states that self-sovereign identity systems are built by independent users from Service Providers (W3C, 2018). This highlights the contrast to current identity management which either relies on several large identity providers such as Facebook (Facebook Connect) and Google (Google Sign-In) or the user has to create new digital identities at each individual service provider (Mühle et al., 2018).

This new type of approach shifts IdM systems from a Provider-centric model, where identity was bound with the service provider, to a user-centric model (Augot et al., 2017). The identity is freed from any provider because it is stored, accessed and authenticated through the chain. As Cameron et al. (2008) state: “The core requirement for user control is that the flow of information from Claims Providers to Relying Parties only happens at the request of the user”. The blockchain replaces the registration, verification, and authorization authority that is typical of for example SSO identity management.

Mühle et al. (2018) explain how the process works in SSIdMS: “The actual identity claim is stored in the user-controlled storage, typically off-chain for privacy considerations. The relying party, also called claim-verifier, can then compare the publicly available identifier with the identifier in the claim that has been handed to him by the user. After authenticating the user with the authentication method presented in the public blockchain, the claim itself can be verified and accepted or rejected by the relying party.”

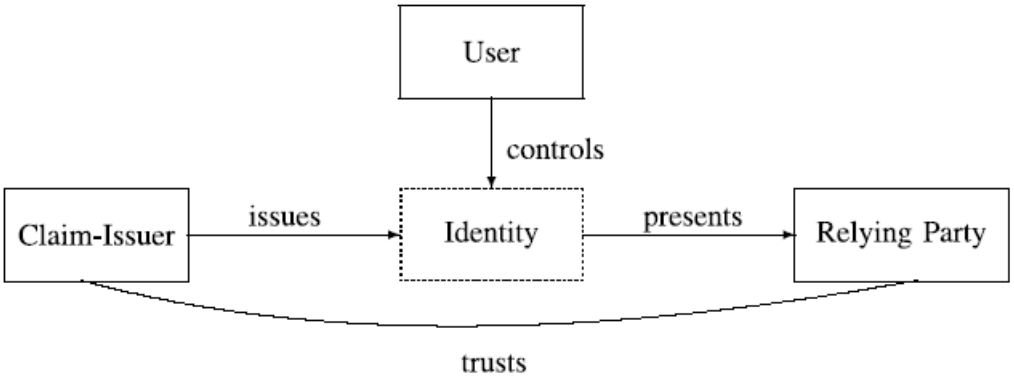

Figure 2 - SSIdMS Typical Functioning

Therefore, in SSIdMS, the users have full control on their identities and how credentials and private information are shared with Relying Parties. This approach completely overcomes the privacy issues concerning all the other IdM. This is the opinion of the Sovrin Foundation’s white paper (Tobin & Reed, 2016), where SSI is described as the natural and logical prosecution of the work on a more user-centric identity management.

Some examples of SSIdMS are UPort, ShoCard and Sovrin. Here we will mention some details of the last one, since it has been in the SSI ecosystem for a few years and meets the basic principles on this field. Sovrin is an open-source permissioned DL where only trusted institutions – the *steward* – can become a node of the chain. Trusted institutions might be universities, states, banks etc.

Sovrin’s aim is to equip users with the full control over their identities, disclosing only the information they want to the Relying Party. To manage the digital identity users will use an app where they are able to authorize the information disclosure.

In the following figure we report the core concepts of Sovrin’s SSIdMS from the white paper (Tobin & Reed, 2016):

Table 2 - Sovrin White Paper's Fundamental Concepts

Security The identity information must be kept secure	Controllability the user must be in control of who can see and access their data	Portability the user must be able to use their data wherever they want and not be tied to a single provider
Protection	Existence	Interoperability
Persistence	Persistence	Transparency
Minimisation	Control	Access
	Consent	

Concluding on SSI, a good summary of what an SSI is, was given by Pon et al. (2016) "Open, decentralized systems enable individuals to fully own and manage their own identities, leading to the idea of "self-sovereign" identity systems. These systems use combinations of distributed ledger and encryption technology to create immutable identity records. The individual creates an identity "container" that allows them to accept attributes or credentials from any number of organizations, including the state, in a networked ecosystem that is open to any organization to participate (e.g., to issue credentials)."

Summarizing, SSIdMS brings the following conditions to IdM systems:

- A user can operate with or without state credentials
- Individual owns and manages the identity container
- Identity is non-revocable by state or private firms
- Typically enables granular sharing of credentials: user can decide what credentials to disclose to a Relying Party.

5.2.3 Existing implemented B-Based IdM systems

Aiming to be aligned with European regulations, we find ESSIF IdM, part of the European Blockchain Services Infrastructure (EBSI). ESSIF is a generic and interoperable Self-Sovereign Identity (SSI) Framework which defines the necessary specifications and builds the supporting services and capabilities that will allow citizens to create, control, and use their own digital identity (including identification, authentication, and other types of identity related information) without having to rely on a single, centralised authority. ESSIF is a part of a broader ecosystem on decentralised identity and will interact with other systems and platforms of public and private organisations.
As such, ESSIF will not only facilitate all types of digital interactions between different public and private sector parties, but also processes between citizens and public administrations or private parties across all EU MS. ESSIF aims to be compliant with GDPR as well as aligned with eIDAS to ensure that ESSIF can benefit from existing legal frameworks, allowing ESSIF to provide digital evidence providing support to legal enforceability. All this in alignment with the eIDAS revision whose aim is "to improve its effectiveness, extend its benefits to the private sector, and promote trusted digital identities for all Europeans, and create a secure and interoperable European Digital Identity which gives citizens control".
Other IdM implementations can be found in the literature.
Without entering into details of all the different kinds of B-Based IdM systems, in the next table we show the list of existing implementations proposed by Lim et al. (2018). This list gives information on the type of Blockchain used, the type of network, if the solution described is an identity management system or, for example, only an authentication system, and the current implementation status.

Table 3 - List of the existing B-Based IdM systems

Solution	Description	Propose type	Blockchain	Network	ID Mgmt	Auth	Status
Sovrin [11]	Decentralized global public utility	Non-profit foundation	Hyperledger Indy	Public Permissioned	Yes	No	Completed (September 2016)

	for self- sovereign identity						
Waypoint [28]	Decentralized multi- factor authentication system	Company	Ethereum	Private	No	Yes	Beta stage (October 2017)
Bloom [38]	Blockchain project for credit scoring and identity management	Open source	Hyperledger	Permissioned	Yes	No	Completed (January 2018)
BlockStack [31, 33]	Decentralized services for naming/DNS, identity, authentication and storage	Start-up	Ethereum	Private	Yes	Yes	Completed (October 2017)
ShoCard [39]	Identity platform to protect consumer privacy	Start-up	Ethereum	Public	Yes	No	Completed (December 2017)
Uport [40]	Identity management	Company	Ethereum	Public/Private	Yes	No	Completed (October 2016)
I/O Digital [41]	Identity management based on the Blockchain	Start-up	Ethereum	Private	Yes	No	Completed (January 2018)
BlockAuth [42]	Developing identity registrar base on the Blockchain	Start-up	Ethereum	Permission-less	Yes	No	Completed (July 2014)
UniquID [43]	Identity and access management of connected things	Open source	Ethereum	Permission-less	Yes	No	Beta Stage (June 2016)
Jolocom [44]	Applications for user to own their personal digital identity	Start-up	Ethereum	Public/Private	Yes	No	Development stage (February 2018)
Cambridge Blockchain [45]	Identity Blockchain	Start-up	Ethereum	Permission-less	Yes	No	Alpha Stage (June 2017)
KYC.LEGAL [46]	User identification and verification to prevent fraud	Company	Ethereum	Permission-less	Yes	No	Completed (February 2018)
CertCoin [47]	NameCoin based decentralized authentication system	Open source	Hyperledger	Permissioned	No	Yes	Completed (May 2014)

Authenteq [49]	Identity verification platform that uses a facial recognition algorithm to create a digital identity on a blockchain	Company	Ethereum	Permission-less	Yes	No	Completed (August 2014)

5.3 B-Based IdM System: Benefits

After having discussed the landscape of B-Based IdM, we briefly summarize the main benefits of the application of DL technologies to IdM, and the possible shortcomings.

5.3.1 Trustlessness

The use of the Blockchain might definitively resolve the issue of trust in IdM. As we discussed, this is an outstanding problem for federated IdM - if intended between IPs and RPs - and also between the Identity Provider and the user. In this second case the existence and the reliability of online identities relies on the trust the user gives to the IP, since the first cannot fully control her identity.

Blockchain instead does not require trust, since trustworthiness is defined as relying on an actor ability, benevolence, and integrity (Mayer et al., 1995). These concepts do not apply to algorithms but to intermediaries, figures that the BC completely overcomes. This element is furtherly stressed in SSIdMS since the user-centric model ensures that all the agency on the identity is in the hands of the user.

As we showed, the application of DL technologies is particularly useful in the case of a federated environment, where trustability is the main issue. In centralized IdM systems there seems to be no purpose in applying this kind of technology since the main benefits, trustability, would not be useful.

5.3.2 Immutability

Blockchain is tamper-resistant and cannot be modified without a general consensus of the nodes. Therefore unwanted or illegal modification of the chain, and therefore of the identities, is highly unlikely.

On the other hand, centralized or non-B-Based federated environments are at constant risk of being violated with the resulting systemic consequences for all the other IPs, who cannot control each other's systems.

Tamper-resistance is incredibly important for information transactions such as banking or State IdM, where legally relevant data are exchanged.

5.3.3 Transparency and Interoperability

The chain where data are stored, given a public chain, is transparent to every node (and even to every user) and therefore fully auditable. This property increases reliability of B-Based IdM systems and also increases users' trust. Moreover, the data stored in the chain are highly interoperable between multiple different services and Relying Parties. Easy interoperability will supposedly enhance the adoption of this technology and reduce the technical costs.

5.3.4 User centeredness

This last benefit highly depends on how the B-Based IdM system is designed. If a Self-Sovereign approach is adopted, users will have the full control of the use of their identities.

5.4 B-Based IdM System: Shortcomings

This next section will outline the main concerns and shortcomings of B-Based IdM systems, as today conceived. We will divide them into three major groups of security and privacy, environment and user awareness.

5.4.1 Security and Privacy

That Blockchain is tamper-resistant is not totally true. While it is surely harder to illegally manipulate a blockchain than a simple log or registry stored in an private database, also BC can undergo cyber attacks that can compromise the reliability of the data stored in the chain and, most of all, of the consensus mechanism. Although it is not the scope of this deliverable to enter into very technical details of BC security, we must at

least cite the 51% threat. This is a cyber attack where a group of hackers gain 51% of the computing power or the hash rate of a chain and are therefore able to "legitimately" add new blocks to the chain. Since transactions generally await a certain amount of time before being confirmed, a hacker obtaining the 51% can confirm fraudulent transactions (Ye et al., 2018). This is even more dangerous since when a transaction is confirmed it cannot be reverted, or it would cause a fatal flow inside the chain.

This problem clearly affects trustability. Therefore, while BC do not have the characteristics of trustworthiness highlighted by (Mayer et al., 1995), it has another type of trust issues: those relying on the security and reliability of the consensus mechanism, be it the proof of work, proof of stake or the Byzantine fault-tolerant mechanism (Auinger & Riedl, 2018).

Moreover, since the BC is open and readable by everyone (at least public BC), privacy issues are at stake.

Users' information transactions, even if pseudonymized, might be traceable and then user privacy might be at risk (Ishmaev, 2020). As Dunphy & Petitcolas (2018) state:

"There is a tightening regulatory landscape for storing and processing personal data. For example, the GDPR grants end users new powers over personal data and places new obligations on data controllers and processors. This creates a challenge for the design of identity-focused immutable ledgers that reference personal data and that provide inherent transparency to data that they store."

5.4.2 Environmental issues

More and more awareness is growing on the environmental impact of Blockchain and, in general, of distributed ledgers. Most of all, Proof of Work (PoW) requires enormous amounts of energy in order to guarantee the necessary computing power to mine new blocks (Vranken, 2017). On the other hand, much research is carried out nowadays to find a more environmentally friendly solution for the consensus mechanism (Roberto Leonardo et al., 2019).

There is a trade-off between security and use of resources: best security can be achieved in a big public blockchain with a PoW consensus algorithm, but many resources are wasted in this case; a bit less of security can be achieved in a permissioned blockchain, but it is still a lot, since the data would be replicated in every node and dishonest transactions would be seen and discarded.

5.4.3 User Awareness

User-centredness in design is certainly a step forward for technologies. Instead of putting corporate needs and benefits at the core of the design of the object (or the process) is the user herself that becomes the centre. This means increased usability, better communication and the empowerment of the user, that is now in the condition of choosing, for example, which data to share. On the other hand, this approach puts a lot of responsibilities on users' hands while discharging responsibility from the provider. These responsibilities include privacy options, security and (in SSI) the existence of the identity itself. In fact in SSI if the password is lost the identity is irremediably lost. With Dunphy's (Dunphy & Petitcolas, 2018) words:

"There appears to be a widespread assumption that users are equipped to conduct effective cryptographic key management and would intuitively understand the implications of referencing identity attributes in a DLT."

Identity Management Systems, even more if BC-based, are not intuitive technologies. Providers and designers cannot pretend from users to spend time in understanding very technical issues in order to correctly utilize IdM systems. When we refer to users at the centre of the design process, we should remember that this firstly involves accessible usability.

Therefore, the awareness, or the willingness to become aware, of users cannot give for granted or, as Dunphy states: "If It Isn't Usable, It Isn't Secure".

6 EU Regulatory and Standardization Framework

In this last chapter of the deliverable, we discuss the existing regulations and standards for Identity Management Systems and those specifically based on Distributed Ledger and Blockchain. As we will see, there seems to be a total lack of regulation on the specific point of conjunction of BC and IdM, while the two are already separately regulated on the European level. This lack should be furtherly addressed in order to ensure compliance.

A more extensive analysis of existing relevant standards will be performed in the D3.4 ("Standards and related impacts and implications") of IMPULSE. While this document (D3.1) tracks the EU framework of the legislative-regulatory aspects in a broad sense, combining aspects of regulation law and standardization on issues such as security, privacy and informed consent acquisition, the aim of D3.4 is to create a well-grounded documentation of the current technical standards related to the IMPULSE project, mainly to be used as framework for the co-creative design of IMPULSE and the piloting to ensure the compliance with the prior art.

6.1 The lack of regulation law and standardization

When looking at the legal and standardization framework on identity management based on blockchain, what immediately stands out is the nearly total lack of dedicated legislations and standards. On the side of the EU framework, there is nothing on B-Based IdM while on the identity management in general we find for example EIDAS (910/2014). On the standard side only one standard directly addresses B-Based IdM; we discuss it in the next sections. Other standards address IdM in general or distributed ledgers in general.

Therefore, what we underline in the first instance is the lack and therefore the urgent need of an EU regulation law and standardization on blockchain-based identity management systems.

6.2 Relevant regulation law framework

In this section we discuss the current relevant regulatory frameworks for B-Based identity management systems: GDPR applicability and EIDAS regulation on IdM.

The GDPR applicability discussion includes other frameworks, WP29 opinions and relevant regulation on Blockchain. For this last, the use of Blockchain is today mainly regulated for economic transactions (as cryptocurrencies) and therefore the actual regulations generally do not have relevant applications for IdM, where identities are stored and attributes are exchanged in the chain.

Finally, we make a brief introduction to the new proposal by the Europe Commission for a trusted and secure Digital Identity for all Europeans, published by the Commission on the 3rd of June 2021.

6.2.1 GDPR compliance of IdM systems based on blockchain

The GDPR compliance of IdM systems based on blockchain is debated. Nevertheless, limited scientific literature is facing up the issue systematically and, therefore, further understanding is crucial. Many scholars point out some difficulties for the blockchain in order to be compliant with the GDPR. Here we will list some of these open issues, mainly taken from Sim et al. (2019).

The most problematic point is the article 17 "*right to erasure*": the blockchain, in order to be tamper-resistant, is also immutable, and therefore does not allow information to be deleted. This is also highlighted by Hristov & Dimitrov (2018) as a backbone of blockchain GDPR compliance.

For the same reason the right of rectification (article 16) seems to be hardly implementable in B-Based identity management systems since no modification can be done to a block after it is added. If a block is modified, in fact, it would alter the entire chain since the hash of the following block would not point anymore to the preceding one.

Again for the same reason, it is not possible to revoke consent (article 7).

The definition of the data controllers (article 4) is hard to be done since the chain is replicated in every register, as peer-to-peer technologies require.

On the side of data minimization, the blockchain goes against Article 25 since the data are not stored only between the participants involved in a transaction but replicated throughout the nodes.

Another urgent problem regards the anonymization/pseudonymization of personal data on the blockchain. GDPR does not apply to anonymized data but does apply to pseudonymized data.

The problem is therefore to understand if hash identifiers on the blockchain should be considered anonymized or pseudonymized data. WP29 and the French Data Protection Authority (CNIL) seem to agree on the fact that these data are pseudonymized and therefore GDPR applies:

"*the very architecture of blockchains means that these identifiers are always visible, as they are essential for its proper functioning. The CNIL EBSI GDPR Assessment 14 therefore considers that this data cannot be further minimised and that their retention periods are, by essence, in line with the blockchain's duration of existence*" (CNIL)[4]

While WP29 states that "*If the range of input values the hash function are known they can be replayed through the hash function in order to derive the correct value for a particular record. For instance, if a dataset was pseudonymised by hashing the national identifcation number, then this can be derived simply by hashing all possible input values and comparing the result with those values in the dataset*." (WP29, 2014)

In the end, The EU Blockchain Observatory and Forum (2018) states that the problem of the pseudonymity or anonymity of hashing is still a grey area:

"*Hashing is at the heart of many of the most important properties of blockchains, providing much of the 'magic' of decentralisation. This question of whether hashed personal data should be considered personal data is hotly debated at present, and unfortunately much of this debate relies on rather complex details. Also, it should be kept in mind that not all hashing algorithms are equal and that the most advanced algorithms should always be preferred. As stated above, these issues have not been conclusively settled by the data protection authorities, the edpb or in court. At this stage, a desirable outcome of the debate regarding the status of hashed personal data could be: it depends. the gist of it could potentially come down to the question of identifying potential reversibility or linkability risks*".

Moreover, Self-Sovereign IdM, Kondova & Erbguth (2020) 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, a data protection impact analysis (DPIA) will be required.*"

Finally, another issue involving personal data pursuant to the GDPR is the linkability risk (The EU Blockchain Observatory and Forum, 2018):

"*Linkability risk, or the risk that it is possible to link encrypted data to an individual by examining patterns of usage or context, or by comparison to other pieces of information*".

6.2.2 eIDAS regulation

The eIDAS (electronic IDentification, Authentication and trust Services) regulation is a fundamental step to ensure trustable and reliable digital identities. Before this regulation, the standard for trusted authentication was constituted by cryptographic smart cards but the reduced user-friendliness and easiness of use prevented a massive diffusion of this technology. e-IDAS, on the other hand, abandons physical devices, such as smart cards, in order to ensure trusted identities and prefers other types of authentication.

The main aim of e-IDAS is to provide interoperability for European identity and signature verification. From e-IDAS a set of standards came out that now constitute a common framework in Europe for the authentication of e-signatures and e-identities. The electronic seal, in the e-IDAS regulation (ENISA, 2017), is defined as

4 https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data

"data in electronic form that attach or logically associate some other electronic data to ensure their origin and integrity" Advanced electronic signature should meet certain requirements:

- It provides unique identifying information that links it to its signatory
- The signatory has sole control of the data used to create the electronic signature
- It must be capable of identifying if the data accompanying the message has been tampered with after being signed. If the signed data has changed, the signature is marked invalid
- There is a certificate for electronic signature, electronic proof that confirms the identity of the signatory and links the electronic signature validation data to that person

Moreover, as reported by Dumortier (2017):

"*the eIDAS Regulation distinguishes between three assurance levels for electronic identification means issued under an electronic identification scheme: low, substantial and high. The distinction refers essentially to the degree of confidence in the claimed or asserted identity of a person. Each level is characterized by reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity. The lower this risk of misuse or alternation is, the higher the assurance level will be*".

On the compliance of blockchain in IdM with e-IDAS no topic-based literature seems to have been produced. At first sight, it appears that there is no reason to think that the integration of the blockchain in the already existing e-IDAS standards will bring issues or will end up being in contradiction with the regulation. In fact, as also Alimehaj et al. (2021) seem to support, the e-IDAS security and cryptographic requirements are not only met by the blockchain, but even overcome. In fact, Alimehaj et al. (2021) claim that the use of blockchain to store digital seals adds another layer of security to the actual technology and, moreover, it enables to sign with electronic signatures any type of object, if stored on a blockchain, while actual technologies only allow to sign and seal certain types of documents (e.g. PDF).

The next figure, from Alimehaj et al. (2021), summarizes the pros and cons of using the blockchain for digital seals and, therefore, digital identities.

Table 4 - Blockchain and e-IDAS Regulation

Digital seal	Digital seal with blockchain	Pros and cons
Digital seal appearance in the document	Same document and invisible digital seal after printing	Use digital seal with blockchain if its main intent to provide digital verification
Only PDF documents	All data formats	Usage of digital seal with blockchain has wider scope
Recognises only digital certificates in Adobe Approved Trust List	Works with private/public key	Use digital seal with blockchain when you trust to third party
Does not support parallel seal	Supports seal of the same document from entities in distance al the same time	Use digital seal with blockchain when you need signage from different parties as form example contract signing between different parts
Mistakes are allowed while a document with the digital seal can be deleted	A stored digital seal of the document in blockchain cannot be changed	Use digitai seal with blockchain when yoll need more transparency (example eVoting)
Digital seal can be verified Digital only by a receiver who has a document with a digital seal	Digital seal can be verified from all members in chain subscribed in Stream and possess an original document	Do not use digital seal with blockchain when you need only one part in exchanging document.
Faster process	Validation of transactions and redundancy takes more time	Do not use digital seal with blockchain when execution time is crucial for your app

As always, the immutability of the chain represents the most important issue also in the case of digital seals and signatures, but it does not seem to go against any part of e-IDAS.

Further analysis must be done on the compliance of B-Based IdM systems with e-IDAS regulation, given the urgent importance of digital signatures and certificates in identity management.

An eIDAS amendment proposal, which can be found here, presents the highest level of ambition and aims to regulate the provision of a highly secure personal digital identity wallet issued by Member States. As you can see in the "Regulation - COM(2021) 281" document and I quote: "this proposal expands the current eIDAS list of trust services with three new qualified trust services", one of them being the electronic ledgers. It also talks about attribute certificates.

The creation of a standard for B-Based IdM systems must take into consideration e-IDAS in order to make all the technical instruments compliant with this regulation.

6.2.3 The Europe Commission proposal for a trusted and secure European Digital Identity

The Commission on the 3rd of June proposed a framework for a European Digital Identity which will be available to all EU citizens, residents, and businesses in the EU. Citizens will be able to prove their identity and share electronic documents from their European Digital Identity wallets with the click of a button on their phone. They will be able to access online services with their national digital identification, which will be recognised throughout Europe. Very large platforms will be required to accept the use of European Digital Identity wallets upon request of the user, for example to prove their age. Use of the European Digital Identity wallet will always be at the choice of the user.

Under the new Regulation, Member States will offer citizens and businesses digital wallets that will be able to link their national digital identities with proof of other personal attributes (e.g. driving licence, diplomas, bank account). These wallets may be provided by public authorities or by private entities, provided they are recognised by a Member State.

The new European Digital Identity Wallets will enable all Europeans to access services online without having to use private identification methods or unnecessarily sharing personal data. With this solution they will have full control of the data they share.

The European Digital Identity will be:

1. Available to anyone who wants to use it: Any EU citizen, resident, and business in the Union who would like to make use of the European Digital Identity will be able to do so.
2. Widely useable: The European Digital Identity wallets will be useable widely as a way either to identify users or to prove certain personal attributes, for the purpose of access to public and private digital services across the Union.
3. Users in control of their data: The European Digital Identity wallets will enable people to choose which aspects of their identity, data and certificates they share with third parties, and to keep track of such sharing. User control ensures that only information that needs to be shared will be shared.

To make it a reality as soon as possible, the proposal is accompanied by a Recommendation. The Commission invites Member States to establish a common toolbox by September 2022 and to start the necessary preparatory work immediately. This toolbox should include the technical architecture, standards and guidelines for best practices.

6.3 Relevant standardization framework

This last section on standards provides an overview of the existing standards for IdM and Blockchain. As we show in the next passages, only one standard was found on B-Based IdM, we will briefly discuss it.The complete assessment of standards is part of T3.4 “Analysis of existing relevant standards, and related impacts and implications”, which is due to M24.

6.3.1 Keywords for standards search

- Blockchain & Identity Management
- Identity Management
- Blockchain

6.3.2 Search conducted on databases

- Formal standardization organizations (e.g. ISO)
- Informal standardization organizations and other initiatives (IETF, OASIS, W3C)

6.3.3 Standards on B-Based IdM

Relevant standards

- Amount of existing standards found for blockchain-based identity management: 1

Table 5 - Relevant Standards for B-Based IdM

Document identifier	Title	Origin
UNE 71307-1:2020	Digital Enabling Technologies. Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies. Part 1: Reference Framework	71 TECNOLOGÍAS HABILITADORAS DIGITALES (THD)

UNE 71307-1 defines a framework for decentralised identity management aimed to individuals and legal entities, which includes the description of a life cycle approach and the relationship of the main players participating in it, as well as the interrelationships between them.

Technical specifications of the digital identity itself and specifically those of the Spanish National Electronic Identity Document are outside the scope of this standard, since it is regulated based on its own legislation and technical standards. Likewise, this standard does not aim to define specifications that are currently within the scope of REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

6.3.4 Relevant organisations and technical committees

Relevant standards

- UNE[5]

The Spanish technical committee UNE CTN 71 - Digital Enabling Technologies, subcommittee SC 307; Blockchain and Distributed Ledger Technologies; prepared UNE 71307-1. It is the first part of a series planned on the topic of B-Based IdM. The IMPULSE project will exchange closely with UNE in order to support related standardization activities and to present the IMPULSE project (outcomes) to the relevant national (i.e. Spanish) and new European Committees on blockchain and identity management.

6.3.5 Standards on IdM

Relevant standards

- Amount of existing standards found for identity management: 57

Table 6 - Relevant Standards for IdM

Document identifier	Title	Origin
BASI/TR 03156-2.1 V1.1	Public Sector Identity Management in Conjunction with European Registers - Part 2: IT System Architecture and Processes Volume 1: Border Control Version 1.1	Federal Office for Information Security
CWA 15263:2005	Analysis of privacy protection technologies, privacy-enhancing technologies (PET), privacy management systems (PMS) and identity management systems (IMS), the drivers thereof and the need for standardization	

[5] https://revista.une.org/30/ctn-71-tecnologias-habilitadoras-digitales.html

UNE 71307-1:2020	Digital Enabling Technologies. Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies. Part 1: Reference Framework	71 TECNOLOGÍAS HABILITADORAS DIGITALES (THD)
ETSI TS 124175 V 16.0.0	Universal Mobile Telecommunications System (UMTS) - LTE - 5G - Management Object (MO) for multi-device and multi-identity in the IP Multimedia Subsystem (IMS) (3GPP TS 24.175 version 16.0.0 Release 16)	ETSI/3GPP CT 1 MM/CC/SM [lu]
ETSI TS 124382 V 13.3.0	LTE - Mission Critical Push To Talk (MCPTT) identity management - Protocol specification (3GPP TS 24.382 version 13.3.0 Release 13)	ETSI/3GPP CT 1 MM/CC/SM [lu]
ETSI TS 124482 V 16.0.0	LTE - Mission Critical Services (MCS) identity management - Protocol specification (3GPP TS 24.482 version 16.0.0 Release 16)	ETSI/3GPP CT 1 MM/CC/SM [lu]
ETSI TS 124547 V 16.2.0	5G - Identity management - Service Enabler Architecture Layer for Verticals (SEAL) - Protocol specification (3GPP TS 24.547 version 16.2.0 Release 16)	ETSI/3GPP SA 3 Security
ETSI TR 133924 V 16.0.0	Digital cellular telecommunications system (Phase 2+) (GSM) - Universal Mobile Telecommunications System (UMTS) - LTE - Identity management and 3GPP security interworking - Identity management and Generic Authentication Architecture (GAA) interworking (3GPP TR 33.924 version 16.0.0 Release 16)	ETSI/INS
ETSI GS INS 001 V 1.1.1	Identity and access management for Networks and Services - IdM Interoperability between Operators or ISPs with Enterprise	ETSI/INS
ETSI GS INS 002 V 1.1.1	Identity and Access Management for Networks and Services Distributed Access Control for Telecommunications Use Cases and Requirements	ETSI/INS
ETSI GS INS 003 V 1.1.1	Identity and access management for Networks and Services - Distributed User Profile Management - Using Network Operator as Identity Broker	ETSI/INS
ETSI GS INS 004 V 1.1.1	Identity and access management for Networks and Services - Dynamic federation negotiation and trust management in IdM systems	ETSI/INS
ETSI GS INS 005 V 1.1.1	Identity and access management for Networks and Services - Requirements of an Enforcement Framework in a Distributed Environment	ETSI/INS
ETSI GS INS 006 V 1.1.1	Identity and access management for Networks and Services - Study to Identify the need for a Global, Distributed Discovery Mechanism	ETSI/INS

ETSI GS INS 008 V 1.1.1	Identity and access management for Networks and Services (INS) - Distributed access control enforcement framework - Architecture	ETSI/INS
ETSI GS INS 009 V 1.1.1	Identity and access management for Networks and Services (INS) - Security and privacy requirements for collaborative cross domain network monitoring	ETSI/INS
ETSI GS INS 010 V 1.1.1	Identity and access management for Networks and Services - Requirements of a global distributed discovery mechanism of identifiers, providers and capabilities	The Internet Engineering Task Force (IETF)
IETF RFC 7643	System for Cross-domain Identity Management: Core Schema	The Internet Engineering Task Force (IETF)
IETF RFC 7644	System for Cross-domain Identity Management: Protocol	The Internet Engineering Task Force (IETF)
IETF RFC 8224	Authenticated Identity Management in the Session Initiation Protocol (SIP)	ISO/IEC JTC 1/SC 27 IT Security techniques
ISO/IEC 11770-4 AMD 1	Information technology - Security techniques - Key management - Part 4: Mechanisms based on weak secrets - Amendment 1: Unbalanced Password-Authenticated Key Agreement with Identity-Based Cryptosystems (UPAKA-IBC)	ISO/IEC JTC 1/SC 29 Coding of audio, picture, multimedia and hypermedia information
ISO/IEC 23000-21	Information technology - Multimedia application format (MPEG-A) - Part 21: Visual identity management application format	ISO/IEC JTC 1/SC 29 Coding of audio, picture, multimedia and hypermedia information
ISO/IEC 23000-21 DAM 1	Information technology - Multimedia application format (MPEG-A) - Part 21: Visual identity management application format - Amendment 1: Conformance and reference software	ISO/IEC JTC 1 ISO/IEC Joint Technical Commitee for Information Technology
ISO/IEC 24760-1	IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts	ISO/IEC JTC 1/SC 27 IT Security techniques
ISO/IEC 24760-2	Information technology - Security techniques - A framework for identity management - Part 2: Reference architecture and requirements	ISO/IEC JTC 1/SC 27 IT Security techniques
ISO/IEC 24760-3	Information technology - Security techniques - A framework for identity management - Part 3: Practice	ISO/IEC JTC 1/SC 37 Biometrics
ISO/IEC TR 29144	Information technology - Biometrics - The use of biometric technology in commercial Identity Management applications and processes	International Telecommunication Union
ITU-T X Supplement 7*ITU-T X.1250 Series Supplement 7	ITU-T X.1250 series - Supplement on overview of identity management in the context of cybersecurity	International Telecommunication Union
ITU-T X.1250	Baseline capabilities for enhanced global identity management and interoperability	International Telecommunication Union

ITU-T X.1252	Baseline identity management terms and definitions	International Telecommunication Union
ITU-T X.1253	Security guidelines for identity management systems	International Telecommunication Union
ITU-T X.1255	Framework for discovery of identity management information	International Telecommunication Union
ITU-T X.1257	Identity and access management taxonomy	International Telecommunication Union
ITU-T X.1403	Security guidelines for using distributed ledger technology for decentralized identity management	International Telecommunication Union
ITU-T Y Supplement 12	ITU-T Y.2720 - Supplement 8 on NGN identity management mechanisms	International Telecommunication Union
ITU-T Y.2720	NGN identity management framework	International Telecommunication Union
ITU-T Y.2721	NGN identity management requirements and use cases	International Telecommunication Union
ITU-T Y.2722	NGN identity management mechanisms	International Telecommunication Union
ANSI/ATIS 1000035	Next Generation Network (NGN) Identity Management (IdM) Framework	American National Standards Institute (ANSI)
ANSI/ATIS 1000045	ATIS Identity Management: Mechanisms and Procedures Standard	American National Standards Institute (ANSI)
ANSI/INCITS/ISO/IEC 11770-4 AMD 1	Information technology - Security techniques - Key management - Part 4: Mechanisms based on weak secrets - Amendment 1: Unbalanced Password-Authenticated Key Agreement with Identity-Based Cryptosystems (UPAKA-IBC)	American National Standards Institute (ANSI)
NISTIR 7284	Personal Identity Verification Card Management Report	NIST National Institute of Standards and Technology
NISTIR 8014	Considerations for Identity Management in Public Safety Mobile Networks	NIST National Institute of Standards and Technology
NIST SP 800-63B	Digital Identity Guidelines: Authentication and Lifecycle Management	NIST National Institute of Standards and Technology
NIST SP 1800-2	Identity and Access Management for Electric Utilities	NIST National Institute of Standards and Technology
SATR 29144:2016	Information technology - Biometrics - The use of biometric technology in commercial Identity Management applications and processes	SOUTH AFRICAN BUREAU OF STANDARDS
[trust-el-framework-v1.0]	Electronic Identity Credential Trust Elevation Framework Version 1.0	OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC
[Trust-El-Protocol-v1.0]	Authentication Step-Up Protocol and Metadata Version 1.0	OASIS Electronic Identity Credential Trust Elevation

		Methods (Trust Elevation) TC
[PKCS11-Base-v3.0]	PKCS #11 Cryptographic Token Interface Base Specification Version 3.0	OASIS PKCS 11 TC
[PKCS11-Profiles-v3.0]	PKCS #11 Cryptographic Token Interface Profiles Version 3.0	OASIS PKCS 11 TC
[PKCS11-Current-v3.0]	PKCS #11 Cryptographic Token Interface Current Mechanisms Specification Version 3.0	OASIS PKCS 11 TC
[PKCS11-Historical-v3.0]	PKCS #11 Cryptographic Token Interface Historical Mechanisms Specification Version 3.0	OASIS PKCS 11 TC
Verifiable Claims Use Cases 1.0	Final Community Group Report 01 May 2017	W3C
Verifiable Claims Data Model and Representations 1.0	Final Community Group Report 01 May 2017	W3C
Decentralized Identifiers (DIDs) v0.13 **Data Model and Syntaxes**	Final Community Group Report 10 August 2019	W3C

Relevant organisations and technical committees

Relevant organisations and technical committees on international level

- IETF[6]
- ISO/IEC
- ISO/IEC JTC 1/SC 27 IT Security techniques[7]
- ISO/IEC JTC 1/SC 29 Coding of audio, picture, multimedia and hypermedia information[8]
- ISO/IEC JTC 1/SC 37 Biometrics[9]
- ITU
- OASIS
- OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC[10]
- OASIS PKCS 11 TC[11]
- W3C[12]

Relevant organisations and technical committees on European level

- ETSI
- ETSI/INS
- ETSI/3GPP[13]

[6] https://www.ietf.org/
[7] https://www.iso.org/committee/45306.html
[8] https://www.iso.org/committee/45316.html
[9] https://www.iso.org/committee/313770.html
[10] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=trust-el
[11] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pkcs11
[12] https://www.w3.org/
[13] https://www.etsi.org/technologies/3gpp-telecom-management

7 Conclusion

This deliverable highlighted the open issues regarding b-based IdM systems. As we discussed above, the main open issues to be addressed are:

1) The connection between user experience, design and security.
2) The trustlessness or the trustworthiness of the blockchain in IdM.
3) The compliance of b-based IdM systems with GDPR, especially regarding the right to be forgotten (article 17) and the issue of anonymity and pseudonymization (article 32).
4) The lack of a shared and recognized standard on b-based IdM systems

On this last point, the IMPULSE project aims to develop the first common and shared standards framework for b-based IdM systems. Against this backdrop, we started developing a collaboration with the standard agency UNE, the one who proposed a preliminary document on a standard for b-based IdM systems, as discussed in section 6.3.3.

References

- Alimehaj, V., Halili, A., Dervishi, R., Neziri, V., & Rexha, B. (2021). Analysing and comparing the digital seal according to eIDAS regulation with and without blockchain technology. *International Journal of Information and Computer Security*, *14*(2), 171. https://doi.org/10.1504/IJICS.2021.113174
- Augot, D., Chabanne, H., Chenevier, T., George, W., & Lambert, L. (2017). A user-centric system for verified identities on the bitcoin blockchain. In J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, & J. Herrera-Joancomartí (Eds.), *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 10436 LNCS* (pp. 390–407). Springer International Publishing. https://doi.org/10.1007/978-3-319-67816-0_22
- Auinger, A., & Riedl, R. (2018). Blockchain and trust: Refuting some widely-held misconceptions. *International Conference on Information Systems 2018, ICIS 2018*, *December*.
- Bazarhanova, A., & Smolander, K. (2020). The Review of Non-Technical Assumptions in Digital Identity Architectures. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, *3*, 6408–6417. https://doi.org/10.24251/hicss.2020.785
- Bertino, E., & Takahashi, K. (2010). *Identity management: Concepts, technologies, and systems*. Artech House.
- Cameron, K., Posch, R., & Rannenberg, K. (2008). *A User-Centric Identity Metasystem*. https://www.identityblog.com/wp-content/images/2009/06/UserCentricIdentityMetasystem.pdf
- Casassa, M., Bramhall, P., & Pato, J. (2003). *On Adaptive Identity Management: The Next Generation of Identity Management Technologies*.
- Chadwick, D. W. (2009). Federated identity management. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 5705 LNCS* (pp. 96–120). https://doi.org/10.1007/978-3-642-03829-7_3
- Clauß, S., & Köhntopp, M. (2001). Identity management and its support of multilateral security. *Computer Networks*, *37*(2), 205–219. https://doi.org/10.1016/S1389-1286(01)00217-1
- Dhamija, R., & Dusseault, L. (2008). The seven flaws of identity management: Usability and security challenges. *IEEE Security and Privacy*, *6*(2), 24–29. https://doi.org/10.1109/MSP.2008.49
- Dumortier, J. (2017). Regulation (EU) no 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eidas regulation). In *Eu regulation of E-commerce: A commentary* (pp. 256–289). Edward Elgar Publishing. https://doi.org/10.4337/9781785369346.00017
- Dunphy, P., & Petitcolas, F. A. P. (2018). A first look at identity management schemes on the blockchain. *IEEE Security and Privacy*, *16*(4), 20–29. https://doi.org/10.1109/MSP.2018.3111247
- ENISA. (2017). *Security Guidelines on the Appropriate Use of Qualified Electronic Seals*.
- Gramoli, V. (2020). From blockchain consensus back to Byzantine consensus. *Future Generation Computer Systems*, *107*, 760–769. https://doi.org/10.1016/j.future.2017.09.023
- Hristov, P., & Dimitrov, W. (2018). *The blockchain as a backbone of GDPR compliant frameworks*.
- Ishmaev, G. (2020). Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethics and Information Technology*, *0123456789*. https://doi.org/10.1007/s10676-020-09563-x
- Jensen, J. (2012). Federated identity management challenges. *Proceedings - 2012 7th International Conference on Availability, Reliability and Security, ARES 2012*, 230–235. https://doi.org/10.1109/ARES.2012.68
- Jover, R. P. (2020). Security Analysis of SMS as a Second Factor of Authentication. *Queue*, *18*(4), 37–60. https://doi.org/10.1145/3424302.3425909
- Kondova, G., & Erbguth, J. (2020). Self-sovereign identity on public blockchains and the GDPR. *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 342–345. https://doi.org/10.1145/3341105.3374066
- Kumar, V., & Bhardwaj, A. (2018). Identity Management Systems. *International Journal of Strategic Decision Sciences*, *9*(1), 63–78. https://doi.org/10.4018/ijsds.2018010105
- Li, W., Andreina, S., Bohli, J.-M., & Karame, G. (2017). *Securing Proof-of-Stake Blockchain Protocols* (pp. 297–315). https://doi.org/10.1007/978-3-319-67816-0_17
- Lim, S. Y., Fotsing, P. T., Almasri, A., Musa, O., Kiah, M. L. M., Ang, T. F., & Ismail, R. (2018). Blockchain technology the identity management and authentication service disruptor: A survey.

International Journal on Advanced Science, Engineering and Information Technology, *8*(4–2), 1735–1745. https://doi.org/10.18517/ijaseit.8.4-2.6838

- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, *20*(3), 709. https://doi.org/10.2307/258792
- Mead, N. R. (2003). Computer security: Art and science [Book Review]. *IEEE Security & Privacy*, *1*(3), 14–14. https://doi.org/10.1109/msecp.2003.1203217
- Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002
- Olsen, T., & Mahler, T. (2007). Identity management and data protection law: Risk, responsibility and compliance in "Circles of Trust" - Part II. *Computer Law and Security Report*, *23*(5), 415–426. https://doi.org/10.1016/j.clsr.2007.07.001
- Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. *Technical University Dresden*, 1–98. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml
- Pon, B., Locke, C., & Steinberg, T. (2016). *Private-Sector Digital Identity in Emerging Markets*. https://goodid-production.s3.amazonaws.com/documents/Caribou-Digitial-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf
- Roberto Leonardo, R., Giungato, P., Tarabella, A., & Tricase, C. (2019). Blockchain Applications and Sustainability Issues. *Www.Amfiteatrueconomic.Ro*, *21*(Special 13), 861. https://doi.org/10.24818/EA/2019/S13/861
- Särav, S., & Kerikmäe, T. (2016). E-residency: A cyberdream embodied in a digital identity card? In *The Future of Law and eTechnologies* (pp. 57–79). Springer International Publishing. https://doi.org/10.1007/978-3-319-26896-5_4
- Sim, W. L., Chua, H. N., & Tahir, M. (2019). Blockchain for Identity Management: The Implications to Personal Data Protection. *2019 IEEE Conference on Application, Information and Network Security (AINS)*, 30–35. https://doi.org/10.1109/AINS47559.2019.8968708
- Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law and Security Review*, *33*(4), 470–481. https://doi.org/10.1016/j.clsr.2017.03.016
- Sun, S.-T., & Beznosov, K. (2012). *The devil is in the (implementation) details*. 378. https://doi.org/10.1145/2382196.2382238
- The EU Blockchain Observatory and Forum. (2018). *EUBlockchain*. https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf
- Tobin, A., & Reed, D. (2016). *The inevitable rise of self-sovereign identity*. https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf
- Tracy, K. (2008). Identity management systems. *IEEE Potentials*, *27*(6), 34–37. https://doi.org/10.1109/MPOT.2008.929295
- Turkle, S. (1996). *Life on the Screen: Identity in the Age of the Internet*. Weidenfeld & Nicholson.
- Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability*, *28*, 1–9. https://doi.org/10.1016/j.cosust.2017.04.011
- Vukolić, M. (2016). *The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication* (pp. 112–125). https://doi.org/10.1007/978-3-319-39028-4_9
- W3C. (2018). *Verifiable Claims Working Group Frequently Asked Questions*. https://w3c.github.io/webpayments-ig/VCTF/charter/faq.html
- WP29. (2014). *Opinion 05/2014 on Anonymisation Techniques*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
- Ye, C., Li, G., Cai, H., Gu, Y., & Fukuda, A. (2018). Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting. *2018 5th International Conference on Dependable Systems and Their Applications (DSA)*, 15–24. https://doi.org/10.1109/DSA.2018.00015
- Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006
- Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. *Frontiers in Blockchain*, *3*. https://doi.org/10.3389/fbloc.2020.00026