



POLITECNICO MILANO 1863

School of Industrial and Information Engineering

Master of Science in Management Engineering

DIGITAL IDENTITY: THE INTERNATIONAL LANDSCAPE OF ACTIVE SYSTEMS

Supervisor:

Luca Gastaldi

Author:

Simone Pagano, 952848

Academic Year 2021/2022

Contents

| | |
|--|-----------|
| <i>Table of Figures</i> | 7 |
| <i>Abstract</i> | 8 |
| <i>Introduction</i> | 12 |
| 1. LITERATURE | 15 |
| 1.1 What is identity? | 15 |
| 1.2 Difference between Physical and Digital Identity | 15 |
| 1.3 Digital Identity | 16 |
| 1.4 Main Pillars | 17 |
| 1.5 The attributes of a digital identity | 18 |
| 1.6 Features a good identity should have | 19 |
| 1.6.1 Fit for Purpose Identity System | 20 |
| 1.6.2 Inclusive Identity System | 20 |
| 1.6.3 Useful Identity System | 21 |
| 1.6.4 Choice of the Digital Identity System | 22 |
| 1.6.5 Secure Digital Identity System | 22 |
| 1.7 Economic impacts | 23 |
| 1.8 Impacts on Industries | 24 |
| 1.8.1 Sharing Economy | 24 |
| 1.8.2 Healthcare | 25 |
| 1.8.3 Cyberspace | 25 |
| 1.8.4 Banking | 26 |
| 1.8.5 Insurance | 27 |
| 1.9 Types of Data | 28 |
| 1.10 Level of Assurance | 30 |
| 1.11 Models | 31 |
| 1.12 Digital Entities | 33 |
| 1.13 Main Actors in Identity Management | 34 |
| 1.14 Archetypes | 36 |
| 1.14.1 Centralized | 36 |
| 1.14.2 Federated | 37 |
| 1.14.3 Decentralized | 39 |
| 1.14.4 Self Sovereign Identity (SSI) | 40 |
| 1.15 Phases of the process | 43 |
| 1.15.1 Identification | 44 |
| 1.15.2 Authentication | 46 |
| 1.15.3 Authorization | 48 |

| | |
|---|-----------|
| 1.15.4 Identity Management..... | 49 |
| 1.16 Data Privacy | 49 |
| 1.17 Trust Services | 50 |
| 1.18 eIDAS Regulation | 51 |
| 1.19 PSD2, AML, GDPR Regulations..... | 52 |
| 1.19.1 PSD2 | 53 |
| 1.19.2 GDPR | 55 |
| 1.19.3 AMLD5..... | 56 |
| 1.20 Literature gap | 57 |
| 2. RESEARCH METHODOLOGY | 58 |
| 2.1 Digital Identity Observatory | 58 |
| 2.2 Research Question..... | 58 |
| 2.3 Theoretical Review | 60 |
| 2.4 Empirical Framework | 61 |
| 2.5 Source Selection and Data Extraction | 61 |
| 2.6 Screening and Data Integration | 64 |
| 2.7 Descriptive Analysis | 68 |
| 3. RESULTS | 69 |
| 3.1 Digital Identity Projects..... | 69 |
| 3.2 Geographical Distribution | 70 |
| 3.3 Technologies | 72 |
| 3.3.1 Distribution of technologies..... | 72 |
| 3.3.2 PKI (Public Key Infrastructure) | 73 |
| 3.3.3 Cloud-based Architectural Technology..... | 74 |
| 3.3.4 Blockchain Architectural Technology | 75 |
| 3.3.5 Biometrics Technology | 76 |
| 3.3.6 Open Standard Technology..... | 79 |
| 3.3.7 API & SDK Technology | 80 |
| 3.3.8 Typology of Identity | 80 |
| 3.3.9 Sovereign Identity | 81 |
| 3.3.10 Functional Identity | 82 |
| 3.3.11 Decentralized Identity..... | 82 |
| 3.4 Industries of application | 82 |
| 3.4.1 eGov | 84 |
| 3.4.2 Finance | 85 |
| 3.4.3 Healthcare..... | 85 |
| 3.4.4 eCommerce & Retail..... | 85 |
| 3.4.5 Education | 86 |
| 3.4.6 Telco & Mobility | 86 |
| 3.4.7 Enterprise and Tourism & Travels..... | 86 |

| | |
|---|------------|
| 3.4.8 Humanitarian Scope | 87 |
| 3.4.9 Application field of projects | 87 |
| 3.4.10 Application fields and technologies | 88 |
| 3.5 Providers & Economic Sustainability..... | 88 |
| 3.5.1 Service Providers | 89 |
| 3.5.2 Public vs Private SP | 89 |
| 3.5.3 Economic Sustainability | 94 |
| 4. CONCLUSIONS..... | 96 |
| 4.1 Limitations and future research..... | 98 |
| 5. ANNEX..... | 99 |
| 5.1 Population coverage | 99 |
| Bibliography..... | 105 |
| Acknowledgements | 113 |

Table of Figures

| | |
|---|----|
| Figure 1.1 Types of credentials (World Bank Group, 2016) | 29 |
| Figure 1.2 Levels of Assurance (World Bank, 2016) | 31 |
| Figure 1.3 Models of Digital Identity | 33 |
| Figure 1.4 Three identity system archetypes (World Economic Forum, 2018)..... | 36 |
| Figure 1.5 Centralised Identity Management Model (IDM 1.0) (Nitin Naik, Paul Jenkins, 2020) | 37 |
| Figure 1.6 Federated Identity Management Model (IDM 2.0) (Nitin Naik, Paul Jenkins, 2020) | 39 |
| Figure 1.7 Types of ecosystems (Digital Identity and Blockchain and Distributed Ledger Observatory, 2020) | 42 |
| Figure 1.8 Self-Sovereign Identity Management Model (IDM 3.0) (Nitin Naik, Paul Jenkins, 2020) | 43 |
| Figure 1.9 Identity Lifecycle (World Bank Group, 2018) | 44 |
| Figure 1.10 PSD2 Trilemma..... | 53 |
| Figure 1.11 PSD2 has a range of implications for banks (McKinsey Global Institute, 2018)..... | 54 |
| Figure 1.12 Survey with bankers’ responses (McKinsey, Global Payments Practice PSD2, 2017) | 55 |
| Figure 2.1 Empirical framework..... | 61 |
| Figure 3.1 Distribution of projects based on the stage | 70 |
| Figure 3.2 Geographical distribution of digital identity projects in the Globe..... | 71 |
| Figure 3.3 Telco & IoT | 75 |
| Figure 3.4 Projects implementing Blockchain | 76 |
| Figure 3.5 Biometrics distributions for access / authentication factors | 77 |
| Figure 3.6 Typologies of biometrics..... | 78 |
| Figure 3.7 Typologies of identity | 80 |
| Figure 3.8 General Purpose vs Verticals application industries & number of projects per scope | 83 |
| Figure 3.9 Fields of application per project | 87 |
| Figure 3.10 Distribution of technologies among industries | 88 |
| Figure 3.11 Presence of Private and Public Service Providers among 120 International Cases | 90 |
| Figure 3.12 Public Service Providers..... | 91 |
| Figure 3.13 Private Service Providers | 92 |
| Figure 3.14 Public & Private Service Providers..... | 93 |
| Figure 3.15 Economic Sustainability | 94 |
| Figure 5.1 Population coverage in digital identity projects in the last three years..... | 99 |
| Table 2.1 Keyword used for the Data Extraction..... | 62 |
| Table 2.2 Variables collected for the Data Extraction (part 1) | 64 |
| Table 2.3 Variables collected for the Data Extraction (part 2) | 67 |
| Table 3.1 Distribution of technologies in the main digital identity projects..... | 73 |
| Table 3.2 Typologies of biometrics | 78 |
| Table 3.3 Comparing Open Standards | 79 |
| Table 3.4 Distribution of sectors in the International Cases | 84 |
| Table 3.5 Number of Service Providers per project | 89 |

Abstract

English version

In the last decade, digital identity has gone from being a hot topic to becoming a necessary resource in the everyday life of almost every individual. There are eight billion people in the world, of whom just over a billion are those who do not have a physical identifier. Therefore, for those with a physical ID, digital identity represents an opportunity to optimise the identification system, facilitating many operations and services that until yesterday could only be performed by being physically present in a given place. Today, thanks to digital identity, it is possible to carry out countless online transactions, guaranteeing the identity of the user carrying out the transaction to the service provider, through the collaboration of an identity provider that creates and issues and then checks the authenticity of these identities.

In this regard, this Thesis aims to address the issue of digital identity, showing an overview at an international level of the projects developed to date, focusing the analysis on the pioneer countries of digital identity, which, especially in Europe, have invested considerable resources in the dissemination of digital identity, while at the same time pursuing a continuous improvement of the technologies involved in the various identification processes, in order to make digital identity increasingly reliable and of great added value, features that are highly appreciated by the many sectors of the world of work, digital and otherwise, prompting them to adopt a very valuable tool, which is what digital identity is proving to be.

Keywords: Digital ID, Identity, Identities, IDs, Identify, Identifies, identified, Identification, Authentication, Recognition, Onboarding, Passwordless, Verification, Self-Sovereign, Self Sovereign, SSI, PSD2, AMLD5, GDPR, Biometrics, Biometric, Entity, Entities, Service Provider, Trusted, Credential

Versione italiana

Nell'ultimo decennio l'identità digitale è passata dall'essere un argomento di estrema attualità a diventare una risorsa necessaria nella quotidianità di quasi ogni singolo individuo. Nel mondo ci sono otto miliardi di persone, tra queste poco più di un miliardo sono le persone che non dispongono di un identificativo fisico. Dunque, per coloro dotati di un identificativo, l'identità digitale rappresenta un'opportunità per ottimizzare il sistema di identificazione, facilitando molte operazioni e servizi che fino a ieri potevano essere svolti solo essendo presenti fisicamente in un determinato luogo. Oggi, grazie all'identità digitale è possibile eseguire innumerevoli transazioni online, garantendo al fornitore del servizio l'identità dell'utente che compie l'operazione, tramite la collaborazione di un fornitore di identità che crea ed emette per poi controllare l'autenticità di queste identità.

A tal proposito, questa Tesi di Laurea si prefigge l'obiettivo di affrontare il tema dell'identità digitale, mostrando una panoramica a livello internazionale dei progetti sviluppati fino a questo momento, incentrando l'analisi sui paesi pionieri dell'identità digitale, i quali, specialmente in Europa, hanno investito ingenti risorse per la diffusione dell'identità di digitale, perseguendone al contempo un

miglioramento continuo delle tecnologie coinvolte nei vari processi di identificazione, al fine di rendere l'identità digitale sempre più affidabile e di grande valore aggiunto, caratteristiche assai apprezzate dai molteplici settori del mondo del lavoro, digitali e non, spingendoli ad adottare un preziosissimo strumento, ovvero ciò che sta dimostrando di essere l'identità digitale.

Parole chiave: ID Digitale, Identità, IDs, Identificato, Identificare, Identificazione, Autenticazione, Riconoscimento, Onboarding, Passwordless, Verifica, Self-Sovereign, Self Sovereign, SSI, PSD2, AMLD5, GDPR, Biometria, Biometrico, Entità, Fornitore di Servizi, Trusted, Credenziali

Executive Summary

The world is evolving toward greater digitalization, and as a result, more people are using the internet and other digital technology. The advent of the Covid19 epidemic also caused a disruption in other practices, leading businesses to require their employees to work remotely, which increased the need for digitalization due to the instruments required for smart working. The public sector was impacted as well, with services that were previously only available in government offices being moved online. Due to many developments, including e-commerce (with the emergence of over-the-top players like Amazon) and e-government services, the number of online transactions is constantly increasing (which permit efficiency and efficacy avoiding queues). Both sides must be represented in the digital space in order to allow for successful and safe transactions. To access and be recognized on the internet and establish trust, it is therefore necessary but challenging to construct a digital identity. It is crucial to establish the proper privacy standards, preserve citizen data, and at the same time, demand only the precise amount of data required for a secure transaction.

Because of the various advantages connected with this instrument, such as the reduction of costs and time with the subsequent growth in sales of goods and services, therefore the increase in employment and labour productivity, stakeholders are working to improve all elements of digital identity more and more. From a societal standpoint, the Sustainable Development Goals' target 16.9, "Provide legal identification for all by 2030," may not be achievable without the use of digital identity. This goal was set by the UN in 2015. There are predicted to be 1.1 billion people without an identification in 2020, which keeps them out of society and prevents them from doing things like opening bank accounts or purchasing homes.

This Thesis aims at representing the international landscape of active systems working in the Digital Identity industry, to learn about the features, different services and solutions that are provided to address the demands and issues relating to the subject. To achieve the objective, the research methodology was composed by 3 fundamental parts: a theoretical review of the present literature (analysing documents, papers and reports on the topic), an empirical framework utilized to build the census (which at the end collected 120 international cases, each with 65 different variables), and a descriptive analysis in which variables were analysed individually and combined to gather the main insights of the digital identity landscape of active systems to date.

The projects were chosen based on their home countries. A country-by-country split was performed in order to focus on countries with a high level of knowledge and experimentation with digital identity. Following the selection of the most interesting countries, some projects were chosen for each state. There have been countries with 5-6 digital identity projects and others with only one. In this case, the decision was influenced by the project's maturity. Priority was usually given to fully operational projects. After selecting all the projects, extensive research was conducted to assign technical digital identity variables to each one. The main goal was to assess the population's level of coverage for each project, so how many people in a country were using a specific digital identity, essentially the level of adoption of a digital identity, expressed in percentage, taking into account the number of people per country. After receiving this result, the goal became to gather as much information as possible about that project, based on the variables suggested by Digital Identity Observatory experts. The keywords chosen for the extraction by a team comprised of the undersigned and subject matter experts, were

used as filters to extract project information from the Digital Identity ecosystem. The keywords were inserted in research on the Internet. A total of 27 keywords were defined.

The variables were then analysed and combined to form a picture of the Digital Identity landscape of active systems, gather relevant insights, and answer the research question. The outcomes were catalogued in four different dimensions.

The most representative continent in terms of number of projects was Europe. In the *Results* and *Conclusions* chapters there are several bias explaining why almost all the projects were adopted in Europe. Among the different technologies adopted in each project, PKI and API&SDK were the most utilized. The sector most targeted was the Governmental one, but there were more popular sectors, such as Finance and Healthcare. Service providers were proved to be more numerous in the public rather than in the private sector. Finally, the economic sustainability was classified, showing a trend were usually the service providers are the most hit.

Despite some limitations, the work aims to raise awareness about Digital Identity and to create a comprehensive and reliable database from which future research can be launched.

Introduction

Digital identity is a topic that emerged 15-20 years ago, with the first evidence appearing in 2005 papers such as Shim's "Federated identity management" or Windley's book "Digital Identity." After a quiet start, it is now bursting into the spotlight, and it is becoming increasingly important due to the need for proof of existence in the digital world.

The pandemic Covid 19 also provided a strong impetus for the digitization of services in both the public and private sectors, redesigning transactions, and interactions with end users. As a result, digital identity is required to gain access to the digital world.

Organizations in the public and private sectors are switching to online services as a result of the need to cut costs, improve service delivery efficiency, and decrease fraud, particularly benefit fraud (Sullivan, 2018). As a result of this transformation, there have been more digital transactions, which has altered how traditional transactions were carried out. This has enhanced the significance of digital identity and given it a new degree of legal and economic significance (Sullivan, 2012).

Policymakers, regulators, and financial institutions are facing challenges because of the Internet's and Web 2.0's growth in the previous two decades due to the novel ways that interactions between digital entities are carried out (Arner et al., 2019). (Li et al., 2020). From online banking and e-commerce to messaging and trip booking, nearly every sector is relocating its services to the digital sphere. As a result, society has become almost completely integrated. The constant adoption of web applications has significantly altered consumer and business behavior. Businesses must develop new ways to engage with customers in a digitally focused economy. Business relationships with partners, suppliers, and staff have also altered, in addition to those with customers and products (Dib and Toumi, 2020).

The banking sector had the most notable change in the digital transformations (Arner et al., 2019). For example, to access a bank account, it is essential in this industry to have a precise identity system and computerized user recognition. It is very crucial to adhere to the Know Your Customer compliance in this situation. Know Your Customer (KYC) is the practice of confirming the identification of one's own customers, either before or while they are beginning a business relationship with the organization. The word "KYC" also refers to the procedures that are regulated by banks for determining a customer's identification and monitoring consumer risk. Diverse onboarding procedures, identity criteria, and authentication methods are produced by the various KYC needs across industries.

Market integrity depends on an ongoing process of confirming a client's identification and doing KYC due diligence before accepting a new customer (onboarding). The guidelines for these actions are included in a variety of anti-money-laundering (AML), countering the financing of terrorism (CFT), and customer due diligence (CDD) laws and regulations. Additionally, CDD supports how customers' demands are addressed, which is crucial for offering suitable financial services (Arner et al., 2019).

New industries based on digital identity have also emerged as a result of the digital transition, including e-commerce and social media (such as Facebook, Instagram, and Tencent) (e.g., Amazon and Alibaba). Each has (re)defined what constitutes a person's identity and how that identity is verified. To open an electronic commerce (e-commerce) account, for instance, social networking credentials can be utilized. For instance, a Google email identification could be used to verify a person's identity for the online lodging provider Airbnb (Arner et al., 2019).

Moving on to the public sector, several governments, such as Estonia, have taken steps in recent years to create extensive digital identity networks. Such efforts signify a desire to move beyond their ineffective paper-based existence to highly integrated and interoperable digital economies, where it has been decided that at least one type of digital identity is necessary for such transformations (Atick, 2016).

On the other hand, those who apply for digital identities have a lot of benefits, including quicker access to services, the ability to request documents that are supplied digitally rather than on paper, and the ability to avoid lines and moves. People are worried that firms and government agencies will gather and use more personal data than they need. By updating their rights, individuals should regain authority. Key elements include the right to be informed of personal data breaches, the right to data portability, and the right to be forgotten (Rannenberget al., 2015).

The digital world's currency is data. European Data had a 1 trillion-euro market cap in 2020. It depends on trust, just as any currency. To rebuild consumer trust in the digital economy, businesses and governments must involve consumers. Therefore, strict European legislation is required to protect personal data. The value of European data was already 315 billion euros in 2011. However, Europeans have a low level of trust in the way that data is used in the economy. 92% of Europeans were concerned about the way their data is used without their consent even before the surveillance allegations (Rannenberget al., 2015).

In order to achieve uniform standards, nations are working together, and the European Union is constantly paying more and more attention to privacy issues.

The eIDAS regulation was developed by the European Commission in 2014 and is made up of standards for digital signatures, qualified digital certificates, electronic seals, timestamps, and other identity proofing and authentication mechanisms. Its goal is to facilitate digital trust and safety across borders. The European Commission has suggested a regulatory framework that is open to all individuals and businesses as of June 2021. With their national digital identification, which will be accepted in Europe, citizens will be able to access online services thanks to the European Digital Identity.

The Sustainable Development Goals (SDG) of The Agenda 2030 include a target of 16.9, and the European Union and United Nations view digital identity as a tool to meet that goal. The United Nations General Assembly launched the initiative in 2015 with the goal of eradicating poverty in all of its manifestations while making progress in three areas: the environment, society, and economy. There are 17 goals to be accomplished by 2030, broken down into 169 targets, and tracked by more than 240 indicators (Tiresia, 2020).

Promote inclusive and peaceful societies for sustainable development, ensure that everyone has access to justice, and create inclusive, effective, and accountable institutions at all levels, according to Goal 16. The 16.9 specifically addresses the theme of identity, with the United Nations promising to "provide legal identity for all, including birth registration by 2030" (United Nations, 2015).

Estimates from the World Bank's ID4D database indicate that approximately a billion people worldwide lack any type of identity that is legally recognized. A further 3.4 billion people have restricted access to using certain sorts of legally recognized identification in the digital realm (Mc Kinsey, 2019).

The remaining 3.2 billion people participate in the digital economy and have legal identities, but they might not be able to use those identities effectively and efficiently online (Mc Kinsey, 2019).

The population that is socioeconomically disadvantaged also faces the problem of falling victim to what Gilman and Green (2018) have dubbed the "surveillance gap," or the "systemic invisibility" of some social strata. Governments in the global South have launched extensive identification initiatives to address this problem of marginalization. Even while it is obvious that digital identities are necessary, these programs raise questions about their possible harmful effects. Initiatives like ID4D (Identity for Development) contend that properly run digital identity programs may increase the inclusion of marginalized communities and the effectiveness of governance (World Bank, 2016).

Having highlighted the importance of Digital Identity, it is important to understand better what it is, how it works, who is involved in the process, which are the types of ecosystems and so on and so forth. It is important to understand which are the future directions that the sector is taking: looking at the landscape of active systems could give the right perspective of the market and which the further evolution could be.

This thesis aims to explore the Digital Identity theme and analyse the international cases more diffused in the world.

To achieve these goals, this work has been structured in:

- Literature, describing the Digital identity topic including every single aspect and entailment, collected by different articles, reports and books, to give an overview over the theme.
- Research Methodology, illustrating the whole process from the theoretical review to the empirical framework, formalising and explaining the research.
- Results, reporting the outcome of the analysis, thus providing a picture of the Digital Identity landscape of active systems.
- Conclusions, where it is elaborated the work, answering to the research question. It reports also some limitations encountered and which could be the future in depth analysis.
- Annex, where a further insight is given to some of the most adopted and famous projects, among those analysed is conducted.

1. LITERATURE

The chapter illustrates the results of the literature research on the Digital Identity topic, delineating the theoretical background of this work, fundamental to understand the importance of the argument and how much potential is still unexploited.

1.1 What is identity?

In 2022, digital identity is a trend that has recently experienced strong growth and has become a staple for many people and many technological systems. Suffice it to say that for everyone, there are identities linked to appearance, personality and many other characteristics that define an individual. The primary purpose of an identity system is to uniquely identify human beings who are part of society. Nowadays, identity, having taken on a digital connotation, has led us to have irrefutable traces of our identity, such as birth, graduation, marriage and death certificates, social security numbers, postal addresses, e-mail addresses, mobile phone numbers, driving licences, credit card numbers and membership numbers of organisations to which we belong. Moreover, the concept of identity has even expanded to include animals and objects. A place identity is even possible, certifying where people, animals or things are at any given time. It is even possible to identify persons and organisations by means of a legal identity, and one can own goods that are also identifiable through appropriate proofs of purchase and deeds of ownership. Thus, it is a fact that identity has taken on a primary connotation in our lives because of the way it simplifies our lives. Therefore, it is considered increasingly indispensable by the community. The number of frontier technologies that collect data based on the identities of individuals, animals and things is growing steadily. This data is then sent to business systems that can track, analyse, and make decisions (Thompson, 2007). A national government, a consortium of private or non-profit organizations, or a single entity can manage these channels. Furthermore, digital authentication can occur via a variety of modes and technologies, including biometric data, PINs, smart devices, and security tokens (Mc Kinsey, 2019). The next paragraph will focus on the main differences between physical and digital identity.

1.2 Difference between Physical and Digital Identity

The Digital Identity Observatory of Politecnico di Milano has identified some differences between physical and digital identity, the main ones are:

- Proliferation: each person can own just one or few recognized physical identities, which are often associated to a physical document, while it is possible to activate and own more digital identity contemporarily, for example the social network ones.

- Validity: the documents of the physical world are accepted on the whole national territory and in most cases also at international level, while the digital identity is recognized only in the ecosystem of actors that has joined to the system and to prepare the technological infrastructure for the integration with the identity provider.
- Ecosystem: for the physical identity, the institution that release the document is not involved in the next interaction in which the document is required, while for the digital identity the actors are involved in every single interaction, enabling the exchange of identification data required for the service delivery.
- Dynamicity: the physical identity has a predefined and static dataset, including personal data and biometric data stored on the document, while the digital identity is composed by a set of dynamic data, with higher frequency of updating and the possibility of connecting the profile with other information related to the digital interactions of the users.

Having established the main differences between physical and digital identity, the next paragraph will have the aim of building a complete definition of digital identity.

1.3 Digital Identity

In 1600, Leibniz defined identity in terms of the distinguishability of one thing from another. If object A shares absolutely every characteristic of object B, including shape, extent, position in time and space, then A and B are identical: they can identify each other. This is a very useful principle when considering online identity systems, specifically, because of their high dependence on the credential system. When a credential is presented in support of an authentication request, it is essentially used as proof that the person presenting it 'has an identity relationship' with the person to whom it was issued at some point in the past. Thus, a definition of 'identity' in the online world is 'the identity relationship between a person at the time of registration and a person at the time of authentication' (Wilton, 2008). The ability to create and have a unique correspondence for an individual, between a moment belonging to their past and a moment belonging to their present, allows the uniqueness of the individual to be imbued with context and meaning.

Digital identity is often defined as a digital reference to a person (Alamillo, 2020), almost as if it were a label attached to an individual, capable of identifying him and him alone.

It is thus something that an individual possesses and uses in response to requests for digital identification, authentication, or proof of authorisation (Sedlmeir et al. 2021), which are precisely the fundamental steps that a digital identity management system must provide.

As already pointed out, the subject of a digital identity is often a human being, but can also be a legal entity, an animal, or a device, among others. Therefore, discussions on digital identities should not put the focus exclusively on human subjects (Dietz, 2020; Fedrechski et al. 2020; Zwitter et al. 2020).

It can be agreed that identity can be defined as 'one or more attributes applicable to this particular subject or object'. (Rasouli, 2019). For example, a user may possess many different identities and each identity may be dedicated to some of its attributes.

Therefore, to approach a comprehensive definition of digital identity, we can say that it allows individuals to take control of their personal data when it needs to be shared with third parties and thus supports their privacy (Tatli, 2009).

On the other hand, in a full digital world like the one that characterises 2022, identity cannot but be the most important part of any security-conscious system. It allows users, services, servers, and any other entity to be identified and recognised by other systems and parties (Al morsy et al., 2016; Rasouli, 2019). Moreover, the effective management of Digital Identity, data and access to data and applications is the key element to identify, prevent and protect critical assets from inappropriate access and use, safeguarding the business continuity of companies and services to citizens (PwC, 2022).

Based on all the considerations and definitions of identity that have been agreed upon in recent decades, if it should be found the easiest way to define it, digital identity is a fundamental tool with which a person can access services (Sullivan, 2016).

However, it is appropriate to formulate a definitive one that fully covers the role and meaning of digital identity. In this regard, the Osservatorio sull'Identità Digitale (Digital Identity Observatory) of the Politecnico di Milano defines Digital Identity as 'a set of data that allow for the unambiguous identification of a person, a company or an object, which are collected, stored and shared digitally within an ecosystem of actors, through enabling technologies, that allow access to value-added digital services'.

1.4 Main Pillars

From Digital Identity Observatory of Politecnico di Milano's research and from the studies of different digital identity system, four main pillars emerge (which are described more in details in the next chapters):

1. Identity data: key dimensions are the richness and assurance of the data, which have the functions of identifying in unequivocal manner the individual, defining what it can do and tracking its interaction in the digital world. Two types of data are identified: constitutive data (static) such as personal, biometrics and certification, and dynamic data, such as interaction of the person with another entity.
2. Accessible service: the digital identity allows the user to access value-added services, to enable transactions and to make operations in the digital world. Different services could have different criticality levels for which different levels of assurance are requested.
3. Ecosystem: different actors can oversee one or more roles and the combination of them, basing on the configuration of the system, take different levels of concentration.
4. Technology: based on the different infrastructural layer. There are three different types:
 - Architectural: such as blockchain and cloud platforms, which are the infrastructural base of the system, designing its configuration, which can be centralized, federated, and decentralized, and its consequent business model.

- Integrational: such as standard protocol and Application Programming Interface (API), to support the interoperability among different systems.
- Front-end process: such as devices for biometric recognition and algorithms of Artificial Intelligence (AI) and Machine Learning, which constitute the front-end with the user, allowing the entire lifecycle of the digital identity in the phase of identification, authentication, and authorization, making them more fluid and safer.

1.5 The attributes of a digital identity

Nowadays, digital identity provides access to a variety of services such as banking, government, education, and many others. For a digital identity to be considered good, it must have the four characteristics listed below (Mc Kinsey, 2019):

- **Verified and authenticated** to a high degree of certainty. Verification entails ensuring that a person's basic information establishes his or her identity. This process is typically carried out during the initial registration of a digital identity or when an individual's information in the identification system is updated. Authentication, on the other hand, is the process by which an identity established during the registration process is validated. Authentication occurs when an individual, for example, uses his or her ID with the requesting entities, which will provide the individual with the service. The high-security digital identity meets the requirements of government and private institutions for initial registration and subsequent acceptance for a wide range of important civic and economic uses, including access to education, opening a bank account, and establishing job credentials. This property is not dependent on any underlying technology. For unique, high-security authentication and verification, a variety of credentials, including biometrics, passwords, QR codes, and smart devices with embedded identity information, can be used.
- **Unique**, with a unique digital ID. Within a system, an individual can only have one identity, and each identity in the system corresponds to one individual. Most social media identities, for example, lack this feature.
- **Established with the individual's consent**. It means that users register and use the digital ID consciously, knowing what personal data will be collected and how it will be used.
- **Protects user privacy and provides them control** over their personal data. This translates into built-in safeguards that ensure user data privacy and security while also providing individuals with access to their personal data, decision-making rights over who has access to that data, and transparency about who has access to it.

1.6 Features a good identity should have

Identification is important in the digital age because it reduces the complexity of managing records and systems, for human beings, who are mostly classified by others. Think of the refugee who receives a 'refugee identity' from the UNHCR, or the platform worker who is identified by a scan of the national ID she presents with her profile (Masiero, 2020). According to Nyst, such a conversion results in schemes that enable digital identification of individuals, as well as authentication at various points of access and, on that basis, authorisation for them to perform given actions or access given services. The three functions of identification, authentication, and authorization are all performed digitally in digital identity schemes (Nyst et al., 2016). At the World Economic Forum's Annual Meeting in Davos 2018, a community of stakeholders from government, business, and civil society committed to moving digital identities toward a "good" future. Since then, a larger group has joined the conversation, and an initial set of five elements that a good identity must satisfy has been identified. All five are equally important, and there are some tensions between them: for example, features that improve security for individuals and their identities may reduce their convenience. User-centric digital identities must succeed in all aspects in order to provide real value to individuals and thus drive adoption (World Economic Forum, 2018):

1. **fit for purpose**, that is, a digital identity should first and foremost ensure trustworthiness in order for the person who authenticates to have full trust from the digital identity system. This user trustworthiness principle should be met both in the exercise of one's rights and freedoms and/or eligibility to engage in digital interactions. The increasing number of digital transactions stimulates the development of digital identity systems.
2. **inclusive**, because a digital identity must provide all users with the ability to authenticate and access online services equally and without discrimination (based on their identity data).
3. **useful**, that is, a digital identity is useful when it provides access to a wide range of services and interactions that are convenient to the user and is easily accessible and usable by the user. Unfortunately, being useful is not an obvious requirement; in fact, most digital identities turn out to be repetitive in their daily usage and thus limited.
4. **provides choice**, which means that individuals are the only ones who have the authority to decide when and how a system may use their data. Similarly, users are the only ones who can decide whether to share their data and for what reason, as well as for how long and with whom. Users currently have little control over their data. This lack of control is the primary reason why individuals are constantly exposed to risks such as privacy violations, identity theft, fraud, and other abuses.
5. **security**, which refers to individual and organizational safety. Unauthorized data sharing and human rights violations are also security concerns. Unfortunately, there is still no basis for ensuring such consistency. One of the possible causes of this disadvantage is that user identity information is dispersed throughout the digital scope.

Finally, by implementing a secure digital identity, organizations gain a standardized and interoperable approach that can aid in risk reduction when authenticating a customer's identity. However, the digital identity model is currently fragmented because different public and private entities manage identity in their own silos. One possible outcome is that users will have a frustrating digital experience and will

be exposed to risks. To mitigate risks, the public and private sectors would need to collaborate to build a secure digital identity infrastructure. For example, the latter could aim to reduce the amount of transaction data collected in the context of identity verification.

1.6.1 Fit for Purpose Identity System

A fit-for-purpose identity system should be endowed of four main elements (World Economic Forum, 2018):

- **accuracy**, meaning that identity-related data must be error-free, guaranteeing a high standard of care in every aspect, and must give the possibility to be updated. Indeed, a possible output, should the principles of accuracy not be fulfilled, would be to have an identity system containing unreliable data.
- **uniqueness**, which means that the uniqueness of any system's user population must be ensured. The level of risk generated in each transaction where the identification is highly relevant is directly proportional to the level of uniqueness. As a result, high levels of risk necessitate stronger identity assurance. By increasing the reliability of the identity, uniqueness contributes significantly to the fight against identity fraud. To date, one common method of establishing uniqueness in a user population is to provide users with unique usernames that serve as identifiers before combining them with passwords. Another method that has grown in popularity in the last decade is the use of biometrics, which are unique personal characteristics such as facial features and fingerprints. Because biometric data is sensitive personally identifiable information, security and privacy practices must be highly accurate. This emphasizes that uniqueness cannot exist without accuracy, and vice versa.
- **sustainability**, a term that is becoming more common across all fields of technology. In this case, tough identity systems are required from a financial standpoint, as well as a caring and positive attitude toward technology investment, policies, and user expectations (since they are going to evolve). An identity system with these characteristics has a better chance of remaining relevant in the future.
- **Scalability** is a general rule that also applies to digital identity systems. The greater the market demand, the faster and more powerful the system's growth.

Accuracy and uniqueness are two fundamental aspects of user identification and authentication processes. Sustainability and scalability aid in attracting more actors into the system, each with different goals but a common interest in digital identity.

1.6.2 Inclusive Identity System

An identity system should ensure the following elements to make sure that each individual feels included within it and that users have the access they require (World Economic Forum, 2018):

- **equal opportunity**, with no restrictions on use within the target population Every user must have a digital identity that can be authenticated in order for the system to recognize the user.
- **safeguards against discrimination**, which is directly related to the issue of equal opportunity. In fact, if this last one is not followed, users may face difficulties in establishing and using identities, potentially leading to discrimination and exclusion.
- **mechanisms for dealing with unintended consequences**, such as when data and security standards prevent individuals from joining the system and its services. These unintended consequences must be avoided by implementing appropriate countermeasures capable of addressing and managing the issue that prevents the user from having the same rights of the other ones.

Among the benefits of inclusion there are the widespread adoption of the digital identity system and the decrease in the digital divide. This has a positive impact on the system itself by increasing economic development, which can also translate into creating sustainability; in fact, digital identity systems benefit unquestionably if they have an established user base. Standards for identity data and interactions with trust anchors that all users can fulfil will make a digital identity framework more inclusive. If data is not accepted, dependent parties may place greater trust in some identities than others, which could result in discrimination. Standards can proactively identify and rectify gaps that could lead to exclusion. Individuals' rights to privacy and security can also be exercised with the aid of standards for user protection, consent, and control.

1.6.3 Useful Identity System

For people to want to use digital IDs, identity management systems must include (World Economic Forum, 2018):

- **utility**: access to a variety of valuable digital interactions and services is provided by useful digital identities.
- **convenience**: digital identities should be easy to use, register, and administer.
- **ease of use**: user-friendliness results from identification and authentication made as simple as feasible, with friction according to the use-case.
- **interoperability and portability**: while maintaining security and privacy, digital identities should be usable across services, industries, and geographical boundaries.

In addition to making people's life simpler, features like utility, convenience, ease of use, interoperability and portability increase the likelihood that people and organizations will use the system. This boosts the likelihood of widespread adoption and increases the incentives for relying parties to use it as well. Broad acceptance can help increased efficiency as well as financial sustainability. People will require fewer identities to communicate with all the entities they need to because digital identities are acceptable across industries and borders. Fewer identities also mean fewer standalone data silos, which reduce efficiency and increase risk. Digital services frequently span sectoral, regional, and even public-private divides, yet many identities do not. When you want to rent

an apartment in a foreign nation, for instance, the landlord might not accept your local electricity bill or credit history. Mutual recognition, which allows users to authenticate and access services using credentials provided by other systems, could increase collaboration and lower costs, especially for numerous cross-border or cross-sector operations. Convenience is increased by interoperable systems that can exchange data or communicate with one another. Designers must be aware of the dangers associated with interoperability, as a networked system may provide greater opportunities for the spread of security vulnerabilities.

1.6.4 Choice of the Digital Identity System

The guidelines for selecting a digital identity comprise (World Economic Forum, 2018):

- **transparency:** users may see who is gathering and disclosing their information, how it is being used and processed, and for what reason.
- **privacy:** identity systems must incorporate privacy rights into their technologies and procedures so that people have control over who has access to, uses, and maintains their identity data, as well as the ability to change and delete it as necessary.
- **data protection:** to prevent breaches, corruption, or loss of personal data, technology design, operational controls, and legislation will be in place.
- **user control:** people will have greater control over associated opportunities and hazards if they have more freedom to pick which identification systems to employ as well as how to maintain, update, and own their data.

The 1948 Universal Declaration of Human Rights' guarantee of the right to privacy can be upheld or violated depending on how digital identities are created. People are expecting more control over their personal data. Identity systems that satisfy the above-mentioned requirements, will probably increase confidence, reduce the possibility of abuse or manipulation, and be more widely adopted by users. Regulators are also paying more attention to data security and privacy. As regards data protections, GDPR (the General Data Protection Regulation) of the European Union broadens the definition of personally identifiable information (PII). For instance, IP addresses and emails are now included. The GDPR also creates several rights for EU citizens relating to their personal digital data, including identification data, and regulates how PII may be handled. One of these rights is the right to know how businesses are gathering and using their personal data. Users have the option to limit the usage of their data for marketing and request that it be erased.

1.6.5 Secure Digital Identity System

A reliable digital identity system must provide (World Economic Forum, 2018):

- **protection:** strict cybersecurity procedures are regularly improved to reduce risks and thwart unwanted or unintended access, disclosure, or manipulation.

- **data integrity:** although people should be able to ask for their data to be removed, secure systems protect the integrity of digital identification data.
- **liability:** frameworks should incorporate an audit trail, assign blame, and offer redress in the event of a security breach or leak.

Building trust between individuals and depending parties, reducing cybercrimes like identity theft, and preventing undesirable consequences, such as human rights violations, all depend on security. A safe system that safeguards data enables people from all socioeconomic backgrounds to benefit to the fullest. Connected gadgets are becoming more and more commonplace, which makes them perfect targets for hackers. Verifiable digital identities can be used to identify compromised and rogue devices to reduce the potential damage they may do to people and systems. The strongest line of defence against data theft and misuse is educating people on how to keep their data secure and what they can do to reduce risk.

1.7 Economic impacts

Identification can be used by people to interact with businesses, governments, and other people in six different capacities: as consumers, employees, taxpayers, beneficiaries, civically active citizens, and asset owners. Institutions can consequently use a person's identity in a wide range of capacities, including those of commercial providers of goods and services, employers of workers, public providers of goods and services, beneficiaries, governments, and asset registers, which deal with private asset owners. The four factors that have the greatest direct economic value for people around the world are enhanced access to jobs, time savings, and increasing usage of financial services. Cost savings, less fraud, greater sales of goods and services, enhanced labour productivity, and increased tax income are the top five sources of value for institutions in both the public and commercial sectors. By facilitating increased formalization of economic flows, encouraging wider participation of people in a range of services, and permitting progressive digitization of sensitive interactions that demand high levels of trust, digital ID can add economic value for nations. According to Mc Kinsey's examination of Brazil, China, Ethiopia, India, Nigeria, the United Kingdom, and the United States, each nation might in 2030 realize economic benefits from the introduction of digital identity programs equal to between 3 and 13 percent of GDP (Mc Kinsey, 2019). McKinsey distinguishes between basic digital identity, which allows for verification and authentication, and advanced digital identity, which is digital identity with advanced uses. With informed user consent, advanced digital identity makes it possible to store or link more information about individual digital identity owners, which might facilitate advanced data exchange. For instance, while paying taxes, an advanced digital identity system would enable the taxpayer to authorize the taxing authority to digitally access the pertinent bank information, investment account information, and employment records required for timely and accurate filing. These kinds of sophisticated digital identity programs should be created with owner agency and data reduction in mind. Data owners—in this case, the holders of digital identities—need to be educated and empowered to give informed consent and exercise control over the use of their data, while public and private data aggregators must preserve user privacy and be accountable for the data they collect and process. Because larger digital ecosystems can be constructed on top of a basic digital identity

that permits an underlying ability to authenticate through digital channels, the distinction between basic and advanced digital identity may frequently become hazy. According to Mc Kinsey, assuming adoption rates of roughly 70%, a simple digital identity may in the emerging economies release 50 to 70% of the total economic potential. According to Mc Kinsey, assuming high adoption rates, digital identity has the potential to provide economic value in 2030 that is equal to 6% of GDP in emerging economies on a per-country basis and 3% in established economies. Even with a simple digital identity that has the bare minimum of features, a significant amount of value might be collected in emerging economies. It is necessary to have sophisticated digital identity programs with data-sharing features in mature economies because many procedures are already digital and there is less room for improvement. According to McKinsey, of the potential value, individuals may receive around 65% of it in emerging economies and roughly 40% of it in developed nations. (Mc Kinsey, 2019).

1.8 Impacts on Industries

In this paragraph is analysed the impact that digital identity is having the five sectors more deeply involved due to technological evolution, in the last decades.

1.8.1 Sharing Economy

A burgeoning ecosystem of online marketplaces devoted to the exchange of goods and services is referred to as the sharing economy (SE). SE represents a totally independent notion despite sharing its peer-to-peer character with other online ecosystems, such as e-commerce websites (Zloteanu, et al., 2018).

Most consumers are aware that the services they purchase are subject to rules, consumer protection legislation, and governmental oversight, which provides some level of liability, security, and safety. As SE platforms allow for direct and generally unmediated connection between people who have never met before either offline or online, these protections are lessened within the SE. In the absence of the usual signs used to signal quality or reliability in traditional markets, SE operations demand a high level of confidence on behalf of all parties involved (Zloteanu, et al., 2018).

User reputation is a significant factor influencing user behaviour within the SE. A person's reputation can be viewed as an overall indicator of how much people trust them. As a result, in the SE, a solid reputation can successfully play a regulatory role that promotes confidence. Overall, it may be said that the SE's most valuable assets are trust and reputation (Zloteanu, et al., 2018).

Though DI is clearly a complex and nuanced term in general, it takes on a more specific meaning in the SE context due to the interaction between the information that SE users voluntarily disclose and the information that their peers share about their previous encounters with them. Systems that provide reputation-building information are at the heart of any SE platform. These systems typically combine

subjective user contributed content (UGC) into a reputation score, which in turn serves as the foundation of a user's DI on the platform. The majority of SE platforms actively advertise tools that let users share information, rate other users, and establish a reputation on the site. Such content is typically presented as text reviews and numbers, such as scores between 1 and 5 (Zloteanu, et al., 2018).

1.8.2 Healthcare

Highly private information about patients is contained in hospital information systems. Digital identity management stands for a person's capacity to exercise control over their existence and identity. These days, the real and digital worlds are closely intertwined, making it essential to defend digital identity management just as much as physical identity. How to process a patient's digital data while maintaining the patient's privacy and security is a brand-new difficulty (World Economic Forum Report 2018).

In traditional centralized arrangements, the patient's healthcare provider oversees protecting the patient's privacy. As a result, to get treatment, a patient must have faith in the service provider. Traditional centralized methods have several drawbacks. Therefore, hardware or system errors could result in the loss of patient data. Additionally, patients won't be able to track or reverse changes to their data if it has been compromised or altered. Moreover, service providers must be implicitly involved when moving data between data centres. In this sense, patients can benefit from decentralized trustless peer-to-peer transactions by empowering them to take control of their own data (World Economic Forum Report 2018).

To realize a standardized, interoperable healthcare ecosystem that supports self-sovereign identity, certain capabilities must be implemented. Patients control the process of exchanging their health data with other stakeholders in the healthcare ecosystem, thus patients are at the centre of the ecosystem regardless of the source of the health data (World Economic Forum Report 2018).

1.8.3 Cyberspace

All components of a cyberspace-based IT system will require digital identities. Although identifying people in cyberspace is a common application of digital identification, people are only one component of an IT system. Policy makers and engineers must comprehend that an IT system is a tightly connected group of interconnected pieces that all require digital identification in order to conduct cyberspace operations and adequately protect IT assets. An IT system is made up of five different components: personnel, processes, software, hardware, and data (Silver, 1995).

It would be possible to identify correctly, effectively, and rapidly each of the component's entities even in a constantly changing environment by giving each one of them a unique digital identity. Currently, there is still significant effort to be done to precisely identify and keep track of the distinct

parts of an IT system. A more effective digital identity would enable the fusion of cybersecurity with a wide range of other business-related requirements, including (Friedman, 2015):

- asset management
- licensing
- policy enforcement
- disaster recovery
- liability
- productivity and convenience

The increased and expanded demand for new standards is being driven by the need for comprehensive digital identity:

- the push to develop new architectures, technologies, and business models
- the demand for shared services to capitalize on economies of scale and provide user choice and flexibility while increasing security and supporting cyber operations.

Implementing these demands will be difficult as identity programs and capabilities become more complex, especially because complexity can increase significantly, if not exponentially (Friedman, 2015).

IT system managers must be able to identify the systems precisely and instantly they have and who is utilizing them to safeguard them from cyber-attacks. It is impossible to determine whether an IT system has been modified or compromised by an adversary if the entities that compromise it cannot be properly recognized. Verifiable digital identities will relocate trust, allowing managers and users to go from ignorance to increased ability to conduct cybersecurity and cyberspace activities (Friedman, 2015).

1.8.4 Banking

As the world shifts to a digital paradigm, the banking industry has seen significant change because of the digital era. Traditional banks are undergoing constant transformation to improve their physical assets. However, during the past 10 years, the concept of the digital bank, which doesn't rely on intermediaries or direct client-company contact, has emerged, giving the possibility to do an online onboarding. This process is mandatory for a digital bank because all client contacts take place through an app or website. Having a strong digital business model, digital banks results in a strongly supportive attitude regarding the establishment of digital identity systems.

Traditional banks are constantly observing the development of the digital identification scenario to recognize potential financial sector synergies. They are aware that cultural and technological changes are taking place, and some of them are beginning to put online onboarding solutions into practice. Traditional banks use "de visu" client recognition, in the agency, as the foundation for their onboarding

procedure. To meet market demands, however, a growing number of conventional banks have begun merging "de visu" recognition with electronic processes.

The innate characteristic of digital banks and the earlier effort that is being put by traditional banks, can be considered as the first step in creating an internal digital identity that will be issued and controlled by the bank. Banks give each customer a digital identity so they may conduct online operations. In most cases, this identification is also required for offline operations carried out by agencies.

Different methods, including bank transfers, video selfies, and digital identity systems, are available for the remote identification process. Digital banks have a very favourable attitude toward public systems for digital identification, as the ones in Italy where several banks permit customer identification through SPID.

1.8.5 Insurance

The insurance industry is made up of businesses that provide risk management through insurance contracts, although not all insurance businesses provide the same service or serve the same audience. In this regard, it is important to distinguish between traditional insurance providers—who provide a range of insurance services like life, health, property, and accident insurance—and online providers, who typically concentrate on services that are less crucial, like property and accident insurance for cars, and handle all user interactions through an online channel.

The onboarding process typically concludes with the customer purchasing a product and receiving access information to the personal area. The customer is then taken to the business website. Numerous checks are made on the customer's personal information supplied throughout this process, most notably the OTP verification of the customer's email address and/or phone number. By creating a personal space, which is required by sector regulation, these verifications attempt to open up a secure line of communication with the customer. Given the lax identity checks made, the real cost of onboarding is quite cheap, and a potential further expenditure seems unwarranted given how crucial the procedure is.

The majority of insurance businesses do not invest in identification because consumers almost never conduct business online and the first client recognition is done "de visu" by agents. When a customer wants to cancel a significant request from their personal area or does an action that requires a higher LOA, such as purchasing life insurance, a real online identification is carried out. In these circumstances, an additional recognition phase is required, during which the client is typically asked to provide a facial image and an identification document. Online insurance providers include a straightforward identification procedure that charges less expense for the business.

1.9 Types of Data

The owner's photo, name, date of birth, and other personal data are typically stored in the identification. However, as technology advances, a new concept of Electronic Identity Document (e-ID) has emerged: it consists in transposing the same identity in a smart card where the owner's data can be stored digitally, including new features such as facial and fingerprint information for recognition. Furthermore, it includes more complex security measures such as personal information encryption and citizen access to online services. (Waldmann et al., 2012; Páez et al., 2020).

The set of traits that make up all the data needed to identify any entity can be permanent, like a person's birthdate, transient (like an address), or long-lasting, like a social security number (Dib and Toumi, 2020).

In 2016, the World Economic Forum put up a taxonomy of qualities that considers the type of data and entity represented. the following three categories of attributes:

- Inherent: innate to an entity and not determined by connections to other things (e.g., age, height, date of birth and fingerprint).
- Accumulated: built up gradually over time. Over the course of an entity's existence, these characteristics could alter often or develop (e.g., health records, preferences, and behaviours).
- Assigned: affixed to an entity yet unrelated to its fundamental characteristics. They are subject to change and show how an entity interacts with other bodies (e.g., National Identifier Number, telephone number, email address).

At least one attribute must be distinct or unique to provide individuation or individualization between records in order to query the digital identity database and retrieve the record. "*Identifiers*" are these distinctive characteristics that point to a digital identification record (Wayman, 2008). As the number of identity records increases, the need for unique IDs for each identity in the system creates a more complicated problem. Names, numbers, and, increasingly, biometric data are all common identifiers.

An attribute can be helpful in an identity management system even if it is not an identifier. It is possible to restrict access to a record or confirm that both parties agree on whose identity in the database applies if an attribute, which need not be distinctive, is difficult to create or a secret between the system and the individual to whom the record applies. Such a characteristic is known as a "*verifier*" (Wayman, 2008).

IBM¹ outlined "three main ways to identify a terminal user" in 1970:

- by what he knows or can recall
- by a possession
- by a physical trait

¹ IBM, "The Consideration of Data Security in a Computer Environment", 1970, tech. report G520-2169.

This concept was created in the context of access control to computer data records, and it gradually evolved into "what you are, what you know, and what you have" throughout the 1970s (Wayman, 2008).



Figure 1.1 Types of credentials (World Bank Group, 2016)

The US Department of Health, Education, and Welfare (HEW) outlined the following characteristics of the ideal Standard Universal Identifier (SUI)² in a report from 1973 (US Dept. of Health Education and Welfare, 1973):

- Uniqueness: only one SUI per person is allowed, and each person is only allowed to have one SUI.
- Permanence: it can't shift during the course of a person's life.
- Ubiquity: SUIs must be distributed to everyone in the population.
- Availability: they must be simple for anyone who wants them to obtain or verify.
- Indispensability: each individual must recall and accurately record their SUI.
- Arbitrariness: there must be no information in the SUI.
- Succinctness: it ought to be as brief as feasible.
- Reliability: it must be built with an error-detection mechanism.

To sum up, if the entity represented is an individual, the different type of data that may be included are (Mastercard, 2019):

- Biographical data (e.g., name, date of birth, address)
- Biometrics (e.g., fingerprint, face, voice)
- Personal unique identifiers (e.g., passport number, social security number)
- Certifications (e.g., doctor, pilot, university degree)

² US Dept. of Health Education and Welfare, "Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems," (1973).

- Dynamic data from (e.g., financial institutions, retail, mobile) interactions.

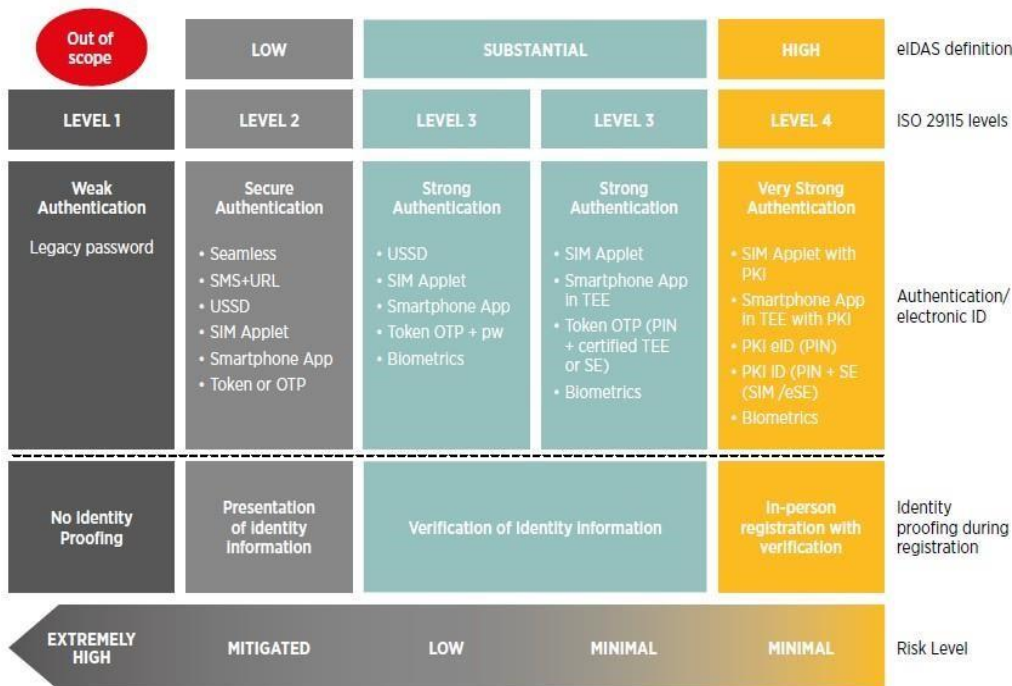
1.10 Level of Assurance

A key feature of all modern identity schemes is that the information needed to establish identity at the time of a transaction varies depending on the requirements of the transacting entity (Sullivan, 2018).

When a person identifies or authenticates herself using one or multiple identity attributes, the degree of confidence that she is who she claims to be depends on the degree of security assurance provided and the context in which the information is captured, referred to as the level of assurance (LoA). The level of assurance (LoA) in an identity transaction, according to the World Economic Forum of 2016, is *"the degree of certainty that the transacting parties have in the veracity of the identity being offered"*. LoAs are crucial for access control and reducing identity theft because they rely on how strong the identification and authentication processes are. The likelihood that service providers may depend on a compromised credential during a transaction decrease with increasing LoA. The level of assurance (LoA) for the identity proofing phase depends on the technique of identification, including the volume of personal data and attributes gathered about a person during enrolment and the level of assurance with which these qualities are determined (i.e., whether they are validated).

The reliability of the technology, the authenticators, and the authentication factors utilized all play a role in how strong an identity credential is. Not all transactions will necessitate the maximum level of LoA; rather, the higher the risk of the transaction, the higher the LoA must be. Different sorts of transactions will necessitate various LoAs. Single factor authentication (such as using an ID number or knowing a password) is frequently insufficient to accurately authenticate users or confirm their identities. For some applications (such as checking a social network profile), this level of risk might be acceptable, but for higher security transactions (such as claiming benefits or signing a legal document), it might be necessary to add more aspects of authentication to the user's credentials. These factors must be robust and secure. The possession of a secure device, such as a physical token, a mobile phone, or a smartcard allows for secure authentication and can be complemented by a personal identification number (PIN) or attribute (such as a biometric feature or behaviour) in order to provide stronger security (GSMA, Secure Identity Alliance and World Bank Group, 2016).

Levels of Assurance



Key: OTP = one-time password; PKI = public key infrastructure; (e)SE = secure element or embedded secure element (a tamper-resistant hardware platform); TEE = trusted execution environment (a secure area of the smartphone); USSD = unstructured supplementary service data ("quick codes"). Note: NISTIC 800-63A draft standard guidelines on identity proofing also allow for virtual-in person proofing and enrollment transactions²⁵

Figure 1.2 Levels of Assurance (World Bank, 2016)

1.11 Models

Digital identity system usage is on the rise in both public and private online environments. While the business sector (banks, travel agencies, etc.) may also be interested in protected solutions strongly tied to the civil identity, the eID ecosystem is thought to be a catalyst for better e-Government adoption by citizens in the public sector. A long-term strategy has been in place in the European Union over the past few years, and it led to the approval of the Regulation on Electronic Identification and Trust Services (eIDAS), in 2014 (Khatchatourov, Laurent & Levallois-Barth 2015).

There are five different types of digital identification models, according to Gartner:

- **Social ID:** a dataset that is added when a person registers on a social network; it has a low level of assurance, is updated frequently, and can be used on other platforms. Social networks are mentioned; for instance, Facebook Login enables account connectivity across several platforms. It enables two-way interaction, which entails expressing gratitude for the service by sharing and liking favourable experiences on social media. Additionally, by connecting the individual with his or her preferences, behaviours, and qualities, it also serves marketing purposes.
- **eCommerce ID (for marketplaces):** as the previous, but for marketplaces.

- **eGov ID:** an identity system created and disseminated by governmental organizations that recognizes individuals uniquely. On the other hand, they demand a high level of security (trust), and occasionally a digital credential is linked to a physical one (such an ePassport or smart card), necessitating identification verification based on several documents. National eID cards, ePassports, and licenses are a few examples. National and international organizations that manage the eIDAS regulation process are present across Europe. Enhancing confidence and safety for electronic funds transfers and interactions with the public sector, it governs the parties participating in electronic transactions and digital signatures.
- **Financial ID:** dataset collected by a bank or a financial institution. This model has emerged as medium-to high assurance Identity Providers. Unfortunately, many banks remain closed off to external service providers and digital services, even if there are cases in which the financial identity is used to sign on government services, for example, in markets such as Denmark and Sweden.
- **Mobile ID:** using SIM card as secure element, Mobile Network Operators (MNOs) are investing in digital identity as a critical aspect to identify mobile subscribers (via SIMs and eSIMs). MNO identity assurance varies from low to medium, in countries where the creation of the account requires minimal verification, to high, in countries in which it requires a valid government ID for issuing a SIM card. An example is the GSMA Mobile Connect is an initiative regarding a new service that enables people to identify and authenticate themselves using their mobile phone, leveraging on the use of mobile devices.
- Over the past few years, regulatory interventions and technological innovations have paved the way for the development and deployment of digital identity systems, but it was the health emergency with its lockdowns that brought about the step change we are witnessing today. A key dimension for understanding the potential use of digital identity is the level of data assurance, or **Level of Assurance (LoA)**, determined by the degree of reliability of user identification and authentication processes, which is strongly interconnected with the criticality of the different services accessible through digital identity. On the basis of these parameters, five digital identity models were identified by the Observatory: on the one hand, Social ID and eCommerce ID systems, characterised by a medium-low LoA that allows access to services with a low level of criticality; on the other hand, trusted systems such as Financial ID, Mobile ID and eGov ID, with a medium-high LoA that opens up opportunities for enhancement in application areas where secure user recognition is required. Focusing on trusted models, Financial ID and Mobile ID have a more business-oriented connotation, with a rich data set and a smoother user experience that make these models attractive to both the user and the service provider. Slightly different is the case with eGov IDs, which in many cases struggle to find a strategy to exploit their hitherto unexpressed potential. In fact, the 'doors' that could be opened with these trusted, certified, and secure 'keys' are many: from opening a current account to signing a contract for a telephone service, via consulting one's health records (Osservatori.net, 2020).

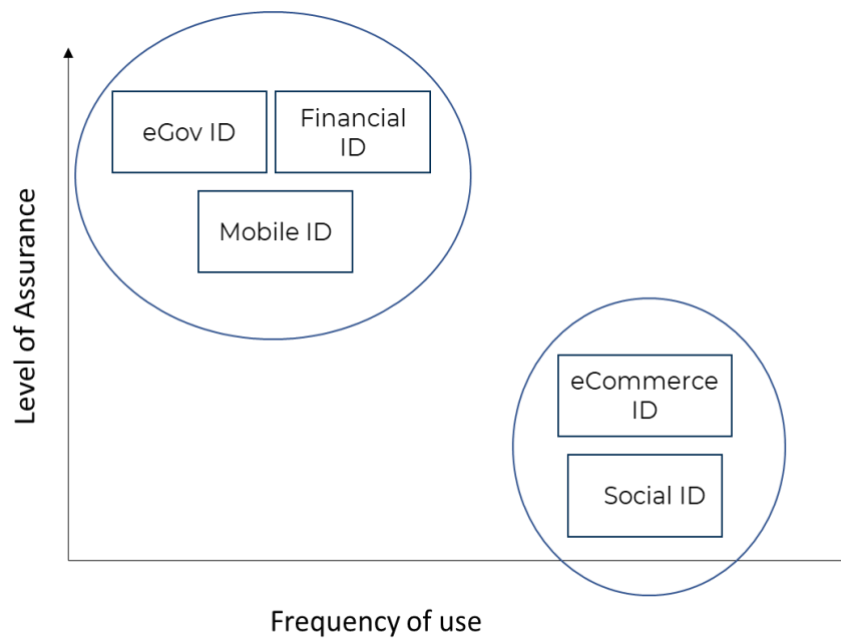


Figure 1.3 Models of Digital Identity

1.12 Digital Entities

It is crucial to accurately identify the subject or entity in an Identity Management System (IDM), which could be a person (citizen or employee), a group of people, an organization (legal entity), a virtual object (such as a computer process, application, or text file), a tangible object (such as electrical appliances and computers), or any other entity that needs access to a specific resource (Jovanovi et al., 2016).

Even if it is simpler for people to associate identity with humans, it is important to distinguish between digital identification systems for people, other things, and legal entities when thinking about them (Arner et al., 2019).

For instance, identity management of things is a key component of the Internet of things (IoT), and numerous academic studies have offered methods and standards to address the IDM's various issues (Hu et al., 2018; Ning et al., 2019). The function of IDM is expanding to include sensors, actuators, and smart devices as a result of the IoT sector's rapid expansion. The primary responsibilities of the position are to monitor sensors and allow access to IoT services and apps. According to Dhelim et al. (2018), the IoT has dramatically changed the era of digital identity from one that was user-centric to one that was entity-centric. As a result, identity management now needs to be focused on all entities using the IoT network. The IoT identity management must be able to handle interactions and data sharing between people and machines, devices and applications, and devices and other IoT entities while taking into account their relationships. This is because all IoT entities share the same interaction ecosystem (Bouras et al., 2021).

1.13 Main Actors in Identity Management

Traditionally, an "identity ecosystem" had only two participants: two people who recognized each other. There are numerous actors in today's digital identity ecosystem (World Economic Forum, 2018).

In contrast to historical circumstances, in which governments had the sole right to manage information about citizens' identities, it is now clear that governments are not the only parties involved (Lips et al., 2009). A digital identity system involves many stakeholders, each of whom plays a different role in the process, depending on the national context, system architecture, and the type and purpose of the digital identity (World Bank Group, 2016).

As well as connecting with government entities online, consumers and companies are increasingly making purchases of goods and services online. For counterparties to communicate with one another and for payments associated with such transactions, there needs to be a trustworthy environment. However, customers may find it difficult or expensive to access "know your supplier" (KYS) information about businesses. Because of this, it is challenging for customers to research the legal standing of potential providers. Businesses are more adept at managing the data of their clients and suppliers. They are aware of their expanding obligations regarding the customer and supplier data they possess, including their obligations under the law and the "know your customer" (KYC) requirements to minimize the risk of money laundering (Gerard Hartsink, 2018).

The following are the predominant roles:

1. **End users**, which are common people and customers who use their identities to communicate with other actors. They freely sign up, verify their identity using credentials, and are then granted access to a set of digital services.
2. **Identity Providers (IdPs)**, which connect with Service Providers (SPs) to obtain the necessary data and verify user data before distributing and managing digital identities. Users are registered, and documents or credentials are issued, to build their digital identities. On behalf of the users, they typically also store and handle data and credentials. National identification authorities are frequently the IdP in the public sector. Service Providers (SPs) are usually digital IdPs in the private sector (World Bank Group, 2016).
3. **Attribute Provider (or Qualified Attributes Operator)**: a company that has verified user data and either verifies or provides these attributes to a third party with the user's permission (World Bank Group, 2016). There is frequently overlap between IdPs and attribute providers. However, in some cases, different actors provide attributes at the request of identity providers or relying parties (e.g., university could be an attribute provider that certifies to a third party that a person has a degree).
4. **Identity Verifier (or Authentication Provider)**: an entity in charge of verifying the user's right to access a service or benefit based on the credential provided, controlling the information verification phase. Typically, service providers oversee authenticating users in the private sector.
5. **Service Provider (SP)**: the company that provides the service to the end user. These could be government agencies or private service providers. SPs may be digital identity (trust)

and authentication providers themselves, or they may outsource these functions to other agencies. In the latter case, the service provider, known as the Relying Party, relies on another party to verify the user's identity.

6. **Technology Provider:** it provides and manages the entire system's technological infrastructure.
7. **Information Provider:** the institution that verifies the recognized document used to identify the user.
8. **Regulatory agencies and institutions:** these are the entities in charge of ensuring that digital identity and authentication providers adhere to legal standards and best practices for the collection, storage, and use of personal data. National and supranational authorities such as the European Data Protection Board and eIDAS requirements are examples.
9. **Standard-setting organization:** it is an organization that develops protocols for digital identification and authentication in order to improve interoperability and build open and scalable solutions. It includes both public sector organizations like the American NIST and private and non-profit organizations like the ISO standard body, FATF, the Open ID Foundation, FIDO Alliance, GSMA, and Secure Identity Alliance (World Bank Group, 2016).

Focusing on the role of the Identity Provider, there are four types of IdP based on functionality (H. Koshutanski, M. Ion, and L. Telesca, 2007):

- **Credential Identity Service:** for user authentication, this type of IdP uses credentials as user identity. Credentials are proof of user identity; the first and most widely used credential is a certificate based on ITU-TX.S09.
- **Identifier Identity Service:** an identifier is a representation of a user, such as a name, an email account, or an ID-Card Number. Identifiers can be assigned to users directly or indirectly; an example of an indirect identifier is the user's temporary identity; when the user requires cross-domain access, the IdP always generates this type of identity and assigns it to the user.
- **Attribute Identity Service:** an attribute is information that can be used to describe a user's identity; it could be part of a credential or the process of identifying a user, such as name, address, and contact information. The IdP should provide a mechanism for user identity attribute verification, which necessitates an interface with the government supervision department.
- **Pattern Identity Service:** pattern identity refers to the IdP's use of patterns, reputation, honour, trust records, and history access records to describe or identify user identity. To maintain computer security, some types of special pattern identity service can be used, for example, the characteristics of an attacker model can be used to identify the hacker attack.

The distinctions between these four types of IdP identity service are subtle (this is why there is overlapping with some of the roles above described, such as Attribute Provider, in the case of an Attribute Identity Service, for instance). A credential always has a corresponding identifier, which will involve both credential identity service and identifier identity service. What type of identity service should be used, and whether two or more services should be combined, is always determined by the

level of trust required by the IDM. For example, identifier identity service is sufficient for web access and other common services, but for high-level services such as online banking, the appropriate credentials are also required (Cao, Yang, 2010).

1.14 Archetypes

Identity systems today – and those that will emerge in the future – are typically divided into three types: centralized, federated, and decentralized. As the names suggest, it is their fundamental structure that distinguishes them, with implications for adoption and trust levels, as well as advantages and challenges for individual users. In the most traditional and widely seen centralized archetype, institutions such as governments or businesses establish and manage identities and related data in their own systems, whereas in the second, federated archetype, this role is shared by multiple institutions. The newest, decentralized archetype, which is mostly still in the pilot stage, seeks to give individuals greater control over their own identity data (World Economic Forum Report 2018).




| SYSTEM ARCHETYPES |  CENTRALIZED |  FEDERATED |  DECENTRALIZED |
|------------------------------------|--|--|---|
| DEFINITION | • A single organization establishes and manages the identity | • Different stand-alone systems, each with its own trust anchor, establish trust with each other | • Multiple entities contribute to a decentralized digital identity; user controls sharing of identity data |
| EXAMPLES | Government electoral roll, bank, social media platform | Sweden's BankID, GOV.UK Verify | Government of Malta education pilot, city of Antwerp pilot |
| LEVEL OF ADOPTION AND TRUST | Adoption dependent on value; trust dependent on system owner and identity proofing | Adoption dependent on establishing trust relationship; trust dependent on identity proofing | Adoption currently in early stages (pilot, proof-of-concept). Trust dependent on trust anchors and attestations |
| STRENGTHS | Can be built with specific purpose in mind; potential for organizational vetting of identity data | Users can access a wider range of services; efficiency for organizations | Increased user control and reduced amount of information collected and stored by organizations |
| CHALLENGES | Generally low user control; centralized risk and liability; potential for abuse | Generally low user control; high technical and legal complexity | Governance model, acceptance and participation is complex; evolving landscape; complex liability |

Figure 1.4 Three identity system archetypes (World Economic Forum, 2018)

1.14.1 Centralized

The system's owner gathers, keeps, and makes use of each person's identity and the data that goes along with it. Typically, a user creates a digital account and stores it in a service provider's database.

Depending on the rules of the service provider holding the user's account, the quality of the data in these identity systems varies. For instance, highly regulated industries like government and finance have stringent identification verification procedures. However, it is simple to create several or even malignant identities in other systems, such as some social networking platforms. Users' privacy may be violated since data are handled by a third party, and their online activities may be linked and eventually tracked (Cao and Yang, 2010). The SP is in charge of managing identities, providing credentials, and performing authentication in its own repository (Pöhn and Hommel, 2020). A token issued by the identity provider following successful authentication must be presented by the user to the service provider, in order to use a service offered by that provider (Dib and Toumi, 2020).

The centralized model fits the needs of managing numerous users. However, it has a number of drawbacks, including the user losing control of his identity data and a number of privacy and trust issues because identity data is stored in the identity provider's internal repository (Modugula et al., 2018). Indeed, centralized architectures may represent "honeypots" of individuals' identity data, which are attractive targets for hackers, and they may concentrate risk and liability with the system owner because the user's identity-related personal and confidential data is always stored and controlled by the organization.

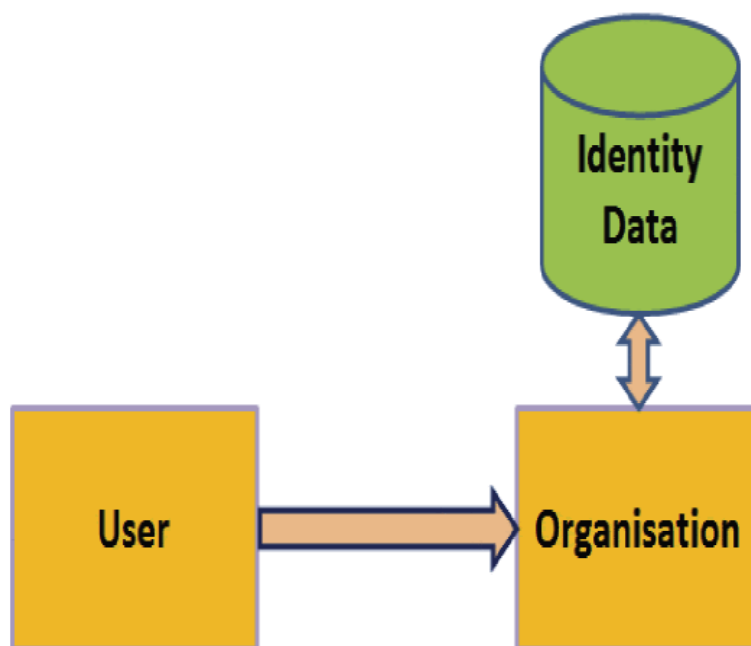


Figure 1.5 Centralised Identity Management Model (IDM 1.0) (Nitin Naik, Paul Jenkins, 2020)

1.14.2 Federated

Mutual trust between two or more centralized systems leads to the creation of a federated identification system (Amoli et al., 2019). That is typically related to developing common standards like eIDAS (Lin, 2020). Users frequently appreciate the ease of use that federated identities offer when

logging into several services on various platforms. They depend on the belief that the user's identity has been independently verified. Since most online users have a Google or Facebook account, this login method is commonly used. But using that technique, identity service providers were able to track users' activities and combine that information with identification data, giving them access to a lot of sensitive information (Dib and Toumi, 2020).

In a federated approach, protocols between SPs are defined, along with regulations and technological standards, to allow identities from various identity domains to be recognized across all domains. Users from one domain can securely and conveniently access services in another domain without the need for additional authentications thanks to a mapping between distinct IDs held by the same user across different domains. Users can access all services in the federated domain with just a set of identifiers and credentials (De Angelis et al., 2016). Using federated identity management, users would only need to sign in once to access a variety of trusted websites or service providers. Users could also have more discretion over how and when service providers disclose their qualities across domains, giving them more control over their personal data (Shim et al., 2005).

Many federated identity management systems are in use. Although people frequently appreciate the easy access to many systems that this archetype might offer, the implementation may be constrained by the difficulty of creating individual trust relationships amongst system owners. As with centralized systems, the degree of identity verification and data vetting varies depending on the system owners involved. In comparison to isolated centralized systems, federated networks can give users access to a greater variety of transactions with a single set of credentials. Users benefit from improved convenience thanks to this compatibility. The system's numerous owners may be able to better manage user identities and access with its aid. Federated systems, like centralized ones, might not allow users much control over how their data is used. The probable requirement for legal agreements, including the division of risks and obligations, as well as shared data and technical standards, creates complexity for the system owners. Due to its complexity, installation may be costly and prevent the system from incorporating many of the services that users would like to use (World Economic Forum Report 2018). Definitely, the two main problems this federated IDM paradigm addresses are:

- by adding a third party called the Identity Provider (IDP), it eliminates the organizational burden of managing identity and credentials securely, which is an additional duty on top of the regular company activities.
- by providing a Single-Sign On (SSO) option, it relieves users of the responsibility of managing several identity-related credentials for numerous systems (N. Naik and P. Jenkins, 2016). However, this IDM approach has a similar problem in that the user has no control over the vast amount of identity-related personal and confidential data that is held by the IDP (N. Naik, P. Jenkins and D. Newell, 2017).

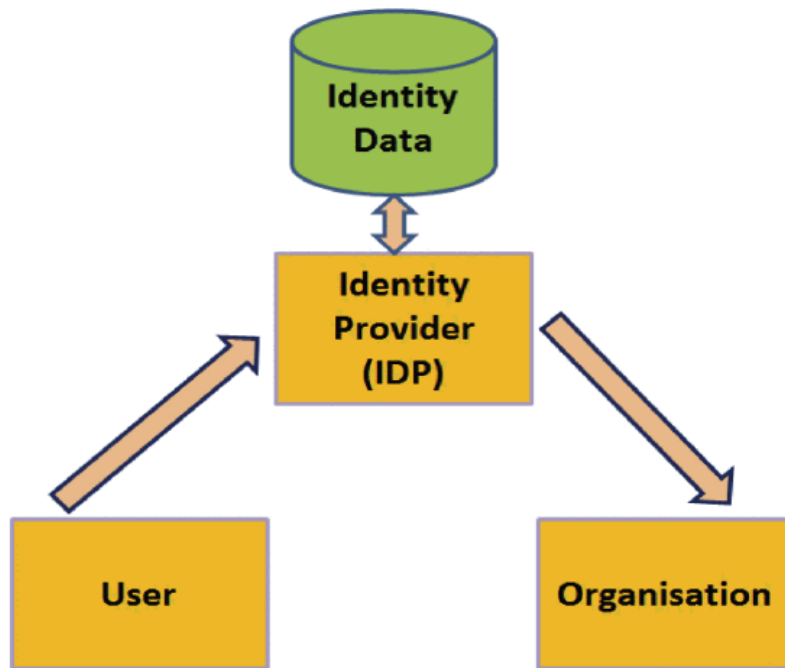


Figure 1.6 Federated Identity Management Model (IDM 2.0) (Nitin Naik, Paul Jenkins, 2020)

1.14.3 Decentralized

Decentralized identity management solutions don't rely on a single or group of system owners to create and maintain IDs. Instead, they typically comprise of a digital device that belongs to a single person and an identity data storage that is also run by the single person. This data store, which is frequently the user's device memory or cloud storage, contains certifications from both conventional trust anchors like governments or banks and additional trust anchors like employers, stores, media sources, or personal connections. The decision to share an attestation or data attribute, as well as with whom, is made by the individual (World Economic Forum Report 2018).

This different archetype is made possible by giving the entity control over as much identity infrastructure and data as possible and by relying on trusted decentralized tools and techniques, such as secure distributed ledgers and cryptographic algorithms, to generate and store mathematical proofs about the accuracy of identity attributes and the data they are associated with. The identification traits are instead primarily stored in a private data storage, and their life cycle is managed by a digital device. As long as the entity in possession of the identity maintains control over it, a decentralized identity is intended to be secure. This indicates that the entity takes ownership of its identity data. The entity develops its own digital identity in a decentralized identification environment. Typically, this starts with the development of one or more distinct IDs, followed by the addition of real and verifiable features. After completing this, the entity can gather credentials from reliable anchors and make them readily available as needed. A variety of cryptographic techniques, including digital signatures, can be used to demonstrate the legitimacy of a credential. Currently, such digital credentials that may be cryptographically confirmed are referred to as Verifiable Claims or Verifiable Credentials (VCs). A VC not only gives a user considerably more control over the qualities that make

up their identity, but it also makes using their digital identity much simpler. The entities themselves produce decentralized identifiers (DIDs). Therefore, no centralized registry, identity provider, or certificate authority is dependent on DIDs. A distributed ledger must be employed to decentralize DIDs (Sunyaev, 2020).

Since it offers a ready-made infrastructure for handling data in a decentralized but reliable way, blockchain (as will be analysed in next paragraphs) can be a strong distributed ledger for various aspects. Due to its decentralized nature, immutability, and transparency, the blockchain can be utilized as a distributed register for decentralized identifiers with ease. A reliable source of historical information in terms of cryptography is VC. Personal devices, such a smartphone or laptop, or some secure solutions made available by third parties can be utilized to store such sensitive information. These devices are currently known as digital "wallets" (Patil et al., 2019). They might appear as software, hardware wallets, cloud services, or mobile phone apps. It is necessary to initially establish a connection between the user and the service provider. The user must be informed of a DID. The user can confirm the service provider's identification in this way. In order to confirm that the service provider is speaking with the identity owner, this latter must additionally get the users DID. Any VCs can be delivered, received, and confirmed once a secure communication channel has been created between the user and service provider (Dib and Toumi, 2020).

The control and transparency that a decentralized system gives each user — management over what identity-related information to reveal, with whom to share it, and for how long — are its greatest strengths. Since individuals are able to govern and expect greater personalisation and transparency, decentralized systems can likewise promote a more engaging digital consumer experience. Through verifiable claims, they can help promote interoperability between current, separate systems. Traditional trust anchors, including banks and governmental organizations, will need to provide attestations to the data store for a decentralized identification system to allow a person to undertake higher-risk transactions. Currently, many of these trust anchors control centralized systems where they control the user relationship. Although it is difficult to alter the nature of this relationship and who owns the valuable data, some established trust anchors are doing so. This decentralized architecture will need to be sufficiently trusted by service providers and relying parties for them to embrace it. Although the technologies and standards needed to enable decentralized identity systems are gaining ground quickly, most current operating frameworks and legal frameworks were created for centralized systems, thus they will need to change in order to support and oversee decentralized systems. Liability determination for potential violations or abuses may be particularly difficult (World Economic Forum Report 2018).

1.14.4 Self Sovereign Identity (SSI)

Recently, no model was able to overcome the problem of an identity's sovereignty and storage-control of the personal and private data that go along with it. Security, privacy, and protection are some of the linked issues with respect to identification that have been impacted by this sovereignty issue (P. Windley, 2017). Whereas the definition of the term "Self-Sovereign Identity" is still ambiguous, some of the idea's fundamental characteristics have become clear. The users' ability to manage their own

digital identity should come first. A user's self-sovereign identity is theirs to own and govern, free from the need to submit to any outside administrative authority or worry that it might be revoked. Without relying on a central repository of identity data, individuals and organizations can keep their own identity data on their own devices and communicate their identity to others who need to validate it.

Due to its independence from any specific silo, it offers consumers complete control, security, and data portability. According to the Sovrin Foundation (Andrew Tobin, 2017), self-sovereign identification is similar to the Internet for identities in that anyone can use it and make improvements to it (Lim et al., 2018). In essence, it is a system for managing identities that enables users to fully control and own their digital identities. In 2018, the World Wide Web Consortium (W3C) working group on verifiable claims stated that system users exist independently from services in a self-sovereign identity. This emphasizes the contrast to existing identity management, which either requires the user to create new digital identities at each individual service provider or relies on a few major identity providers, such as Facebook (Facebook Connect) and Google (Google Sign-In).

In his **Ten Principles of Self-Sovereign Identity** proposal from 2016, Christopher Allen outlined the specifications for a system that would use the self-sovereign identity idea. In a whitepaper, the Sovrin Foundation further divided these Principles into the three categories of security, controllability, and portability (Tobin and Reed, 2016). In its simplest form, security can be defined as the safeguarding of individual user data and the restriction of data exposure to that which is strictly necessary to carry out a certain purpose. A persistent identity was also mentioned as a security prerequisite. However, according to Allen, persistence in this situation shouldn't conflict with a "right to be forgotten". Since control and consent should apply to the removal of the identity as well as its formation and access, this right to be forgotten could also be categorized within the controllability category.

The identity's mobility is another crucial prerequisite for an SSI system, being independent of any specific identity supplier and enabling the user to use their identity wherever they desire. The verifiable statements are at the heart of the SelfSovereign Identity idea. The distinction between a claim and a verified assertion needs to be made in this case. A claim is nothing more than a statement regarding a certain topic. A credential, which some distinguish from claims (Sporny, 2018), lists several claims together with their meta data, such as the issuer and the duration of their validity. Verifiable claims are those that can be supported by the signature of an attestation issuer who has either made the claim themselves or can attest to its accuracy. According to Mühlen et al. (2018), an attestation can be thought of as a proof in the form of a signature attesting to a certain claim and meta data necessary for verification, such as name, validity period, and signing technique.

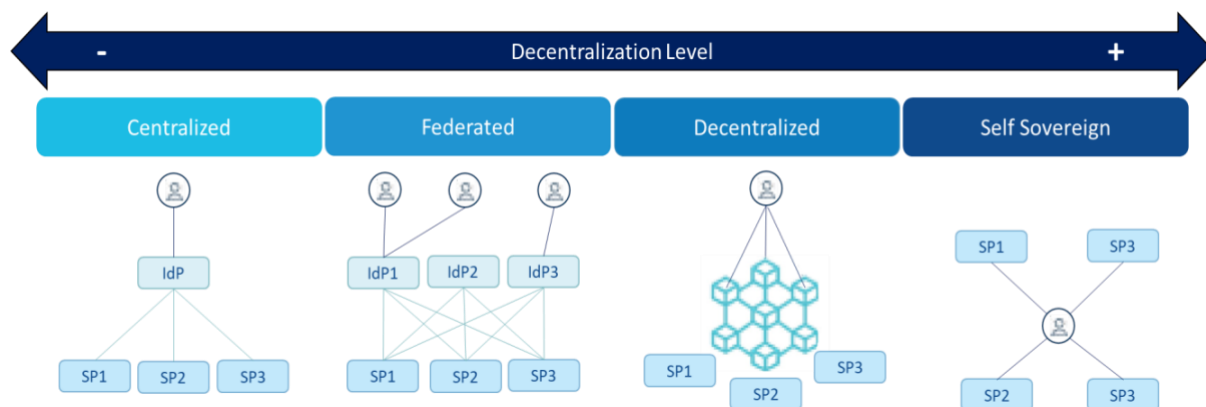


Figure 1.7 Types of ecosystems (Digital Identity and Blockchain and Distributed Ledger Observatory, 2020)

Along with maintaining identity ownership, SSI also keeps all personal data in a user-controlled digital wallet. The Digital Wallet functions similarly to a physical wallet by storing all digital credentials as tangible objects, however these credentials are digitally signed, verifiable, and issued and verified much more quickly than their physical counterparts (A. Tobin and D. Reed, 2016). It is also a peer-to-peer paradigm, meaning there is no intermediary between the user and the SP.

Since the user-owned and -controlled device that the user controls house the Digital Wallet, which stores all identity-related personal and confidential data, SSI takes on three crucial roles: issuer, holder, and verifier. Credentials are made and given to a holder by an issuer. When necessary, the holder can share the credentials with a verifier after receiving them from the issuer. A validator accepts and examines the credentials that a holder has produced. This SSI implementation is based on the **Verifiable Credential (VC)** and **Decentralized Identifier (DID)** standards, which are suggested for developing a cryptographically verifiable digital identity that is entirely controlled by its owner (Sovrin, 2018). Similar information to that of a physical credential in the real world is represented on the Web by a VC. In contrast to other ephemeral identifiers like a cell number, IP address, and domain name, the DID is a permanent, universally unique identity that cannot be removed from its owner who has the associated private key (Sovrin, 2018).

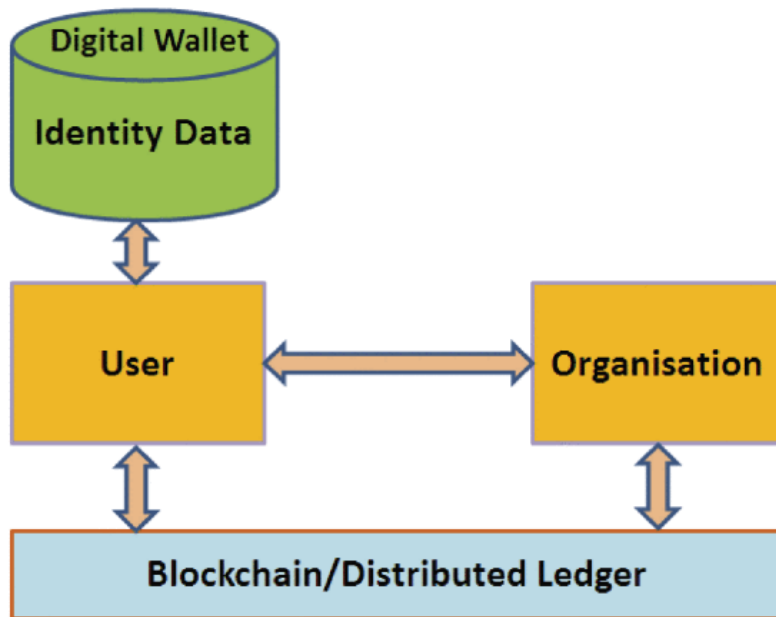


Figure 1.8 Self-Sovereign Identity Management Model (IDM 3.0) (Nitin Naik, Paul Jenkins, 2020)

1.15 Phases of the process

The identity lifecycle is a process that begins when a person asks for a digital ID and ends when the record is deleted and the ID is declared invalid due to a person's death, their request for deletion, or another event (World Bank Group, 2018). According to Nyst, identification, authentication, and authorization are the three functions of digital identity schemes that are all carried out digitally.

- Identification is the process of creation of the identity. Currently, this frequently entails looking at "breeder documents" like passports and birth certificates, checking additional sources of information to confirm the stated identification, and sometimes obtaining biometric information from the person (Nyst et al., 2016).
- Authentication is the process of reaffirming a person's identity after it has been confirmed through identification. To prove that the person is the owner of and in control of the asserted digital identity, they often present or use an authentication credential that was connected to the identity during the identification process (Nyst et al., 2016).
- Authorization is the process of deciding which actions or services may be accessed based on the claimed and verified identity (Nyst et al., 2016). A person who has registered their biometric and/or demographic information with a digital identification system, for instance, will be permitted to access a government service once their information has been matched with their eligibility for the service in question.
- Although not a real phase, it is required to support the management of identification data and attributes. It refers to the requirement for users to update identity attributes, such as occupation, residence, and marital status, or delete (deactivate) a digital identity in

order to invalidate it for fraud or security concerns, or to terminate a digital identity in the event of a person's passing (The World Bank Group, 2018).

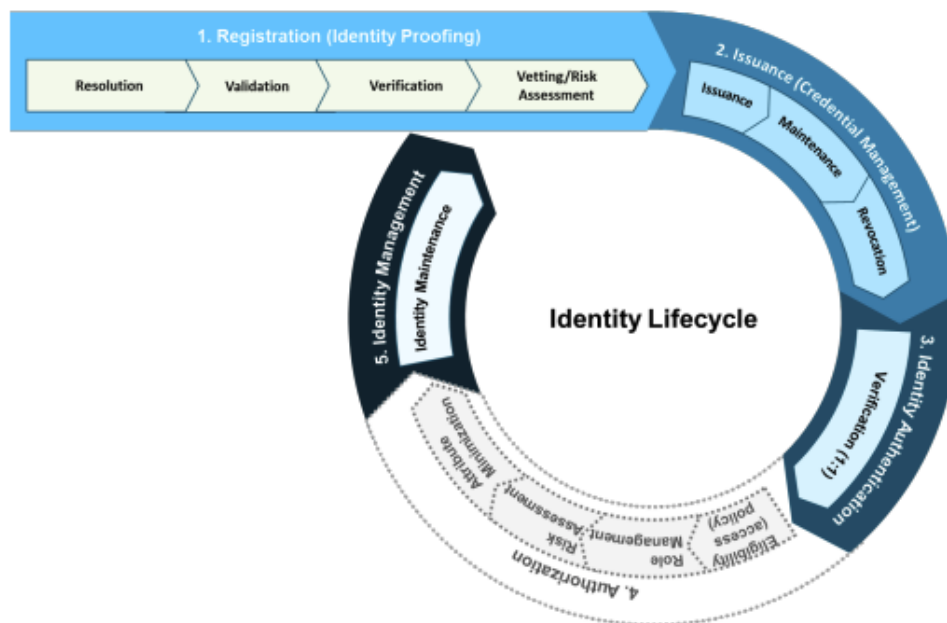


Figure 1.9 Identity Lifecycle (World Bank Group, 2018)

1.15.1 Identification

Identification is the process of identity creation. It corresponds to the registration phase for the user while the client onboarding procedure for the service provider. It is made up of:

1. **Registration.** The phase begins with enrolment, which involves gathering and documenting important identity attributes from a person who asserts a particular identity. These attributes may include biographical information (such as name, date of birth, gender, address, and email), biometrics (such as fingerprints and iris scans), and an ever-growing list of other characteristics.
2. **Validation.** Once a person has registered for an identity, that identity is next verified by comparing the attributes provided with the data already in existence. The validation procedure determines whether one or more of the following characteristics of the claimed identity exist:
 - *Existence/liveness:* It is existent at the time of enrolment (the enrollee is present and alive), and it is localizable (i.e., the person can be reached through their address, phone number, or email).

- *Uniqueness*: it can only be attributed to one person (i.e., the person is unique in the database). De-duplication is another name for this process, which can be carried out by combining a range of attributes (even though biometrics are currently the most accurate) (Gelb and Clark, 2013). The set of data attributes that best describes an individual and is often accessible via a national identity system constitutes a minimum set of unique identity traits. It is necessary for creating a digital identity that is shared by players within an ecosystem and across boundaries. It normally has a number of required qualities, but it may also have one or more optional attributes. The eIDAS Implementing Regulation (2015/1501) of the European Union, for instance, stipulates that the minimum data set of unique identity attributes for a natural (i.e., physical) person includes both mandatory attributes (current family name(s), current first name(s), date of birth, and a unique identifier which is as persistent in time as possible) and additional attributes (first and family name(s) at birth, place of birth, current address, gender). The state is responsible for making sure that when establishing a legal identity, a minimal set of characteristics that serve to identify the person in question must be provided, in compliance with the technical requirements, standards, and legal procedures. Additionally, it is advised that private sector organizations apply the same idea when developing user identities for online authentication so that third parties can confidently verify a person's digital identity. However, best practices suggest that just those properties should be needed for an online service's authentication that are sufficient, pertinent, and reasonable for granting access to the service. User data and privacy are at danger when attributes are used that are out of proportion to the use case.
 - *Linkages*: It can be connected to social identities already in existence, including those found in identity databases, civil registers, population registries, tax registries, property registrations, social security databases, police records, etc (World Bank, 2014).
3. **Verification.** The creation of a connection between a claimed identity and the actual person providing the proof (World Bank Group, 2018). When opening a bank account, asking for a loan, or engaging in other financial transactions, identity verification is a crucial step in making sure a person is who they say they are. While identity verification is a crucial security tool in the fight against new account fraud, it also aids financial institutions' Know Your Customer (KYC) and anti-money laundering (AML) initiatives, which evaluate and track customer risk (OneSpan, 2022). The process used at this stage will have an impact on the overall level of identity assurance. For example, the identity provider may require the users to confirm that the entered emails are their own or it may require a face-to-face meeting to confirm that the document they entered (which has already been validated) matches them.
 4. **Vetting/Risk Assessment.** Assessing the user's profile against a watch list or a risk-based model (World Bank Group, 2018). For those industries that are subject to rigorous restrictions, this phase is particularly important (AML, KYC in Financial services).
 5. **Issuance.** The first step in credential management is issuance, which involves producing and distributing physical or digital credentials such as decentralized identity proofs, e-passports, digital ID cards, and licenses. Therefore, to access the digital service, the user is given either physical or digital credentials, which may include:

- *Smartcards*: these cards include additional security measures and an embedded computer chip that stores digital credentials and/or biometric information. Near Field Communication (NFC)-capable SIM cards or contact/contactless cards can both be used as smartcards. In the absence of an internet connection or mobile network, data saved on a smartcard can be retrieved offline for authentication.
- *2D bar code card*: instead of or in addition to a chip, cards can be customized with an encrypted 2D bar code carrying a person's personal information and biometrics. The 2D bar code is a safe and affordable way to offer a digital identity and to use biometrics to identify bearers. In recent years, Egypt has used it to identify holders during the most recent elections. It has been widely used in Africa, Latin America, and the Middle East, including Lebanon, Mali, and Ghana (World Bank, 2016).
- *Mobile identity*: for a variety of online transactions, portable digital identification and authentication can be provided by mobile phones and other devices. To provide secure and convenient user identity and authentication for eGovernment (eGov) services and other public or commercial platforms, providers, for instance, can issue SIM cards with digital certificates or leverage other mobile network assets.
- *ID in the cloud*: some systems exclusively keep certificates and biometric data on a server, in contrast to portable credentials like smartcards and SIM cards. In this scenario, a physical credential might not be issued or might only be issued in paper form (like the Aadhaar program in India, which only generates paper receipts). An ID stored in the cloud will be safer against theft if it is stored in a tamper-proof environment for secure cryptographic key generation and management (GSMA, Secure Identity Alliance and World Bank Group, 2016).

1.15.2 Authentication

Authentication is the process of acknowledgment of the former identity that was established. It is the stage where a user provides evidence that he or she is the person who originally registered the account. Any piece of information that an authentication server accepts can be used as evidence of identity. One or more authentication elements can be used to identify the user (O'Gorman, 2003):

- **Inherence**: a quality that the client possesses (a characteristic, for example a biometric attribute).
- **Possession**: anything the client possesses (a physical device like a smartphone).
- **Knowledge**: Information the client is aware of (like a password).
- **Behaviour**: an action taken by the client (like a gesture).

According to Feng there are three categories of authentication: single-factor, two-factor, multi-factor, and biological identifications (Feng et al., 2017):

- **Single-factor authentication (SFA)**: Lamport (1981) was the author of the original remote authentication technique that relied on the user password. A password authentication

system based on the public key encryption technique was proposed by Harn, Huang, and Lai in 1989. The classic example of SFA is a PIN or password (Gunson et al., 2011).

- **Two-factor authentication (2FA):** in 1991, Chang and Wu developed two-factor authentication as a smart card. It is a remote password authentication technique based on the Chinese remainder theorem. In light of vector products, Tan and Zhu (2000) developed a remote password authentication method. By developing a dynamic identity technology that enables anonymous user identification, Das (2007) proposed a dynamic ID-based password authentication technique. Das and other researchers' programs were enhanced by Liao (2005), who also accomplished mutual authentication. By combining two distinct authentication components, 2FA may offer improved security when compared to SFA. The benefit is that if one of the components is compromised, security can still be maintained (O'Gorman, 2003). Along with the user ID and password required for two-factor authentication, users must additionally enter a unique code that they typically receive via short messaging service or another unique code they have beforehand (S. Ibrokhimov, K. L. Hui, A. A. Al-Absi, H. J. Lee, M. Sain, 2019).
- **Multifactor and biological identification:** by combining biometric authentication with the currently used two-factor authentication, the technology of three-factor authentication has gradually entered the sights of security researchers due to the universality, uniqueness, and stability of human biology. A fingerprint-based combined smart card that can use three-factor authentication technology for distant user authentication was first proposed by Lee (2002). A remote multifactor authentication system that can hide the user's identity was introduced by Bhargav-Spantzel (2007). Fan and Lin (2009) proposed the use of three-factor authentication, which has been shown to be incredibly secure, to ensure complete confidentiality of personal private. Three-factor authentication based on random numbers and one-way hash functions was proposed by Li and Hwang (2010). Three-factor authentication was proposed by Khan and Zhang (2002) as a method for achieving bidirectional authentication (Neuman et al., 2005; Dang et al., 2007; Xu, 2011).
- **Multi-Factor authentication (MFA):** is a secure authentication process that calls for several authentication methods selected from various credential categories. Similar to single factor, multi-factor authentication is being used more frequently to confirm users' identities when they access cyber systems and information. MFA provides a more effective and secure method of authenticating users by combining two or more methods of authentication (D. Dasgupta, A. Roy & A. Nag, 2017). In the beginning, accessing digital information and resources just required a single password. Initially, the individual was authenticated using just one factor. Due to its ease of use and simplicity at the time, Single-Factor Authentication (SFA) was largely adopted by the community (R. K. Konoth, V. van der Veen and H. Bos, 2016). But it was vital to develop alternate authentication strategies if we began sharing much more sensitive financial and personal information. Furthermore, the introduction of high-speed computing equipment made it simple to employ techniques like brute force to create millions of passwords each second. Multifactor authentication (MFA) security technologies are introduced to address these issues in order to thwart those assaults. The user must provide more than one credential via the MFA technique in order to be authorized. Depending on the application's security requirements, several authentication factors or credentials may be required. The user must sequentially provide the security system with numerous authentication factors. To

prevent compromising one of these credentials from compromising the entire security system, these criteria must be separate (J. J. Kim and S. P. Hong, 2011).

In multi-factor authentication, several different categories of authentication factors are employed, including:

- knowledge factors, also known as knowledge-based authentication, these procedures frequently need a password or the solution to a secret question.
- possession factors, a hardware item, such as a security token or a mobile phone, is often required for customers to log in with.
- inherence factors, these are the criteria for biometric validation (i.e., biological traits of the user). These are referred to as biometric factors and include fingerprints, hand geometry, facial and iris scans, voice and facial recognition, as well as additional characteristics depending on user behaviour, or "behavioural biometrics."
- location factors, an authentication factor is the user's current geolocation. Usually, GPS is used to determine where something is.
- time factors, sometimes used as an authentication factor is the current time. It frequently appears beside the location. For instance, because it is physically impossible, if an ATM card is used in America and then in Russia 30 minutes later, it is reported as suspicious.
- behavioural factors, feature includes user-specific behavioral habits including typing speed, finger pressure on the keypad, voice intonation, and mouse and swipe motions. Behavioural biometrics is what this is known as, and it is typically thought of as less intrusive and more secure than physical biometrics.

Data protection is improved thanks to multi-factor authentication techniques, which increase system security significantly above single-factor password authentication (Mitek, 2021).

1.15.3 Authorization

Authorization is the process of verification of the permission connected to a person's identity, which corresponds to the time when the user has the option of using a service or taking action.

After a person's identification claim has been verified and the access privileges of a relying party or service provider have been established, authorization takes place. Access rights must be connected to the identity and be in accordance with the person's connection with the relying party, independent of the identity provider (The World Bank Group, 2018).

The procedure corresponds to the phase of identity privilege verification and, as a result, with the granting of the ensuing authorization to use particular services or take particular activities (The World Bank Group, 2018b). The authentication process is typically controlled within the context of a firm using solutions for Identity and Access Management or Privileged Access Management (Witty et al., 2005).

1.15.4 Identity Management

It is necessary to enable the management of identity data and attributes even when it isn't a true phase. Users must update identification details including their job, address, and marital status. They can also destroy (deactivate) a digital identity to render it invalid due to fraud or security concerns or terminate a digital identity in the case of a person's demise (The World Bank Group, 2018). The issues of identity management include how to keep up-to-date databases accurate to represent significant life events (such as birth and death), how to employ data analysis to improve the system's performance (including efficiency), and how to preserve privacy and security restrictions (World Bank Group, 2018).

1.16 Data Privacy

The issue of privacy has been a pivotal point in digital solutions for decades. The difficulty in managing privacy in a digital solution is due to the absence of a guarantee, in compliance with the regulations in force, to ensure the real privacy of data. For this reason, the issue of data privacy shouldn't be handled separately. To aid prevent privacy vulnerabilities, privacy should be made the standard and integrated into the design and operation of IT systems and business operations. To meet this need, privacy by design is a real solution. Privacy by design means a methodology for incorporating fundamental privacy concepts into technology itself from the outset. In the case of digital identity, it mandates that data minimization guidelines be incorporated into the engineering and design of digital IDs "by default" (KPMG, 2022b).

Additionally, it involves being proactive rather than reactive, foreseeing risks, and averting intrusive situations before they arise. Actually, it's a crucial element of a more comprehensive customer data and analytics strategy, which may help maximize privacy protection and open up new revenue prospects. This strategy has the necessary scale to deliver many of the advantages of digitization and can also assist develop digital trust with end users and encourage wider adoption (KPMG, 2022b).

The following significant issues have arisen in relation to privacy and digital identity (KPMG, 2022b):

- Adding privacy to the board's agenda: the importance of privacy governance is greater than ever. Boards are increasingly considering how these privacy issues may affect the business and agree that maintaining digital identities is a corporate governance issue. From the viewpoint of the board, the effects of an identity-related breach include possible legal liabilities, regulatory sanctions, brand damage, and the theft of sensitive information and intellectual property.
- Lowering overcollection: a risk can rise as user data collection increases. As a result, excessive data gathering, and retention have drawn a lot of attention. Recent regulations have established guidelines for data minimization, guaranteeing that a company can only request the bare minimum of data necessary for a particular transaction. More focus is being placed on this now because, if regulators knock on user door, he/she must show

that is being compliant. In addition to being risky, data overcollection is also inconvenient since it forces users to repeatedly share the same information with several organizations, posing privacy problems that may subject people to pointless profiling and tracking.

- Identifying privacy champions: it is now very difficult to allocate resources in this area. Organizations should cultivate privacy champions. Champions also find it challenging to survive on the front lines without staff.
- Determining “where privacy lives”: The idea of where privacy should reside within an organization has also seen some change. This opens the door for the chief privacy officer (CPO), who is in charge of overseeing legal compliance and determining how personally identifiable information is gathered, stored, exchanged, and transmitted.
- Data anonymization: the act of processing data so that it is irrevocably de-identified, is receiving more attention lately. 48 percent of Americans said they would feel better at ease with businesses collecting and utilizing their personal information if it was completely anonymous, according to KPMG's US data privacy survey. But some businesses are having trouble with it. As the data is merged with previously gathered, sophisticated data sets, including geo-location, picture recognition, and behavioural tracking, insufficient anonymization may also lead to re-identification.

By establishing clear privacy principles in advance, it is possible to incorporate the necessary safeguards into digital identity systems (KPMG, 2022a).

1.17 Trust Services

Individual rights are well-established in the real world. In general, people may go about their daily lives without worrying about becoming the victim of a crime and with the assurance that the police and court system will stand by them if a problem develops. In contrast, these rights are still being developed in the virtual world, where cyberattacks like online fraud, data breaches, malware, and others are all too widespread and not as explicitly controlled. In order to fully utilize the power of data and technology, local authorities must handle the crucial issue of trust. Citizens will withhold information, refuse permission to exchange data, or just stick to conventional communication techniques if they don't trust government agencies to handle personal data safely (KPMG, B, 2022).

Digital identities can significantly contribute to the growth of trust and to the convenience of services. People currently have to continually establish their identification, frequently by providing more personal information than is necessary for the transaction. Organizations can only check what they need to know when they need to know it thanks to a secure digital identity system. To ensure that local organizations can collaborate on identification, such as transferring or accepting validated information from someone migrating from another region of the country, common rules and standards linked to the storage and processing of identity data are essential. The Pan-Canadian Trust Framework, managed by the Canadian Digital ID and Authentication Council, is an illustration of how such an ecosystem may be created (KPMG, B, 2022).

Data must be protected by local authorities no matter where it is located, which can today be anywhere from a data centre to a cloud environment. There is a need for a "zero-trust" model of security, which safeguards data access via user identification rather than network location and operates under the presumption that networks are untrustworthy. This is even more important given the rise in the use of Software as a Service (SaaS) applications and outsourced cloud computing services, as well as the COVID-19 pandemic's widespread use of remote working (KPMG, B, 2022).

Digital ID can also unlock social value, potentially advancing the realization of principles like inclusivity, rights protection, and transparency that cannot be quantified. Digital ID can encourage greater and more equitable access to healthcare, employment, and education opportunities, as well as promote safe migration and higher levels of civic engagement (Mc Kinsey, 2019).

1.18 eIDAS Regulation

One of the key requirements for the proper operation of the Information Society and, from the perspective of the European Union, the internal market, has been recognized as the development of trust in Internet transactions. To assist people in boosting their confidence in the legitimacy and efficacy of their Internet activities, legal institutions that create legal security basis in connection to these outcomes should be regulated. Consequently, in recent years, the political and legislative agenda has embedded specific lines of action in this respect, particularly in the European Union, with the goal of recognizing the legal effects of electronic equivalents of the primary formal elements of the written document; namely, the guarantee of the identity of the parties and the delivery of the consent, the moment of delivery of said consent, and the moments of issuance and reception of the previous elements, when the parties are at a distance (Alamillo, 2020).

The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation³) adopted on 23 July 2014 provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens, and public authorities. The eIDAS Regulation is the primary trust framework in the European Union and the European Economic Area for the agency of natural and legal persons on the Internet. In this context, the eIDAS Regulation (eIDAS Observatory, 2016):

- assures that persons and enterprises can access public services in other EU countries where eIDs are offered by using their own national electronic identification schemes (eIDs).
- creates an internal European market for electronic trust services, such as electronic signatures, electronic seals, time stamps, electronic delivery services, and website authentication, by ensuring that they work across borders and have the same legal status as traditional paper-based processes.

With eIDAS, the EU has succeeded in creating the proper structure and legal framework that will allow individuals, businesses, and public administrations to securely access services and conduct

³ eIDAS, <https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014.html>

transactions online with only "one click." The implementation of eIDAS will, in fact, increase security and convenience for any online activity, including submitting tax returns, enrolling in a foreign university, opening a bank account remotely, establishing a business in another Member State, authenticating for internet payments, responding to online solicitations for bids, and much more (European Commission, 2022).

The eIDAS Regulation modification proposal and a document with recommendations for the creation of a pan-European digital wallet were made public by the European Commission on June 3, 2021. With the help of the European Digital Identity Wallet app, users will be able to access a variety of services locally or remotely and demonstrate their identity anytime it is necessary. It is an electronic wallet that may securely house users' digital identities as well as the dematerialized copies of their identification documents, such as their driver's license and possibly their passport. Be aware that this is not yet another electronic citizen recognition project or even the dreaded replacement of existing national digital identities; rather, it is presented as an effort to harmonize the articulated range of credentials already in users' hands by combining them into a single, more secure, easier-to-use, and more interoperable virtual wallet (Osservatori.net, 2021).

A regional identity document that eIDAS proposes offers enormous efficiency in relationships between states in all industries, but especially when it comes to consumer movement and use of financial services (Electronic Identification, 2022).

The goal of the Commission is to provide access to an interoperable system that allows for the storage and use of digital identification data for access to a broad range of services for all individuals and organizations operating inside the European Union. The following qualities will need to be respected by the European digital identity (Osservatori.net, 2021):

- **be accessible to anyone**, EU citizen or resident who wishes to use it.
- **be widely usable**, for instance, allowing citizens to use their digital identity wallet to prove their identity or that they possess certain attributes in order to gain access to public and private services.
- **grant users' full control over their data**, allowing them to choose which identity-related attributes or certificates to share with third parties.

The European Digital Identity Wallet app would cover the limit of every eIDAS notified national digital identity, since it would allow a full integration among European countries.

1.19 PSD2, AML, GDPR Regulations

The Revised Payment Services Directive (PSD2) was implemented concurrently with the General Data Protection Regulation (GDPR) and the 5th EU Anti-Money Laundering Directive (AMLD5). As a direct consequence, when (new) FSI players consider joining and trying to navigate the new branch payments market, they must consider three laws with vastly different goals and spirits. These three regulations form a complex framework that occasionally causes conflict or contains aspects that have not yet been fully crystallized, resulting in the **PSD2 Trilemma**. Each of the three laws was written with

a specific goal in mind. Whereas PSD2 allows for greater access to payment data, GDPR is focused on data restriction, and AMLD5 is focused on combating financial crime (Deloitte, 2022).

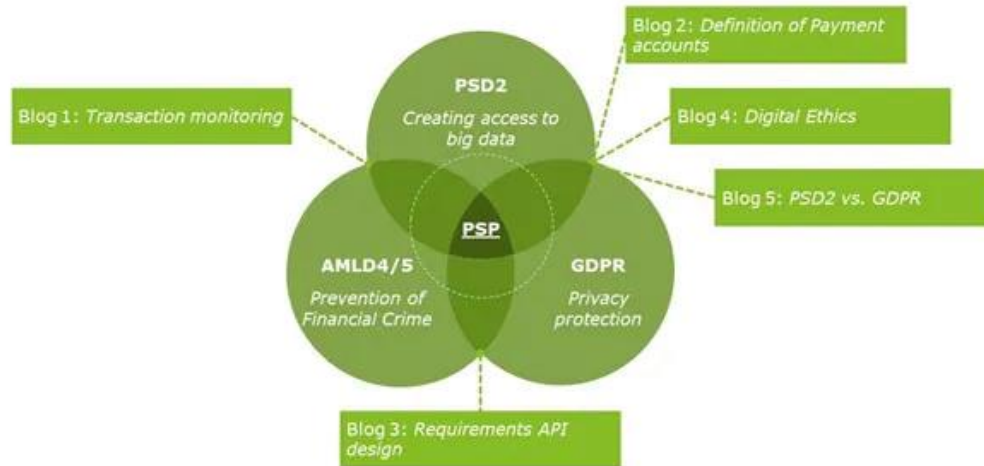


Figure 1.10 PSD2 Trilemma

Despite the fact that the goals and essence of PSD2, GDPR, and AMLD5 differ greatly, the three rules constitute a complex framework in which various challenges await parties who want to reap the benefits of PSD2, specifically to provide insight into the risks and opportunities that exist between big data, privacy, and the prevention of financial crime (Deloitte, 2022).

1.19.1 PSD2

Part of a global trend in bank regulation that emphasizes security, innovation, and market competition is the second Payment Services Directive (PSD2). PSD2 is a significant step toward commoditization in the EU banking industry by mandating banks to grant other authorized payment-service providers (PSPs or Third-Party Payment Service Providers - TPPs) connectivity in order to access customer account data and to start payments (McKinsey Global Institute, 2018).

The two main topics addressed by PSD2 are the introduction and regulation of new parties and services in the e-banking market, as well as the creation of new guidelines for licensed third-party providers to use the recently opened banking infrastructure related to customer account access (XS2A), with their express permission, with additional enhancements to payment processing security through the introduction of Regula (Forester, Rolfe & Brown, 2017).

Banks primarily lose out on the PSD2. They are required to freely grant the payment service providers access to the user's accounts as account servicing payment service providers (Wolters & Jacobs, 2019).

The banks also face fresh opposition. They were in charge of account access prior to PSD2. No lawful access was granted to other payment service providers.

This trend may also be advantageous to the banks. They can access the accounts of customers of other banks thanks to the PSD2 because they offer payment initiation and account information services. These chances, however, are unlikely to overcome the negative effects of heightened competition. Large technology firms like Facebook, Apple, Amazon, Microsoft, and Google are also predicted to pose a greater threat to them than other banks (Wolters & Jacobs, 2019).

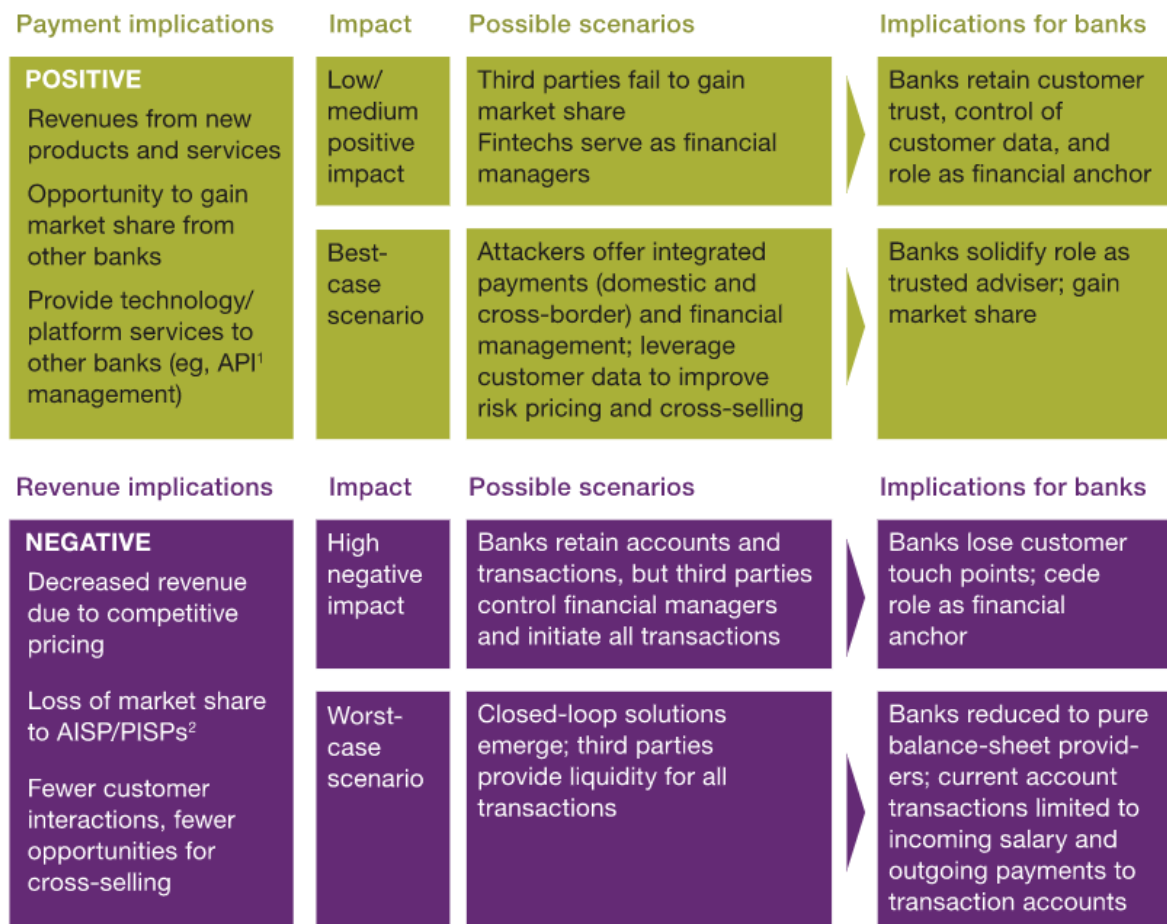


Figure 1.11 PSD2 has a range of implications for banks (McKinsey Global Institute, 2018)

PSD2 will have winners and losers, with banks coming under heavy fire from new nonbank PSPs. Agile firms that have the resources to invest in novel approaches and fresh business models have a better chance of successfully addressing these issues (McKinsey Global Institute, 2018). In 2017, McKinsey conducted research to identify the TPPs that would benefit most from PSD2 legislation.

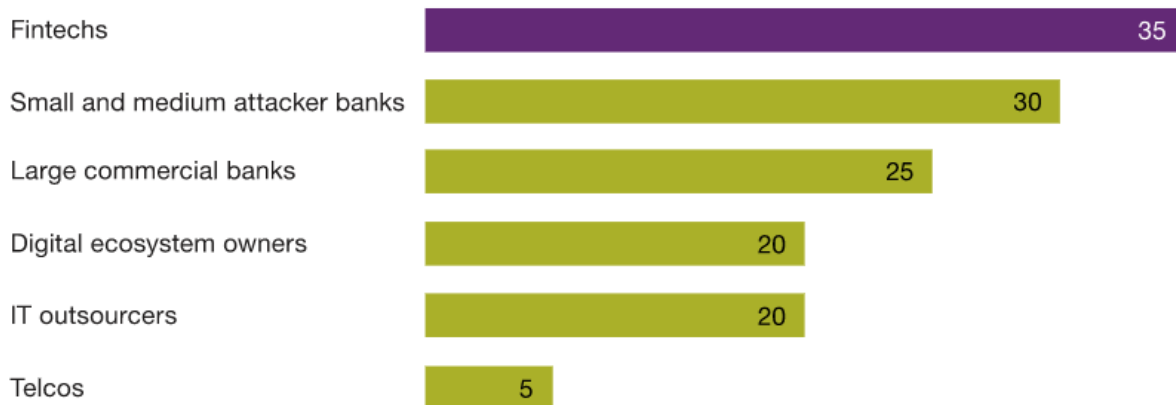


Figure 1.12 Survey with bankers' responses (McKinsey, Global Payments Practice PSD2, 2017)

FinTech firms have emerged as the financial industry's main rivals in recent years. These businesses can be referred to as entities leveraging new technologies to deliver items that are either complementary or competitive to comparable products offered by regulated financial institutions, as FinTech is an acronym for financial technology (Kuszewski, 2018). They want to make traditional services more individualized, transparent, and easily accessible through digital channels while also enhancing the user experience and process efficiency. These changes will provide alternatives to traditional financial services (Vasiljeva & Lukanova, 2016). According to The Fintech Times, European fintech is the largest investment sector in the world, making about 20% of all global investments (The Fintech Times, 2019).

Considered that, it becomes easier to understand why PSD2's main objective is to end banks' exclusive legal right to access their customers' accounts (Wolters & Jakobs, 2019), as FinTechs and other new entrants can only survive in this new environment by accessing banking data through the API due to high capital requirements and other costs that act as significant barriers to entry and starting a business (Choi & Park, 2019).

On September 14, 2019, these regulations ought to have gone into effect.

1.19.2 GDPR

The strictest privacy and security law in the world is the General Data Protection Regulation (GDPR). Although it was created and approved by the European Union (EU), it imposes requirements on any organizations that target or gather information about individuals residing in the EU. The rule becomes effective on May 25, 2018. Europe is signalling with the GDPR its tough stance on data privacy and security. For small and medium-sized businesses, GDPR compliance is a frightening proposition due to the regulation's scale, scope, and relative lack of specifics (SMEs). The GDPR specifies that any information relating to an individual who can be directly or indirectly identified is considered personal data. Email addresses and names are obviously personal information. Political viewpoints, browser

cookies, ethnicity, gender, biometric data, and location details can all be considered personal data. Data processing includes all manual or automated operations on data, such as gathering, recording, organizing, structuring, storing, using, and deleting. There exist seven protection and accountability standards listed in Article 5.1-2 must be followed when processing data (GDPR.EU, 2020):

- Legitimacy, equity, and openness. Processing must be legitimate, equitable, and open to the data subject.
- Purpose restriction. It is only allowed to use data for the legal purposes that were made clear to the data subject when it was gathered.
- Data minimization. It should be only gathered and analysed the minimum amount of data required to fulfil the outlined objectives.
- Accuracy. It must maintain the accuracy and correctness of personal data.
- Storage restriction. It may only keep personally identifying information if it's required for the intended use.
- Integrity and confidentiality. Processing must be carried out in a manner that provides the necessary security, integrity, and confidentiality (e.g., by using encryption).
- Accountability. It is the data controller's duty to demonstrate compliance with all these GDPR tenets.

1.19.3 AMLD5

The 5th Anti-Money Laundering Directive (AMLD5) was published in the Official Journal of the European Union on June 19, 2018, and all EU Member States had to implement it by January 10, 2020 (Dow Jones, 2022).

AMLD5 sought to ensure that terrorist funding and money laundering were no longer feasible within the EU financial system. The European Commission does this to prevent criminal groups from laundering their illicit funds. Additionally, it makes it harder for terrorist groups to get financial support. The EU is attempting to tackle financial crime through such laws, but not at the price of the global financial system (Cointelegraph, 2022).

Even while AMLD5 does not directly contradict with PSD2 criteria, the Directive's objective makes it more difficult for people that want to enter the payments business (Deloitte, 2022).

The European Commission develops the idea of a "Digital Single Market" by standardizing electronic identity methods using eIDAS. With legislation like PSD2, 5AMLD, eIDAS, or GDPR, Europe is leading the world in financial regulation and enabling businesses to benefit from the opportunities that result in the financial system's disruption (Electronic Identification, 2022).

1.20 Literature gap

Digital Identity trends are continuously evolving thanks to huge investments in the research. It's important to underline that Digital Identity solutions and regulations are very different around the world. For instance, in Europe there is the eIDAS regulation, which aims at providing a common normative basis for secure electronic interactions between citizens, businesses, and public administrations and at increasing the security and effectiveness of electronic services and e-business and e-commerce transactions in the European Union. Compared to electronic identification systems, the regulation envisages that each Member State can notify the electronic identification systems provided to citizens and companies for the purpose of mutual recognition. The eIDAS regulation was issued on 23 July 2014 and is fully effective from 1 July 2016 (AGID, 2022). On the other hand, in the rest of the world there are various systems for digital identification. Some of them are quite developed, while other ones are in their infancy. Focusing on eIDAS regulation in EU, studying the solutions adopted by European countries and in the meantime looking at the most developed solution in the Rest of the World, constitutes the best practice to cover a topic which has never been mapped in the current literature or in documentation available on digital identities. The objective of this report will be to accomplish provide the analysed academic landscape and practitioner-oriented reports with an overview of digital identity at the international level, what projects have been developed and their characteristics, as no adequate report or documentation exists to date.

2. RESEARCH METHODOLOGY

This Chapter explains in detail the process to reach the results attended and the motivations that push the research on the topic. Firstly, it is described the process of analysis of the scientific literature, and then how the international cases sample was reviewed, enlarged, and analysed.

2.1 Digital Identity Observatory

The whole project was elaborated in collaboration with Osservatori Digital Innovation of the School of Management of the Politecnico di Milano, which permitted the access to the whole knowledge accumulated during the years, such as scientific database, archives, and censuses, sharing news and supporting the work along the process of screening and further extraction. In particular, the project was developed with the Digital Identity Observatory, which was born to address the homonym topic, that is taking more and more importance along the years. It started on 27th November 2019 as Working Table, and, after having analysed how the topic is becoming more and more central for the digital transition, it became an official observatory in 2020. This evolution represents the growing importance of the subject, motivating the thesis.

The research started with an analysis of the current literature on the topic. Then extracting the list of variables used to create a census of international digital identity projects working, with a general and technical description. Successively, other dimensions, such as technologies, areas of application and value proposition, will be analysed to find possible clusters and give the conclusion of this paper.

2.2 Research Question

Looking at the Literature chapter, currently there is a growing digital identity trend which is different with respect to the geography considered. Therefore, this work has the aim of clarifying why there is so much diversity in terms of development and use for the digital identity. Digital identification is expected to become more significance than before. According to Deloitte, “digital identities are becoming the foundation of our rapidly evolving technology-based and data-driven economy and society,” and “digital identity should be at the core of any leading, data-driven organisation.” On the other hand, traditional identification solutions are less and less able to meet the needs of our society as it becomes increasingly digital, which forces everyone to look for new ways to generate, manage, and safeguard their digital identities in the future.

A major cause that contributed to accelerate digital identity system evolution and penetration was the COVID-19 pandemic along 2020 and 2021. That was the period when users started to notice the need of signing up for digital identity. This feeling has risen significantly in the last two years, and it

will go on rising over the next years. Talking about numbers, it is forecasted a significant increase, by more than 50%, from 4.2 billion of users having a digital identity in 2022 to 6.5 billion in 2026, according to a Juniper Research analysis (Juniper Research, 2022).

Furthermore, Facebook's recent name change to Meta and the growing investments in the metaverse are a clear sign that the creation of a digital identity for this universe will be necessary to ensure the accuracy of the avatars' identities. At the same time, data leakage takes on a greater dimension as real life is represented in digital identities, increasing the possibility of avatar theft and fraud on a scale never previously witnessed. Because of this, it's critical to comprehend how each resource may both assist users in protecting themselves when utilizing their digital identities and facilitate the development of trust inside and between platforms (Forbes, 2022).

As society digitizes, more and more nations are beginning to acknowledge and provide to their citizens digital identity. A proposal for a digital identity for all European residents was made public by the European Commission this year, enabling the storage and management of all official papers through a digital wallet (European Commission, 2022). The small European nation of Estonia, which has been utilizing this system for many years and has a population of roughly 1.3 million, is an example of where this already occurs in practice. In the nation, 99% of services—including voting, forming a business, and even issuing birth certificates—can be accessed online. A digital ID ecosystem serves as the foundation for connecting people to these amenities. However, by embracing digital, the nation has able to save 2% of its GDP in addition to making life easier for inhabitants (International Peace Institute, 2016).

As a result, variables including user experience trends, new legislation, public acceptance of new technologies, and others will continue to influence how digital identity develops in the future.

It becomes very clear that a trend of digitalisation is in place, bringing companies and people to adapt to the new context that is evolving. There are different advantages like cutting cost and enhancing benefits as explained above, but the sector is still maturing, since standards are set, but continuously evolving and adapting to the context.

In this market big opportunities, it is fundamental to create a full picture of the current panorama of digital identity projects around the world. Looking at the projects currently available and fully operating around the world, new directions in which the market could find new solutions, to understand which are the new initiatives that would drive the sector, can be found. Therefore, the research question that this work will answer is:

→ How is the picture of digital identity system at the international level in 2022?

Basically, what it is needed to proper answer to the research question is an international census of the digital identity projects. Indeed, it would allow to examine through punctual variables every single characteristic of each active project in the world. Gathering many relevant data about digital identity will allow to make statistics and reason about the most likely consequences and trends that should follow in the next years. Among the basic question that the census can help with answering there are:

- Where are the projects run?
- Which are the technologies that are used in the digital identity projects?
- Which are the sectors more targeted?
- How do the actors behave?

- Who are the targets of the value proposition?
- Which are the value propositions offered?
- Which kind of services do the projects develop and offer?

The process to answer to these questions follows several steps. Firstly, an analysis of the literature was necessary to understand the state of the art of the digital identity ecosystem. The literature review allowed to understand the state of the art and track the selection of variables to be included in the census construction. Finally, the analysis and the evaluation of the projects to understand the results in order to answer to the research question.

Every step of the process mentioned above has been described in detail in the following paragraphs.

2.3 Theoretical Review

In order to have a complete overview on the Digital Identity topic, an analysis of the literature was necessary in order to bring together all the fragmented information related to the theme, to understand which are the intersections and the research gaps. To collect the documents, Scopus was used as a primary source database, helping in gather all the reports and articles connected to the main topic. The process had 3 main steps:

1. Extraction: during this phase, the whole material related to the topic was downloaded from the database. The sections “Article title, Abstract, Keywords” were selected in order to extract a complete list of documents. The keyword used in this phase was “Digital identity” and some filters were added, such as English language and Subject Area (like Computer Science, Engineering, and Business Management and Accounting). The output was a CSV file containing different information regarding the 1222 selected documents (like title, authors and year).
2. Screening: in this phase, the first 200 abstracts per number of citations were read in order to determine their pertinence, this allowed to classify the documents into relevant and not relevant. The ones belonging to the first category were downloaded and organised for deeper analysis.
3. Analysis: the papers classified as relevant were classified based on the authoritativeness of the publication journal. The classification was based on the guidelines of the Italian Engineering Management Association and allowed to cluster the papers in five classes: Goldstar, Gold, Silver, Bronze, Copper. Then, all the documents were entirely read in order to have a complete view on the state of the art of the theme, and each of them was categorized based on the research question and on the topic described, like biometrics, digital signature and social impact.

The output of the theoretical review was an excel file containing the key points of all the documents read. Few other documents were extracted from Google Scholar in order to further enrich the collected information. The content of the papers has informed the analysis presented in detail in Chapter 1, helping to have a complete understand on the main topic.

2.4 Empirical Framework

Several phases were followed in order to carry out a descriptive analysis of the digital identity projects. Firstly, a review of secondary sources was performed to create an excel sheet of projects working in the digital identity environment.

The full description of every digital identity project was read in order to act a first screening phase. The ones not considered in target with the definition of the observatory or if a primary source was missing were excluded. After compiling the census of relevant digital identity cases, which amounted to 120 projects, the excel file was enriched using several variables (described in full detail in the next paragraph) which were found to be relevant based on the analysis of the literature.

The entire process, shown in Figure 2.1, will be explained in detail in the next paragraphs.

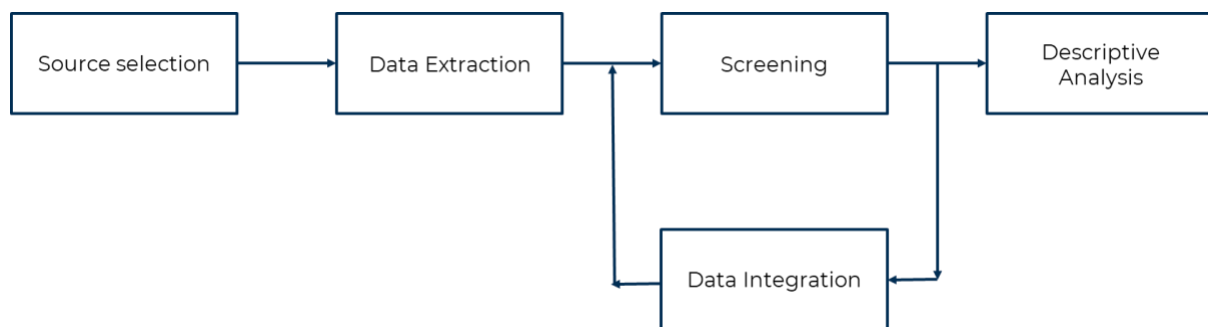


Figure 2.1 Empirical framework

2.5 Source Selection and Data Extraction

The projects included in the source selection have been selected based on their belonging countries. A splitting per country was performed, in order to focus on the country having a good level of knowledge and experimentation about digital identity. After selection of the most interesting countries have been picked up some project per state. There have been countries with 5-6 projects and others with just one digital identity project. In this case the decision depended by the maturity of the project itself. Usually, priority was given to fully operational projects. After selecting all the projects, much research was carried out in order to associate technical digital identity variables to each one. The main point was to assess the level of coverage of the population per each project, so how many people in a country were using a specific digital identity, basically the level of adoption of a digital identity, expressed in percentage, taking into account the number of people per country. After getting this result, the goal become to find as much as possible information related to that project, basing the research on the variables suggested by the experts of Digital Identity Observatory.

The list of keywords, decided by a team composed of the undersigned and experts on the topic for the previous extraction, were used as filters to extract project information belonging to the Digital Identity

ecosystem. The keywords were inserted in research on the Internet. A total of 27 keywords were defined. The keywords used for the extraction are summarized in Table 2.1.

| Extraction Keywords | | | | | | | |
|---------------------|----------------|----|----------------|----|----------------|----|--------------|
| 1 | Digital ID | 8 | Recognition | 15 | Self-Sovereign | 22 | SSI |
| 2 | Identity | 9 | Verification | 16 | Entities | 23 | Data Privacy |
| 3 | Identities | 10 | Biometrics | 17 | ID | 24 | PSD2 |
| 4 | Identification | 11 | Biometric | 18 | IDs | 25 | Identify |
| 5 | Authentication | 12 | Entity | 19 | KYC | 26 | Identifies |
| 6 | Onboarding | 13 | ID Wallet | 20 | Trusted | 27 | Credential |
| 7 | Passwordless | 14 | Self Sovereign | 21 | identified | | |

Table 2.1 Keyword used for the Data Extraction

Then all the information that satisfy one or more of the four criteria mentioned above, containing at least one of the previous keywords were extracted. It has been decided to extract just the needed information. The 18th variables are summarized in Table 2.2.

| CATEGORY | VARIABLE | DESCRIPTION |
|----------|-----------------|---|
| Main | Project name | The name of the digital identity project |
| | Link | The website link of the project |
| | Country | Country in which the project has been developed |
| | Geographic area | The continent in which the Country is located |

| | | |
|----------------------|---------------------------------|--|
| General Information | Launch date | The date when the project was announced |
| | Operational start date | The date when the project started being operational |
| | eIDAS | If the project is eIDAS notified |
| | Population Coverage | A percentage calculated as: Nr. Users / country population |
| | Accesses through the system | Nr. of access in the digital identity system since it was made operational |
| | Linked to a physical document | If the project is linked to a physical document |
| | Digital version of the document | If the project has a digital version of document |
| Trust Services | Signature | If the signature functionality is available |
| | eDelivery | If the eDelivery functionality is available |
| State of the Project | Announcement | The project has been only announced |
| | PoC / Experimentation | The project is in the testing phase, not yet operational |
| | Operational | The project has been released and it's available |
| Robustness | Robustness | Whether the project is recognised as trusted or untrusted |
| Type of Identity | Sovereign | If the project is based on a Sovereign Identity |
| | Functional | If the project is based on a Functional Identity |
| | SSI | If the project is based on a Self-Sovereign Identity |
| Ecosystem | Governmental Agency | If the project ecosystem includes Governmental Agencies |
| | Financial Institution | If the project ecosystem includes Financial Institutions |
| | Trust Service Provider | If the project ecosystem includes Trust Service Providers |
| | Telco | If the project ecosystem includes Telco Companies |

| | |
|---------------------|--|
| Technology Provider | If the project ecosystem includes Technology Providers |
|---------------------|--|

Table 2.2 Variables collected for the Data Extraction (part 1)

All variables were gathered inside an excel sheet, which contains 120 digital identity projects, each with 25 variables, divided in 7 macro categories.

2.6 Screening and Data Integration

After having updated the official list of the projects – in fact, 30% of the projects were added to the initial list of projects provided by Digital Identity Observatory experts – it was necessary to check if the information extracted for the new project, but also for the ones already present, was coherent with each project. The reason is the time delay between the evolution of each project and the updating of the information on the Internet, which can require time. In this time span a project could have been put in stand-by or started to include new service provider or it may have changed the value proposition, exiting from the boundaries taken into consideration.

Moreover, the intention planned was to increase the dimensions of analysis, so once checked that the state of the project was updated together with all main and general variables, other variables were checked by different sources on the Internet. It has been decided to use the projects website because they are fully managed by companies or Governmental entities relatively to country to which the project belongs. The added variables were organised in categories, which are summarized in Table 2.3.

| CATEGORY | VARIABLE | DESCRIPTION |
|----------------------------|---------------|--------------------------------------|
| Architecture | Centralized | If the architecture is Centralized |
| | Federated | If the architecture is Federated |
| | Decentralized | If the architecture is Decentralized |
| Architectural Technologies | PKI | Use of PKI technology |
| | Cloud | Use of Cloud technology |
| | Blockchain | Use of Blockchain technology |

| | | |
|--------------------------|---|---|
| | SW on PC | Use of Software on Personal Computer |
| Protocols | SAML | Use of SAML or SAML 2.0 protocol |
| | OIDC | Use of Open ID Connect Protocol |
| | API & SDK | Use of API & SDK |
| Secure Element | Smart Card | Use of Smart Card as Secure Element |
| | SIM | Use of SIM as Secure Element |
| | Cloud | Use of Cloud as Secure Element |
| Smart Card | Smart Card Reader | Use of Smart Card Reader |
| | Reader via NFC Smartphone | Use of NFC Reader via Smartphone |
| | Card with OTP | Use of a Card with OTP |
| | Other Reader | Use of a not listed Reader |
| Mobile | SMS for OTP reception | Use of SMS for OTP reception |
| Biometrics | Finger | Biometrics identification using the finger |
| | Palm | Biometrics identification using the palm |
| | Vein | Biometrics identification using the vein |
| | Face | Biometrics identification using the face |
| | Iris | Biometrics identification using the iris |
| | Voice | Biometrics identification using the voice |
| | Behaviour | Biometrics identification using the behaviour |
| Access / Use Credentials | Social security numbers / physical document | Use of social security number credentials or physical document number credentials |

| | | |
|----------------------|-----------------------------|--|
| | User ID | User ID as Credentials for access or use |
| | Phone Number | Phone Number as Credentials for access or use |
| | Password | Password as Credentials for access or use |
| | PIN | PIN as Credentials for access or use |
| | OTP | OTP as Credentials for access or use |
| | Biometrics | Biometrics as Credentials for access or use |
| | #MFA | Number of Authentication factors needed for access or use |
| Phase of the Process | Identification | If the project has an identification phase |
| | Authentication | If the project has an authentication phase |
| | Authorization | If the project has an authorization phase |
| | Maintenance | If the project has a maintenance phase |
| Data typology | Personal | If data retrieved from the user are personal |
| | Biometrics | If data retrieved from the user are biometrics |
| | Certifications / Attributes | If data retrieved from the user are certifications or attributes |
| | Dynamic | If data retrieved from the user are dynamic |
| Field of Application | General Purpose | Solution developed for General Purpose |
| | eCommerce & Retail | Solution developed for eCommerce & Retail companies |
| | Finance | Solution developed for Financial Institutions |
| | Telco | Solution developed for Telecommunications companies |
| | Healthcare | Solution developed for the Healthcare sector |

| | | |
|-------------------------|--------------------|---|
| | Travel & Tourism | Solution developed for Travel & Tourism |
| | eGov | Solution developed for digital Governmental services |
| | Enterprise | Solution developed for Enterprise use |
| | Humanitarian Scope | Solution developed for Humanitarian organizations |
| | Mobility | Solution developed for Mobility |
| | Utility | Solution developed for Utilities companies |
| | Gaming | Solution developed for Gaming companies |
| | Education | Solution developed for Education |
| Service Provider | Public | If the Service Providers include the public sector, the government and/or government agencies |
| | Private | If the Service Providers include the private sector |
| | Number | Number of total Service Providers per project |
| Economic Sustainability | Service Provider | Whether the cost is borne by the Service Providers |
| | Identity Provider | Whether the cost is borne by the Identity Provider |
| | User | Whether the cost is borne by the Final User |

Table 2.3 Variables collected for the Data Extraction (part 2)

The end result was an excel sheet, which contains 120 digital identity projects, each with 65 variables, divided in 14 macro categories.

2.7 Descriptive Analysis

The final output derived from the phases of extraction, screening and integration is an excel database composed by 120 digital identity projects, each one described by 100 variables, grouped in 21 macro categories.

The aim of the analysis was to manage this amount of information and variables in order to take a comprehensive picture of the context, extracting insights and answering to the research question. Thus, variables were analysed singularly and then combined to have a clear gaze on the market. The descriptive analysis was made according to different perspectives:

- **Geographical:** made to understand the distribution of the digital identity projects around the globe, which are the countries in the world, mainly in Europe, in which there is a greater focus on Digital Identity.
- **Technological:** made to understand which the technologies are more used by the digital identity projects to develop an overall vision on which technologies are more accurate and which ones will be the main protagonists in the next years.
- **Sectors of application:** the analysis shows which sectors are more developed in terms of digital identity solutions and applications, and which are the technologies more applied for the various sectors.
- **Economic sustainability:** the analysis shows which actors in the digital identity projects are the cost bearer referred to the authentication and use of digital identity.

3. RESULTS

In this chapter, the report discloses which are the results deriving from the antecedent procedure, explained in the previous section. Analysing the different variables and characteristics of the sample, the research tries to cluster them, understanding which the main trends are involved in the Digital Identity projects ecosystem. The results count 120 digital identity projects.

The analysis focuses on different aspects like:

1. Geographical distribution.
2. Technologies.
3. Application field.
4. Providers & Economic sustainability.

3.1 Digital Identity Projects

A digital identity project can have different stages:

- announcement
- PoC / testing
- operation

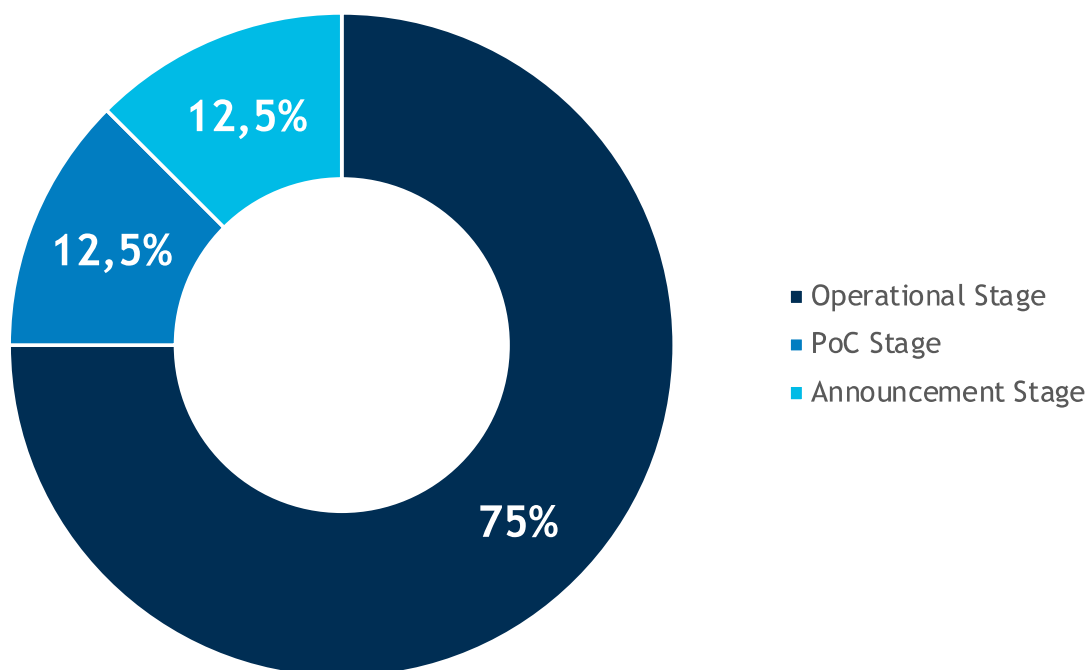
The *announcement* phase happens once the digital solution has been implemented and it is ready to be tested. In this stage the expected behaviour of the solution is established and needs to be tested and validated. Each announcement corresponds to a launch date, during which the project is announced officially to customers.

The *proof of concept (PoC)* aims to determine the feasibility of the idea or to verify that the purpose behind the project will work as intended. Basically, this stage stands for testing the solution in a real working environment, in order to assess the main functionalities, to discover every possible bug or issue that could prevent the digital solution to perform, and to behave in a secure and trustful way, compared to how it was conceived.

Finally, in the absence of bugs and other relevant issues, the PoC can be considered as successfully concluded. Therefore, the digital solution is ready to be used. It is when customers begin to use the solution in their production environment (B2B), or when customers simply begin to adopt the solution themselves (B2C), that the project can be called *operational*. At this stage, the project reaches a fully operational state, therefore, reliable statistical analyses can be carried out, assessing any strengths and weaknesses of the digital solution. When a project reaches its fully operational state and becomes available all round, then that moment can be spotted as “start date of operation”.

In this report, 90 digital identity projects out of 120 fall in the operational phase, while the remaining 30 projects are sliced between PoC and announcement projects, 15 per each respectively (Figure 3.1).

Digital Identity Projects



SAMPLE OF ANALYSIS: 120 PROJECTS

Figure 3.1 Distribution of projects based on the stage

3.2 Geographical Distribution

In this report, being an international census, the analysis of the geographic distribution of digital identity projects takes on a rather relevant connotation. The purpose of this analysis is to understand which areas are the most active in the world, in terms of digital identity, among the 120 samples analysed, revealing which countries should be considered as central hubs. The Figure 3.2 shows how the 120 digital identity projects, used as samples, are distributed around the world in absolute terms, and indicates the number of projects per continent. Indeed, on the global scale, the six continents share the number of digital identity projects in this way:

- Europe, 84 projects
- Asia, 19 projects
- North and South America, 8 projects
- Africa, 5 projects

- Australia/Oceania, 4 projects

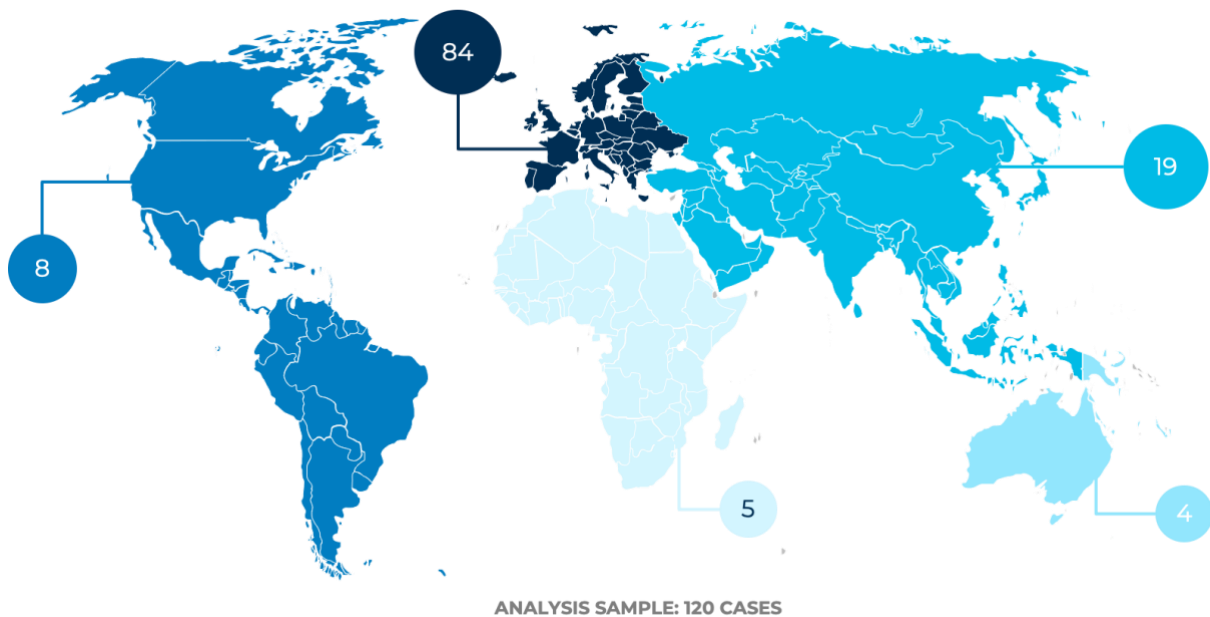


Figure 3.2 Geographical distribution of digital identity projects in the Globe

Europe is the continent with the highest number of digital identity projects (70% of the census), and it clearly outperforms the other continents: Asia (16%), Americas (7%), Africa (4%) and Australia/Oceania (3%).

This is due to an imbalance in the geographical location of the projects analysed. In fact, there is a natural bias for the European area.

The reason why most of the projects analysed have been selected from the European continent is because Europe promoted investment on digital identity, with the aim of supporting new norms issued by European Government. Clear examples proving that are:

- eIDAS regulation, came into force in 2014. As explained in the Literature section, the eIDAS legislation intends to increase the security and effectiveness of electronic services, e-business, and e-commerce transactions in the European Union, as well as to provide a consistent normative framework for secure electronic interactions between individuals, businesses, and public authorities.
- PSD2 regulation, came into force in September 2019. As discussed in the Literature chapter, PSD2's main objective is to end banks' exclusive legal right to access their customers' accounts. In fact, new industries have started from September 2019, to have the same legal rights as banks. Thanks to PSD2 legislation companies belonging to sectors as FinTech can survive and compete in the market against banking sector by accessing banking data through the API.
- bias for the European Union area, mainly due to research difficulties, since it was very hard to find sources and documentations that were not written in English or Italian (such

as Chinese, Russian, and many other Asian countries). If on the one hand for the Asian projects there was a language related issue, on the other hand, as regards Americans, Oceania, and Africa cases, they are quite undeveloped in terms of digital identity.

3.3 Technologies

Until now it has been seen how digital identity projects are distributed worldwide. Then, the focus has gone in depth with the 10 most continuous and documented projects of the last years, focusing on how each project offers services and which these services are. There is another fundamental component that needs to be examined, which is the technology that supports digital identity, without which it would not be possible to identify, authenticate, authorize people, animals, and things. Therefore, the following analysis will focus on the technologies implemented on the 120 samples of analysis of digital identity projects, mainly gathered in European countries. A digital identity project can make use of different kinds of technologies contemporarily. The ones taken into consideration are: blockchain, cloud, API & SDK⁴, Open Standard (OIDC⁵, SAML⁶), AI and analytics, mobile device (smartphones are not considered), proximity device, and biometrics, which had its subcategories (face, voice, fingerprint, iris, vein, palm, finger bone, behaviour).

3.3.1 Distribution of technologies

As first step it is necessary to understand the distribution of technologies in the 120 projects samples. As result it will be easier to map the most relevant ones.

| TECHNOLOGY | PERCENTAGE OF 120 PROJECTS | NR. PROJECTS |
|----------------------|----------------------------|--------------|
| Biometrics | 30% | 36 |
| Open Standard | 46% | 55 |

⁴ Software Development Kit (SDK) is a collection of tools which allows a programmer team to create a mobile application, which can be connected to other software

⁵ OpenID Connect (OIDC) is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

⁶ Security Assertion Markup Language (SAML) is a standard for the exchange of authentication and authorization data between security domains, typically an identity provider and a service provider

| | | |
|----------------------|-----|----|
| API & SDK | 52% | 62 |
| Blockchain | 8% | 10 |
| PKI | 78% | 94 |
| Cloud | 3% | 4 |

Table 3.1 Distribution of technologies in the main digital identity projects

As regards the Table 3.1, it is important to highlight that although the number of projects samples is 120, it should not be expected a technology per project, in fact, a project can support more than one of the considered technologies.

Looking at the whole census, the most diffused technology is **PKI**, used by 94 digital identity projects, followed by **API & SDK** with 62 projects using it, then **Open Standard** with 55 project making use of it, to whom follows **Biometrics** with 36 projects implementing it, then **Blockchain** with 10 using it, and finally **Cloud** only with 4 projects adopting it. Every result for each technology will be analysed in the next paragraphs.

3.3.2 PKI (Public Key Infrastructure)

Public Key Infrastructure was the most implemented technology among the 120 digital identity projects, with a presence of 78%. The reason why the PKI is so popular in digital identity projects is because it guarantees secure data communication in unsecure networks, such as Internet.⁷ Since for a digital identity is very likely to make use of digital certificate establishing rules of encryption and decryption of data exchanged among users, companies, providers and so on and so forth, it was an expected result finding out a massive use of this technology.

⁷ PKI is important because by being a certificate-based technology helps organisations establish reliable signatures, encryption and identities between people, systems, and things.

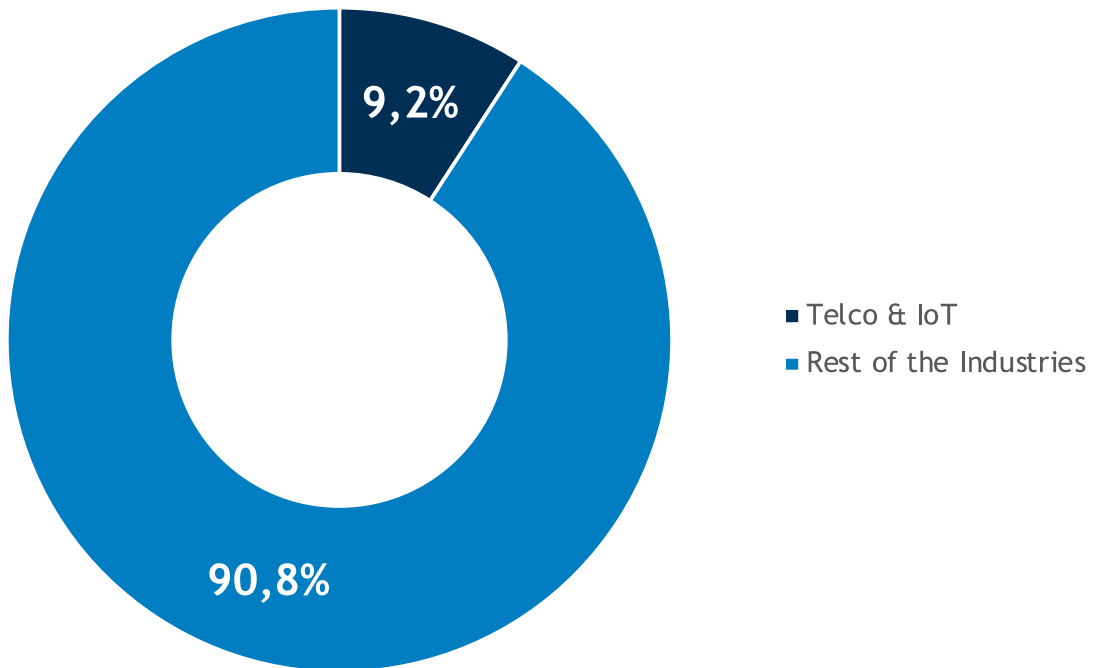
3.3.3 Cloud-based Architectural Technology

The cloud-based architectural technology was the least present among 120 digital identity projects. Only 4 projects endowed with a cloud-based mechanism, offering users standardize connection to trusted service and identity providers, were found out during the analysis. They are:

- the Finnish Trust Network (in short FTN, Finnish digital identity)
- Verimi (German digital identity)
- Cl@ve (Spanish digital identity)
- SwissID (Swiss digital identity)

Although cloud-based technologies are a minority in the analysis carried out, they will very likely have a great success in the IoT market, since the trend of using cloud solution is usual of this industry. Also, PKI would perfectly fit with a cloud implementation (this is the case of FTN and Cl@ve projects). In any case, considering the current digital identity trend, under a point of view of fields of application, it makes sense that cloud-based solutions are very few spreads, since neither their more natural application fields – Telco and IoT – results to be among the most the most promising sector for digital identity solutions adoption (Figure 3.3).

Telco & IoT



ANALYSIS SAMPLE: 120 CASES

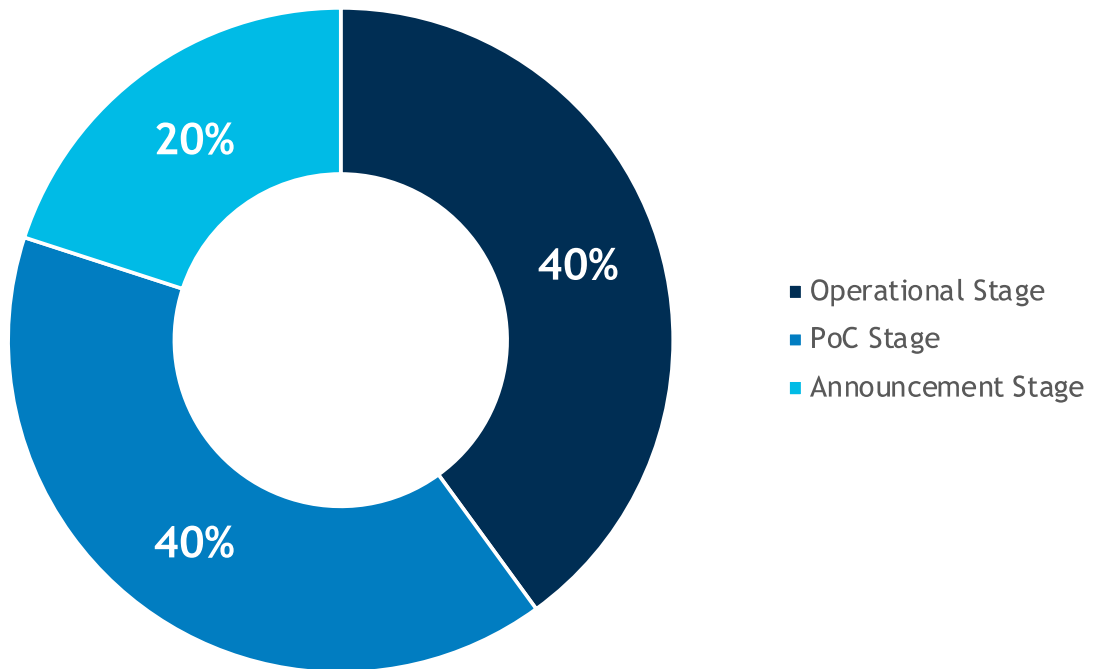
Figure 3.3 Telco & IoT

3.3.4 Blockchain Architectural Technology

As regards the Blockchain, there were found 10 digital identity projects among the 120 samples. Here the list of projects:

1. Jolocom (Germany) is in the PoC stage.
2. Dizme (Italy) is in the PoC stage.
3. eID (Macedonia) has been announced.
4. Blockcerts (Malta) is in the PoC stage.
5. Irma (Netherlands) is in the PoC stage.
6. MyID Alliance (South Korea) is fully operational.
7. IdentiCAT (Spain) has been announced.
8. Validated ID (Spain) is fully operational.
9. Zug ID (Switzerland) is fully operational.
10. NDID (Thailandia) is fully operational.

Projects implementing Blockchain



ANALYSIS SAMPLE : 10 CASES THAT UTILIZE BLOCKCHAIN TECHNOLOGY

Figure 3.4 Projects implementing Blockchain

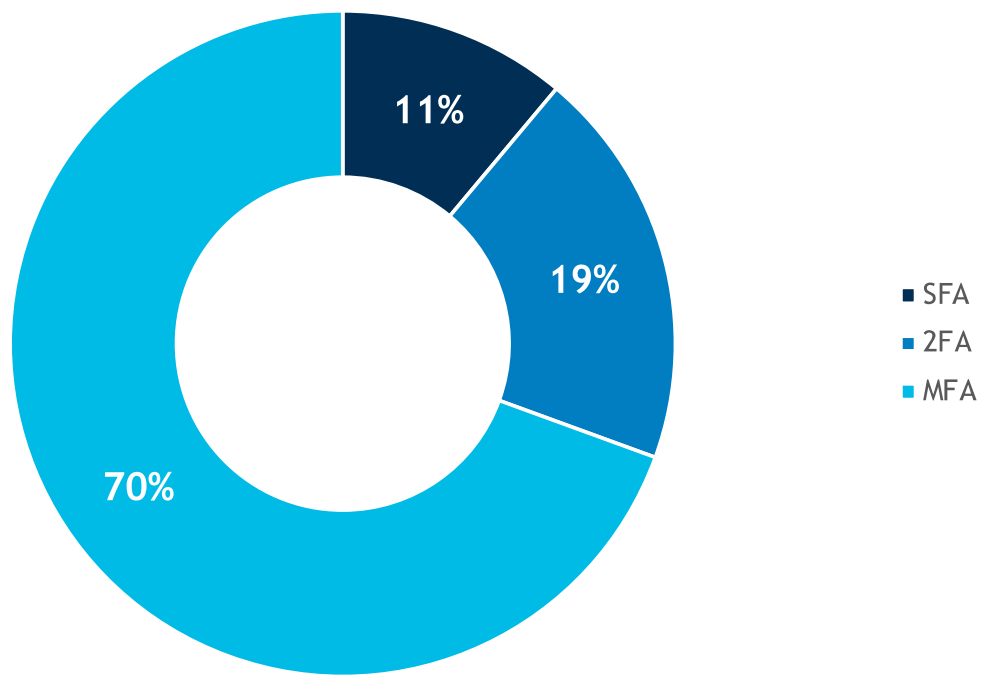
What appears is that blockchain is still too immature in the sphere of digital identity. This statement is based on the evidence that, since Blockchain-based digital identity needs a decentralized architecture and given that decentralized architecture is still quite new as technology, the number of projects implementing a digital identity based on Blockchain is limited. A further confirmation is provided by looking at the Figure 3.4, where 60% of the projects analysed are not in an operational status. In fact, 40% are in a testing phase (PoC), while the remaining 20% has only been announced.

3.3.5 Biometrics Technology

Taking under analysis the biometrics is an important step. In the Table 3.1 it was shown that the number of projects who included biometrics in their implementation is 36. It means that 30% of the projects analysed implement a biometrics technology system. It makes sense to understand what

percentage of biometrics is used as single method of access, to see if there are any systems that rely solely on biometric technology. The Figure 3.5 shows that just 11% of the projects out of the total 36 analysed have biometrics as their sole authentication method. 19% provide at least one other technology for authentication. While 70% provide at least two other technologies in addition to biometrics. The reason for the cases where biometrics is the sole authentication factor is its complexity and above all the fact that not all devices used to use digital identity services (smartphones, tablets, PCs, etc.) support biometric systems for recognition or authentication.

Access / Authentication Factors



ANALYSIS SAMPLE: 36 CASES

Figure 3.5 Biometrics distributions for access / authentication factors

Also, it makes sense to understand the different typologies of biometrics that can be implemented in a digital identity project. In the Table 3.2 and in the Figure 3.6 can be observed the distribution of biometrics types.

| BIOMETRICS | NR. PROJECTS |
|------------|--------------|
| Face | 22 |

| | |
|---------------------|----|
| Finger | 39 |
| Iris | 2 |
| Palm | 1 |
| Vein | 1 |
| Not Declared | 3 |

Table 3.2 Typologies of biometrics

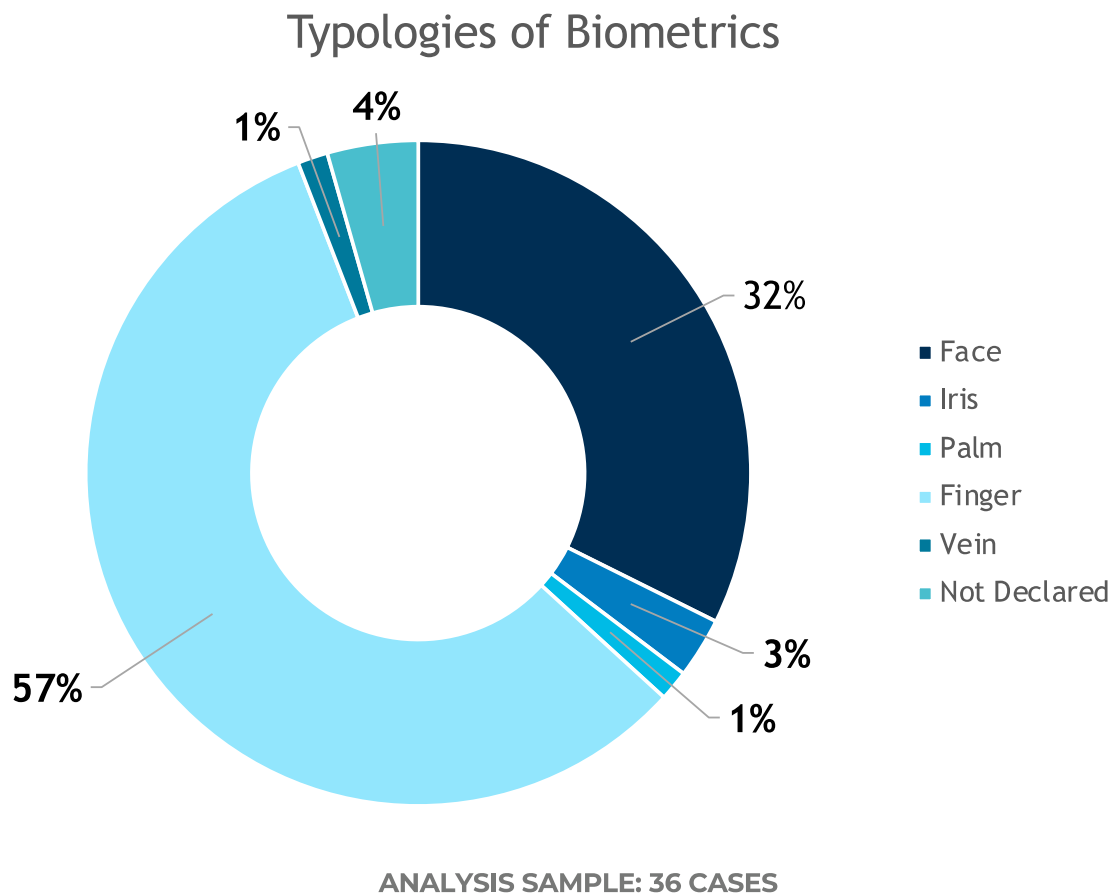


Figure 3.6 Typologies of biometrics

Basically, the most adopted recognition system is the fingerprint one, used by 39 projects, followed by face recognition implemented in 22 projects. Then, iris with only 2 projects implementing it and finally palm and vein with 1 project each. Other biometric recognition systems (behaviour, voice, finger bone, etc) are less diffused, because they are new kind of solutions, thus time is needed to develop and spread adequate devices that support these recognition systems. What can be resalted on the Figure 3.6 and Table 3.2 results is that the most

two spread biometrics type coincide with the most implemented ones in the devices normally used by users. In fact, smartphones and tablets usually have these two kinds of biometrics typologies. The rest of the biometrics type are more industry sector related, not to be destined to B2C users.

3.3.6 Open Standard Technology

The Open Standard technology is implemented in 55 out of 120 projects samples. It can be:

- SAML⁸ (Security Assertion Markup Language)
- OIDC⁹ (OpenID Connect)

Similar authentication systems like SAML and OIDC offer single sign-on for users. Both protocols are quite safe and can be tailored to increase user privacy by limiting the user attributes (also known as claims) that are shared. Both use a third-party identity supplier as well for authentication.

The Table 3.3 shows the distribution of these two standards inside 55 projects.

| TECHNOLOGY | PERCENTAGE OF 55 PROJECTS | N. PROJECTS |
|-------------|---------------------------|-------------|
| SAML | 65% | 36 |
| OIDC | 80% | 44 |
| BOTH | 45% | 25 |

Table 3.3 Comparing Open Standards

In the research the reason why OIDC is more used than SAML (+15% in the 55 considered samples) is easier than SAML to get up and run. Also, it adapts better with API interfaces, which are always included in the 55 projects examined. If the choice was based only on these mentioned parameters, then every project would have enough by implementing OIDC only. Nevertheless, SAML technology is usually preferred by big companies which look for highest security standards, that SAML covers better than OIDC.

⁸ SAML based Authentication is a method of identity verification that leverages an identity provider to authenticate users centrally to a broad range of unaffiliated websites. <https://cpl.thalesgroup.com/access-management/saml-authentication>

⁹ OIDC is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner. <https://openid.net/connect/>

3.3.7 API & SDK Technology

After PKI technology, the API & SDK technology is the most spread in the 120 international cases examined, counting 62 projects, which means 52% of the whole census. The reason why this technology is so massively applied is that API interfaces allows authentication platforms to integrate seamlessly with new and existing corporate implementations. While SDK help organisations to transparently incorporate trusted identities into existing applications.

3.3.8 Typology of Identity

Now the analysis moves to the typology of identity which could be of three types:

1. Sovereign
2. Functional
3. SSI (Self Sovereign Identity)

Looking at the below figure, it results quite clear that in the 120 projects analysed there is not a balance among the three typologies of identity. Indeed, the outcome sees Sovereign Identity as the most implemented type of identity (81 out of 120 projects are based on it), and it accounts for the 68% of the overall projects. Then, the second type of identity more implemented is the Functional one, which accounts for 29% of the overall projects (35 out of 120 projects are based on it). Finally, the last type of identity in terms of projects in which has been implemented, the Self Sovereign Identity, weighting only for 3% of the overall projects (4 out of 120 projects are based on it).

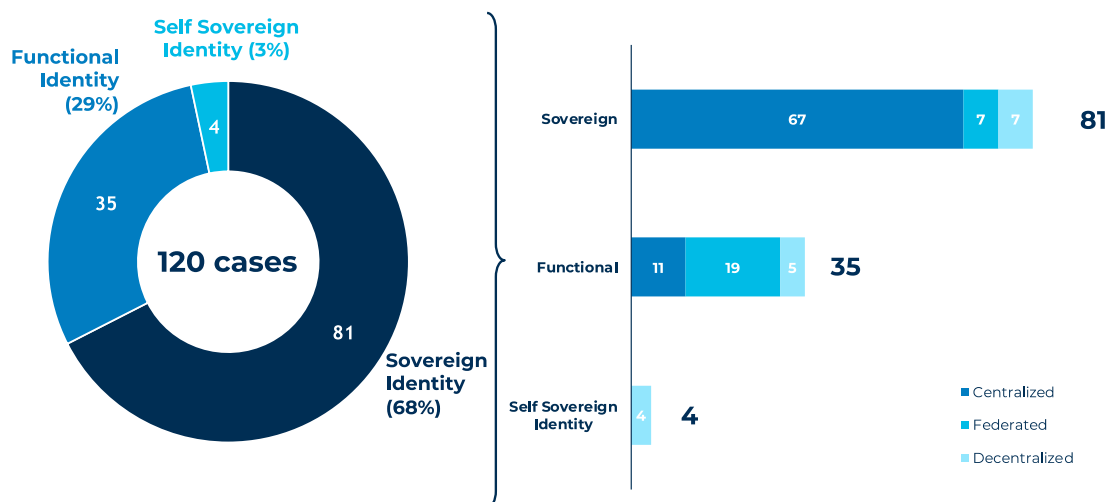


Figure 3.7 Typologies of identity

It is very interesting to understand the correlation between the typology of identity and the architecture adopted per each of the 120 sample projects. As the Figure 3.7 shows, every type of identity (Sovereign, Functional, SSI) is split based on the architecture that characterised the specific project. The architectures are:

1. Centralised
2. Federated
3. Decentralised

3.3.9 Sovereign Identity

Looking at the Sovereign Identity projects, it can be observed that a huge majority of the projects, having implemented this type of identity, are featured by a centralised architecture (67 out of 81 projects), standing for 82% of the projects with a Sovereign Identity. This is an expected outcome since under a Centralized Architecture, the digital identities of citizens are managed in a central database and each citizen is associated with their identity through one or more factor authentication. Indeed, in terms of ecosystem, almost every service that offers digital identification are based on Centralised Architecture, since these ecosystems allow organizations to have full control over user's data. However, Centralised Architecture having a centralised database are exposed to a high risk in case of data breach, losing all users data because of hackers and criminals. In summary, Centralised Architecture allow building services with specific purpose in mind and give the potential for organizational vetting of identity data.

For what concerns the matching between Sovereign Identity and Federated Architecture, it occurs in 7 out of 81 projects (standing for 9% of the projects with a Sovereign Identity). There are more actors involved in the process of digital identity since the Federated Architecture allow the user to relate to more services providers contemporarily and therefore to wider range of services. The advantage of having a wider environment with more services where to access using the same credentials, is really appreciated both on user and organization side and it raises organization efficiency.

Finally, the matching between Sovereign Identity and Decentralised Architecture, it occurs in 7 out of 81 projects (standing for 9% of the projects with a Sovereign Identity). Even in this case there is a drastically reduction of projects involved in Decentralised Architecture. The reason is because it is an innovative architecture, as explained in the Research Methodology chapter. Nevertheless, it is starting to spread deeper thanks to increased user control and reduced amount of information collected and stored by organizations.

3.3.10 Functional Identity

Analysing the Functional Identity projects, it can be noticed a countertrend with respect the Sovereign Identity. In fact, most of the projects include a Federated Architecture are 19 out of 35, standing for 54% of the projects with a Functional Identity. This is because Functional Identity marry the same philosophy of Federated Architecture, namely, they are open to a wider range of service providers and ecosystems (governmental, financial, technology service providers, etc) as well.

Then, takes the second place the Centralised Architecture with 11 out of 35 projects, standing for the 32% of the projects with a Functional Identity. In this case it is worth the reverse concept with respect Federated Architecture, since the Centralised one allow building services with specific purpose in mind and give the potential for organizational vetting of identity data, and both concepts are not completely matching between them.

Finally, the Decentralised Architecture is present only in 5 out 35 projects having a Functional Identity, standing for the 14% of the projects with a Functional Identity. Here it is valid the same reasoning as per Federated Architecture.

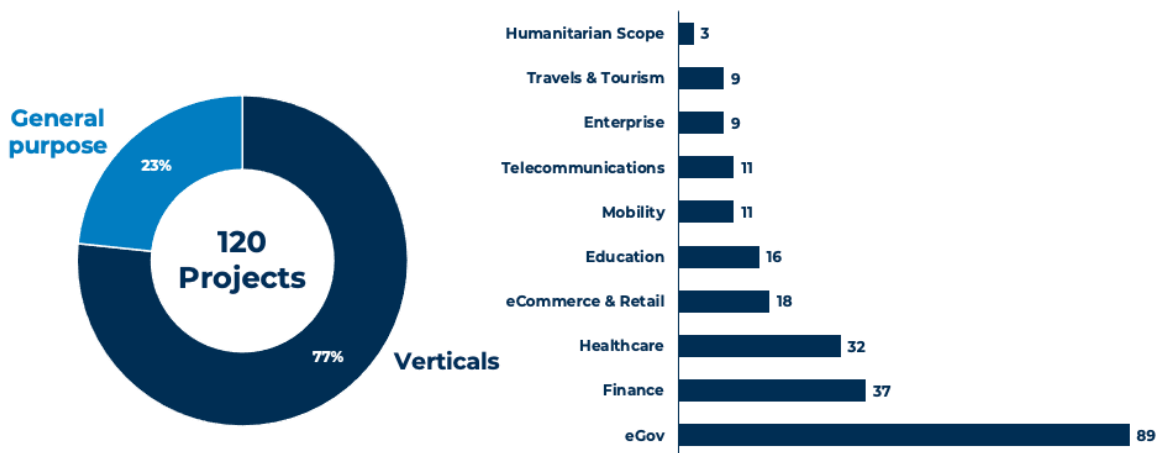
3.3.11 Decentralized Identity

Lastly, the SSI identity, which only has projects including a Decentralised Architecture. The reason is simple, the Self Sovereign Identity is a decentralised digital identity model based on Blockchain technology. It is based on restoring control over one's personal information to the user and would resolve the limitations of the digital identification systems prevalent to date, namely those based on the presence of Identity Providers. There are only 4 projects out of 120 including it, because the concept of SSI is as innovative as it is revolutionary in scope and is therefore at the centre of a major debate about its potential benefits and potential uses.

3.4 Industries of application

This analysis was made to understand which sectors are more targeted by the project working in the digital identity ecosystem and the related technologies involved. In a first division, projects are split in two macro categories:

- General Purpose projects
- Verticals projects



SAMPLE OF ANALYSIS: 92 PROJECTS WITH VERTICAL OFFERS

Figure 3.8 General Purpose vs Verticals application industries & number of projects per scope

The first ones are projects that are adopting a solution targeting very different kind of sectors, not related to a particular one. It has been decided to insert in this category the projects with 4 or more possible application fields. On the other hand, projects categorized as vertical, are the ones with a value proposition more focused on a specific industry. It has been decided to insert in this category the projects with maximum 3 application fields. Looking at the Figure 3.8, a significant majority of the digital identity projects (77%) is vertical, which means that the more of two thirds of the 120 projects analysed find a connotation inside a well-defined ecosystem, such as eGov, Education, Mobility, etc.

The 10 vertical application fields considered are:

1. eCommerce & Retail
2. Finance
3. Telecommunications
4. Healthcare
5. Travel & Tourism
6. eGovernment
7. Enterprise
8. Humanitarian Scope
9. Mobility
10. Education

The objective of this paragraph is to analyse the trend characterizing each sector (Table 3.4).

| TECHNOLOGY | PERCENTAGE OUT OF 120 PROJECTS | N. PROJECTS |
|--------------------|--------------------------------|-------------|
| eCommerce & Retail | 15% | 18 |
| Finance | 31% | 37 |

| | | |
|-----------------------------|------|----|
| Telco | 9% | 11 |
| Healthcare | 27% | 32 |
| Travel & Tourism | 8% | 9 |
| eGov | 74% | 89 |
| Enterprise | 8% | 9 |
| Humanitarian Scope | 2,5% | 3 |
| Mobility | 9% | 11 |
| Education | 13% | 16 |

Table 3.4 Distribution of sectors in the International Cases

Focusing on the industries, it can be observed that eGov, Finance and Healthcare sectors are the most involved industries. The firms belonging to these industries pursue a business model that sees digital identity as a recent main trend upon which basing a portion of the digital business strategy, with the goal to allow these companies to create a competitive advantage in their own industry, and generally being compliant with active regulations, thanks to the adoption of digital identity solutions. In the eCommerce & Retail and Education sectors, businesses are flowing more and more decisively through the direction that sees the adoption of a digital business strategy whose includes the prioritisation of digital identity projects implementation, and since the digital identity adoption is following an increasingly growing trend, it is expected that these sectors as well start to include more companies in the adoption of digital identity solutions. As regards Telco, Travel & Tourism, Enterprise, Humanitarian Scope, and Mobility, it can be confirmed that the digital identity trend has penetrated in these industries as well. However, it is a marginal trend by the moment, since there are other trends having a major importance with respect the digital identity one, such as 5G in the Telco industry.

3.4.1 eGov

eGovernment is the application field that mostly adopt digital identity solutions. Being digital identity very pushed by the European Commission, the most common thing is that the first customer deciding to rely on this could only be the governments of the various EU countries. In fact, as results in the Table 3.4 highlights, there are 89 out of 120 which are adopted by customers of eGov industry,

meaning 74% of the projects of the whole census. Probably the main trigger was induced by EU in 2014 when the eIDAS¹⁰ regulation was created.

3.4.2 Finance

Looking at the results showed in the Table 3.4, the financial application field place as second adopter of digital identity solutions. The number of projects sample belonging to the financial sector is 37, corresponding to a 31% of the whole census. As seen in the Literature chapter, the PSD2 and the AML regulation affect a lot the decisions taken by the companies of this sector to choose digital identity solutions.

3.4.3 Healthcare

Considering the results showed in the Table 3.4, the healthcare application field place as third adopter of digital identity solutions. The number of projects sample belonging to the healthcare sector is 32, corresponding to a 27% of the whole census. As introduced in the Literature chapter, one of the main problems in this sector is how managing with the needed privacy and accuracy patient data in an hospital, for instance. The adoption of digital identity very likely is what have been considered as a solution, since the significant percentage of digital identity projects adopted by companies of the healthcare sector.

3.4.4 eCommerce & Retail

Looking at the results showed in the Table 3.4, the eCommerce & retail application field place a good adopter of digital identity solutions. The number of projects sample belonging to the eCommerce & retail sector is 18, corresponding to a 15% of the whole census. Being a sector involving an incredible set of customers, both B2B and B2C, it has many reasons to decide pursuing the digital identity trend, among which giving to the accounts of users, in the eCommerce for instance, a higher level of security.

¹⁰ The eIDAS regulation aims at providing a common normative basis for secure electronic interactions between citizens, businesses and public administrations and at increasing the security and effectiveness of electronic services and e-business and e-commerce transactions in the European Union. <https://www.agid.gov.it/en/platforms/eidas#:~:text=The%20eIDAS%20regulation%20aims%20at,transactions%20in%20the%20European%20Union>.

3.4.5 Education

Focusing on the results showed in the Table 3.4, the education application field is another active adopter of digital identity solutions. The number of projects sample belonging to the education sector is 16, corresponding to a 13% of the whole census. In the education sector the digital identity can be very useful by, for example, giving a digital representation of all the actors belonging to this field as users (teachers, students, full-time staff, etc). The trend is still in the early phases, but education has the potential, if supported with adequate investments, to convert in one of the most evolved sectors thanks to a significant adoption of digital identity solutions.

3.4.6 Telco & Mobility

Looking at the results showed in the Table 3.4, telecommunications and mobility application fields are also adopter of digital identity solutions. The number of projects sample belonging to the telco and mobility sectors is the same, 11, which is corresponding to a 9% of the whole census, per each of these two sectors. The reason why companies belonging to these sectors have started investing in digital identity solutions is:

- in the case of telco sector, for being more attractive in terms of security, a topic that is always of worth and specifically. Also, looking at the IoT industry, which is investing a lot on 5G, the digital identity can be seen as an instrument enriching positively user experience.
- In the case of mobility sector, thinking of the car sharing world, it would be amazing one day to have the possibility to rent a car or lease it through services that guarantees user identity.

3.4.7 Enterprise and Tourism & Travels

Considering what have emerged from the results showed in the Table 3.4, enterprise and tourism & travel application fields are young adopter of digital identity solutions. The number of projects sample belonging to the enterprise and tourism & travel sectors is the same, 9, which is corresponding to 8% of the whole census, per each of these two sectors. The reason why companies belonging to these sectors have started investing in digital identity solutions is:

- in the case of enterprise sector, for improving/maintaining a high level of reputation thanks security guaranteed by digital identity solutions.
- In the case of tourism & travel, hotels and many other structures belonging to this sector need to adapt to the changing required by the market in order to stay competitive, and being more digital, by offering digital solutions for the identification is a good start.

3.4.8 Humanitarian Scope

Focusing on the results showed in the Table 3.4, the humanitarian application field is the least active adopter of digital identity solutions. The number of projects sample belonging to the education sector is 3, corresponding to a 2,5% of the whole census. In the humanitarian sector the digital identity can be very useful by, for example, giving a digital representation of all the actors belonging to this field as users (needy, immigrants, war fugitives, etc). The trend is still in the very basic early phases, as census results showed.

3.4.9 Application field of projects

Considering the projects analysed in the *Annex* chapter called *Population Coverage*, it is possible to look at the distribution of fields of application, each project covers in the Figure 3.9.

| | General Purpose | eCommerce & Retail | Finance | Telco | Healthcare | Travel & Tourism | eGov | Enterprise | Humanitarian Scope | Mobility | Education |
|--------------------------|-----------------|--------------------|----------|----------|------------|------------------|----------|------------|--------------------|----------|-----------|
| itsme | | X | X | X | X | X | X | X | | X | X |
| SPID | | | X | X | X | | X | | | | X |
| SwissID | | X | X | | X | X | X | | | X | |
| mojeID | X | X | | | X | X | X | | | X | X |
| BankID | | X | X | | X | | X | X | | | |
| FranceConnect | | | X | | X | | X | | | X | |
| Projects / Sector | 1 | 4 | 5 | 2 | 6 | 3 | 6 | 2 | 0 | 4 | 3 |

Figure 3.9 Fields of application per project

Looking at sectorial distribution of projects can be noticed whether a project is general purpose oriented whether vertical oriented. Being these 7 projects some of the most advanced in the European Union, they are all general purpose since they are distributed along with many fields of application.

3.4.10 Application fields and technologies

Looking at sectorial distribution of technology, it is possible to notice a quite imbalance distribution of technologies among those in the Figure 3.10.

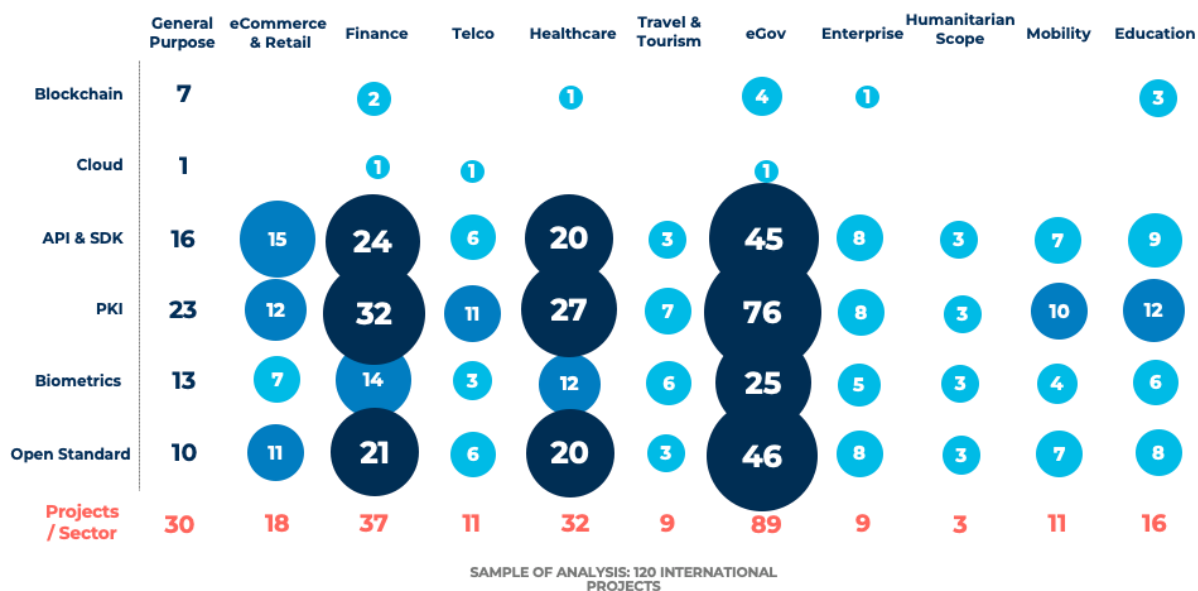


Figure 3.10 Distribution of technologies among industries

The technology most utilized in almost every sector is PKI (reflecting how managing certificate is important for the digital identity systems), except for the eCommerce & Retail sector in which API dominate (due to the interoperability that companies' system needs). At the second place API and Open Standard take turns in the sectors (the first one for the interoperability needs and the second supporting PKI), even though in the healthcare sector also the blockchain is quite used, probably due to the high sensitivity of data.

3.5 Providers & Economic Sustainability

In this chapter are presented the results referring to Providers of identity and services, having a focus on the economic sustainability as well.

3.5.1 Service Providers

A fundamental role when analysing digital identity projects is covered by the service provider, which guarantees to the final user the service that will allow the digital identification towards different ecosystems and platforms. In the Table 3.5 are gathered some the projects sample, randomly selected. Per each project it is reported the number of services available. This number varies from few tens to almost 1000 times more (9607 service providers for the Italian digital identity). Based on the number of service providers can be denoted the relevance of a digital identity. In fact, the more are the service providers the more are the possibilities of selection for the final users. Therefore, from a customer point of view is preferable to have many services providers. Based on that, PortenID, FranceConnect, yes and SPID would be more preferable digital identity than the other ones, from user point of view, since the formers would guarantee a wider access to services.

| PROJECT | NR. SERVICE PROVIDERS |
|--------------------------------|-----------------------|
| PortenID (Norway) | 1000+ |
| BankID (Sweden) | 600 |
| FranceConnect (France) | 1400+ |
| itsme (Belgium) | 258 |
| SPID (Italy) | 9607 |
| yes (Germany) | 1000+ |
| SwissID (Switzerland) | 34 |
| mojeID (Czech Republic) | 223 |

Table 3.5 Number of Service Providers per project

3.5.2 Public vs Private SP

The service provider role can have a double connotation:

- Private
- Public

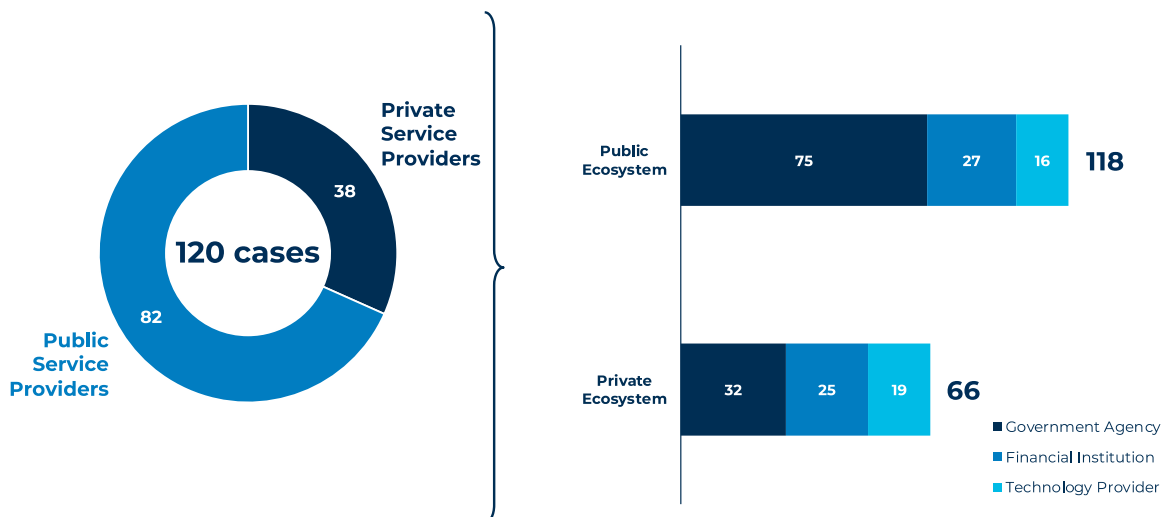


Figure 3.11 Presence of Private and Public Service Providers among 120 International Cases

In the Figure 3.11 it is made explicit that within 120 sample projects there is a quite imbalance regarding the type of providers adopted. In fact, there are 82 out of 120 projects that only use Public Service Providers, corresponding to the 68% of the projects. On the other hand, there are 38 out of 120 projects using either only Private Service Providers or both typologies of providers, corresponding to 32% of the projects.

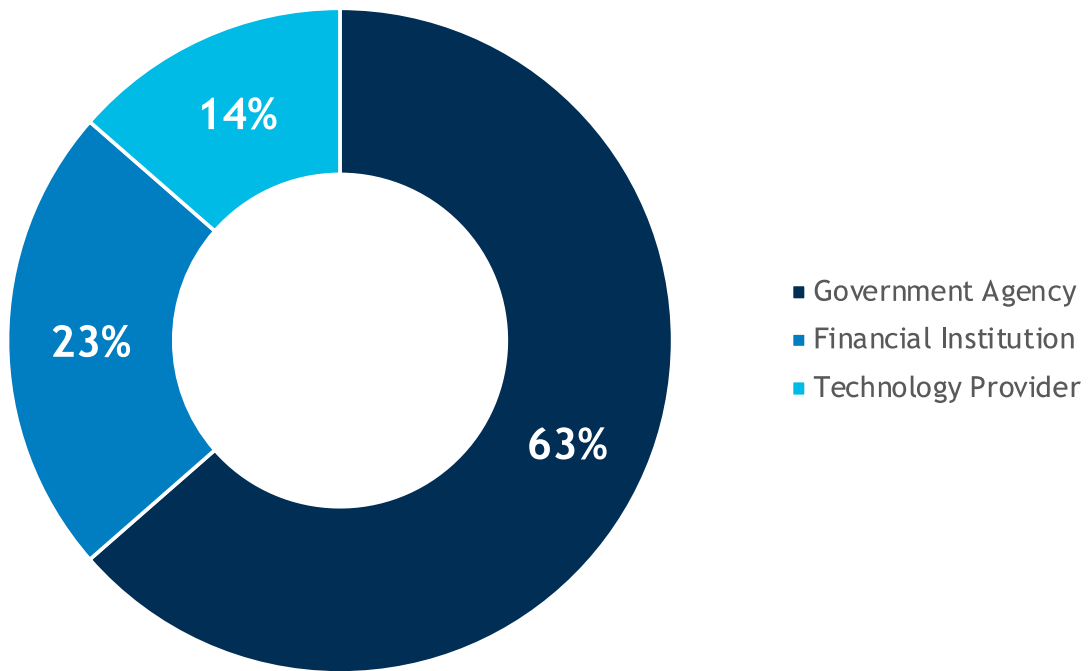
The reason why there is a huge majority of projects contracting only Public Service Providers is that most of the services are restricted to the governmental area, aimed at identifying and recognising individuals to enable administrative or bureaucratic operations. Indeed, looking at the ecosystem it results quite clear that both the projects supported by public providers and the projects employing private providers have an indisputable majority of cases for which the ecosystem of relevance is that of governmental agencies. The presence of the financial ecosystem is very important as well, since banks and other financial institutions due to regulations compliance (such as PSD2, explained in the Literature chapter) need to be supplied with services able to recognise people, letting individuals identify themselves through the service provided.

Finally, a small portion is also reserved for technology providers. Technology service providers offer technology services, often Software-as-a-Service (SaaS), to specific market segments or industries serving hundreds of thousands or even millions of customers per year. These services typically include document-based transactions that require signature. They also include deep integration with company systems and customizations such as SSO (Single Sign On) integration. The reason why in the technology ecosystem there is a few presences of service providers is mainly due to the spreading delay that characterize this sector, as already explained in the industries application paragraph, when talking about Telco industry.

The reason why there are more public SP than private ones is that the digital identity, at its beginning, has been pushed for governmental scope, but progressively it has been understood the usefulness of having private services as well, which guarantee the acceleration of diffusion of the digital programme.

So nowadays there are private service providers also in the governmental ecosystem, as confirmed in the result of the Figure 3.11.

Public Service Providers

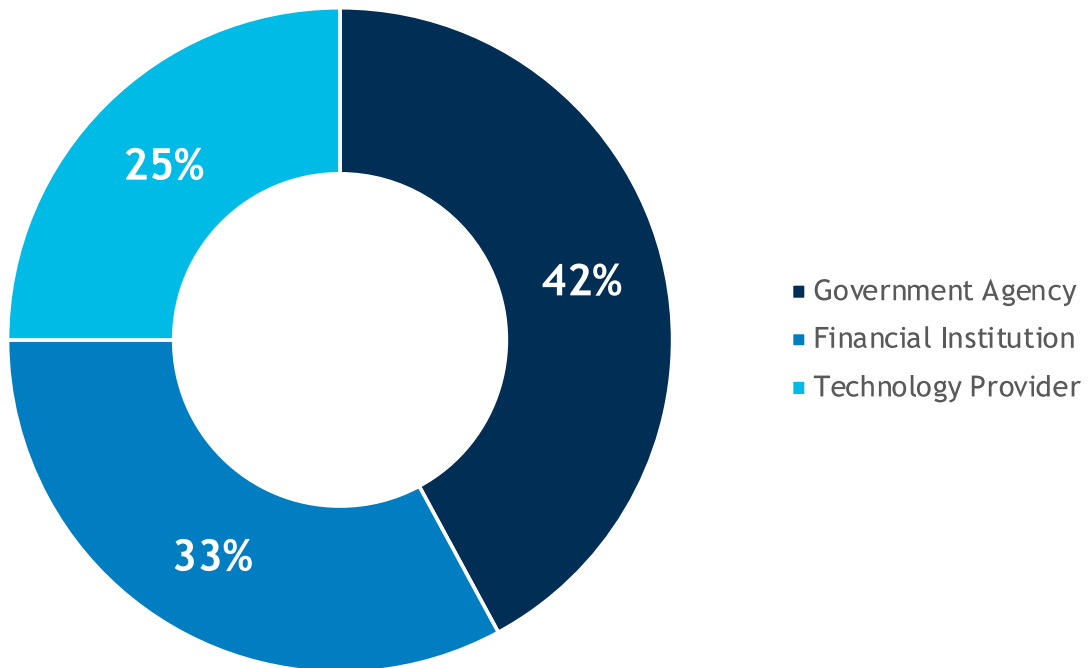


SAMPLE OF ANALYSIS: 120 PROJECTS

Figure 3.12 Public Service Providers

Looking at the Figure 3.12, it can be observed a zoomed result for public service providers, specifically, the Government Agency represents 63%. This means that considering the 82 projects employing only Public Service Providers, 63% of these projects have at least a governmental scope. Then, Financial Institution covers 23%, while Technology Providers the remaining 14%.

Private Service Providers

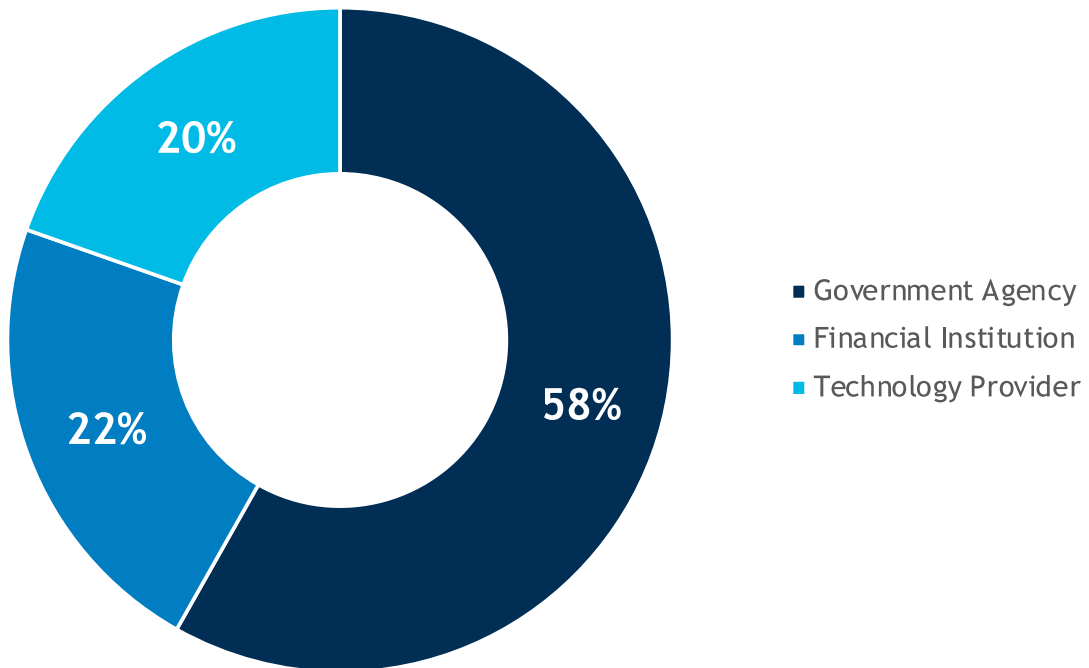


SAMPLE OF ANALYSIS: 120 PROJECTS

Figure 3.13 Private Service Providers

Looking at the Figure 3.13, it can be observed a zoomed result for public service providers, specifically, the Government Agency represents 42%. Quite less with respect the Public Ecosystem, but still representing the majority. Then, Financial Institution covers 33%, a significant higher percentage considering the Public Ecosystem. This is quite expected, since Financial Institutions are usually private entities. Finally, Technology Providers accounts for 25%. The reason why also Technology Provider presence has increased is due to the same reason for Financial Ecosystem, namely, even Technology Provider benefits when the sector is the private one.

Public & Private Service Providers



SAMPLE OF ANALYSIS: 120 PROJECTS

Figure 3.14 Public & Private Service Providers

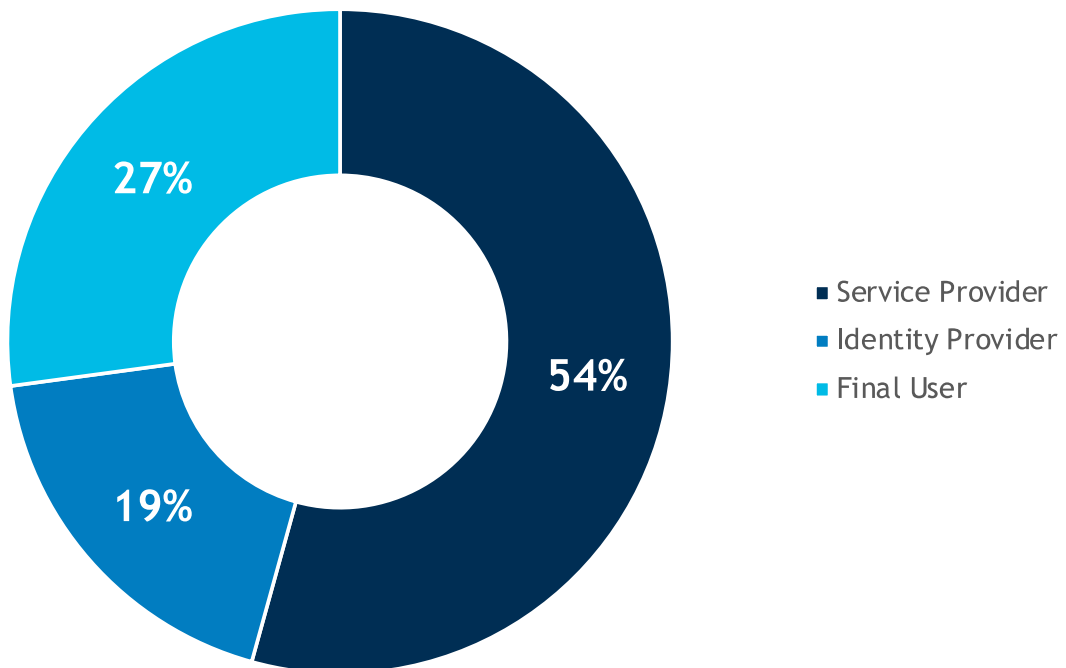
It is useful also to look at the ecosystem level how the distribution becomes when there is not the condition of the service provider driving the data. By looking at the Figure 3.14 can be noticed that the Government Agency represents 58%, it means lower than the distribution including only Public Ecosystem, but higher than the distribution including only Private Ecosystem and above all always being in the first place. Then, Financial Institution covers 22%, quite lower percentage considering the Private Ecosystem, even if only a bit lower when taking into account the Public Ecosystem. Finally, Technology Providers accounts for a 20%, which is quite lower if only considering the Private Ecosystem, but also quite higher with respect the only Public Ecosystem.

3.5.3 Economic Sustainability

The last part of the analysis focused on economic sustainability regarding digital identity system. It is important to spot the actors inside the digital identity world taking on the economic sustainability. The main players are:

- Service Provider, which is an entity that uses the identity provided by the identity provider to verify the identity of the user (whether authentication or first recognition).
- Identity Provider, who is an entity creating and managing the virtual identity of final users on behalf of Service Provider, in fact, Identity Provider is usually paid by the latter.
- Final User, the company or the individual getting a digital identity, thanks to which will be able to benefit from the services offered by the Service Provider.

Economic Sustainability



SAMPLE OF ANALYSIS: 120 PROJECTS

Figure 3.15 Economic Sustainability

As shown in the Figure 3.15, the burden of economic sustainability often falls on Service Providers. In fact, based on the analysis gathered, Service Providers in 57% of the cases are accountable for the

economic sustainability, which means that they pay a fee to the Identity providers. Then, the second category is the Final User, standing for the 27% of the cases as accountant for the economic sustainability. It means that the Final User is paying to receive the service (from the Service Providers), which allows the Final User to be virtually identified by Identity Providers. Finally, the third case is when the Identity Provider is the cost bearer, that occurs in 19% of the cases. This is meaning that Service Providers are not paying the Identity Provider or maybe are not paying that much to cover Identity Provider's costs.

4. CONCLUSIONS

This chapter reports a sum-up of the results, described in the previous ones. Summarising the output of the descriptive analysis on the sample, it will be possible to identify important characteristics of the Digital Identity ecosystem, finding the answers to the research question of the work. The chapter will be concluded by explaining the limitations of the thesis and giving some starting point for deeper future research.

It can be stated this work is one of the first attempts developed with the objective to build a solid and current picture of digital identity trend, through the collection and examination of data. The outcome described in the previous chapters gives an overview on the international state of art for digital identity projects. These projects are mainly localized in European countries. In fact, the analysis showed 84 out of 120 projects in Europe, because of the European bias found out along with the research. For instance, the language limitation that did not allow to retrieve important information about Asian and Russian projects, for whom Digital Observatory Innovation experts confirmed a digital identity trend similar to the European one, in terms of diffusion, effort and technologies. Moreover, the European legislations that came into force in the last 10 years. Some examples could be the eIDAS and the PSD2 regulations, which contributed accelerating the innovation process in the digital identity sphere and therefore, creating an innovation gap with other world areas, such as the Americas, Oceania, and Africa.

However, in 2020 an event occurred, which contributed to accelerating even more the digital identity innovation. This event was the pandemic Covid 19, thanks to which, digital identity services saw a powerful growth in terms of adoption and use. This led to a large increase of the population adopting digital identity services. The research confirmed that for almost all the projects' outcomes. In this specific case, no bias was noticed since the pandemic Covid 19 spread indiscriminately over the whole world.

The analysis on technologies demonstrated how much PKI and API&SDK are important in the digital identity ecosystem. The former highlights the relevance of a secure identification of the entities, by guaranteeing secure data communication in unsecure networks, such as Internet. Also, it covers a primary role as that of digital certificate establisher of rules of encryption and decryption of data, exchanged among users, companies and providers. As regards the latter (API&SDK), it reminds how the interoperability between systems is one of the most relevant aspects for companies nowadays. Blockchain is used by few projects, proving that companies are still working to find the right way to exploit its real potential. Cloud confirmed the good potential of combination with digital identity, with the possibility of creating an improvement in the technology industries, but it still lacks expertise and practice to be better spread.

Looking at Open Standards, in the research OIDC resulted more utilized than SAML. The reason why OIDC is more used than SAML (+15% in the 55 considered samples) is because it is easier than SAML to get up and run. Also, it adapts better with API interfaces, which are always included in the 55 projects examined. If the choice was based only on these mentioned parameters, then every project would have enough by implementing OIDC only. Nevertheless, the other part of results showed that SAML technology is usually preferred by big companies which look for highest security standards, that SAML covers better than OIDC.

Focusing on biometric recognition, face and fingerprint remain the dominant factors in terms of numerosness and funding. In the middle, Palm, Iris and Fingerbone, not totally consolidated solutions yet. The other three solutions (Behaviour and Voice) are still in the developing phase, and they will need time to affirm themselves in the market, which means adopted in some digital identity project.

Looking at the identity types, the Sovereign Identity is foremost present, accounting for 68% of the projects. The reason behind this undiscussed majority is that in a system of sovereign identities, the user who holds the identity always has complete and sovereign authority over it, and this allows the user to share data with third parties securely and without exposing himself to unwanted data leaks. The most found out match was Sovereign Identity and Centralized Architecture, which is due to the high level of security these two technologies guarantee when implemented in a same project. Considering the Functional Identity, it matched more with Federated Architecture, since both technologies are built with the scope of connecting to as services providers much as possible. Lastly, the SSI identity, which only matched with projects including a Decentralised Architecture. The reason is simple, the Self Sovereign Identity is a decentralised digital identity model based on Blockchain technology, which being an innovative architecture is not spread yet.

The analysis of the sectors of application spots that in the majority of the projects are adopted vertical purpose propositions, targeting specific sectors. The sector discovered as the dominant one was the eGov, being digital identity very pushed by the European Commission, so the first customers deciding to rely on the implementation of digital identity systems, were the governments of the various EU countries. Then the financial application field, underlining the relevance of the PSD2 regulation compliance, followed by healthcare and eCommerce & Retail, that with education are among the sectors more impacted by the Covid 19 pandemic, which could be one of the possible factors of development. As regards the general purpose, namely, it was not targeting specific sectors, but developing solutions suitable for different kind of contexts, in the research emerged only a 23% of projects, satisfying such characteristics.

As regards the Service Providers it was discovered a trend showing more public SP than private ones. This is because digital identity was at the beginning almost exclusively pushed in a governmental environment for providing eGov services. But in the last years the trend changed, seeing now private industry growing fast and investing more than public sector. Finally, the economic sustainability was examined. The outcomes showed the service providers in 57% of the cases are accountable for the economic sustainability, which means that they pay a fee to the Identity providers. Then, followed respectively the final user and the identity provider. This means that also the final user can pay to receive the service (from the Service Providers), which allows the final user to be virtually identified by identity provider. Then, the case when the identity provider is the cost bearer, could mean that they do not get profit from Service Providers are not paying the Identity Provider or maybe the service provider is not corresponding that much to the identity provider to allow it to cover its costs.

From this significant quantity of information extracted from the work, is possible to answer to the question research, since a clear picture of the current active systems that are present in the international landscape was provided.

4.1 Limitations and future research

The methodology presented in the results chapter has been designed and reviewed during the work to obtain a research process as rigorous and replicable as possible, in order to create a reliable source of information on the Digital Identity ecosystem. It is important to take into considerations the limits regarding resources and data collection, and possible bias introduced.

The first bias is represented by the difficulty of finding recent information for every one of the 120 projects taken under examination. Unfortunately, not every information is reported in English by the international countries, that are not English speakers. In fact, thinking of China, Japan, Russia, South Korea, Kenya and many more, the information collected for the projects run in these countries were reduced to the minimum terms. Furthermore, on the other side, there were many projects in early stages (announcement or PoC), in areas such as Americas and Oceania. Here the bias was due to low pushing and low effort in investing on digital identity technologies. The unbalance was mainly caused by a sort of unfair and devoted commitment that some area such as the European Union was implementing a lot of regulations and legislations since 2014, with the only objective of developing and make growing fast the technology able to support digital identity. The eIDAS, PSD2, AMLD5 and GDPR are the main regulations came into force.

Seen the difficulty of finding interesting material on some countries and their projects, in this work some important case could have been escaped from the list of 120 projects analysed. Also, the number of papers is still reduced to manage creating a fully satisfying map for digital identity, able to lead to a complete comprehension of the technology and above all, the main drivers able to drive digital identity to a next step. But on the other hand, this gives the possibility to collect all the possible information under a unique work, that can constitute the base for further future developments. For example:

- The list of projects could be continuously updated in order to understand if the sector is growing in terms of number of projects and in terms of development of technologies.
- Another direction could be analysing more in detailed the most developed and successful projects, by the moment, in order to understand which are the competitive advantages that have helped them in growing more than the others.
- The analysis of the most digital country (Estonia) could open to new directions in terms of main drivers to be pursued.
- The technical information collected per each project could be updated and validated in the future months.
- A regression analysis could discover different performance factors related to the Digital Identity ecosystem, for example explaining which factors are more valuable to help having a higher spread of the digital identity solutions usage.

5. ANNEX

Intro

5.1 Population coverage

Although many projects are launched and the majority manage to reach a fully operational state, this does not mean the project is already spread in a specific geographic area. A project can be defined as spread in a specific geographic area, when it is adopted by a significant percentage of the population. For instance, the coverage of population in a country is a very useful parameter to rely on, in order to establish the level of dissemination of a project. Because of trends of last years, mainly due to pandemic Covid 19, digital identity services saw a powerful growth in terms of adoption and use. This led to a large increase of the population adopting digital identity services. In the figure 3.5 is shown how some of the most reliable, famous, and performing projects have been growing in terms of population coverage in the last 3 years (international systems not based on smartcards are included in the chart, so digital use only).

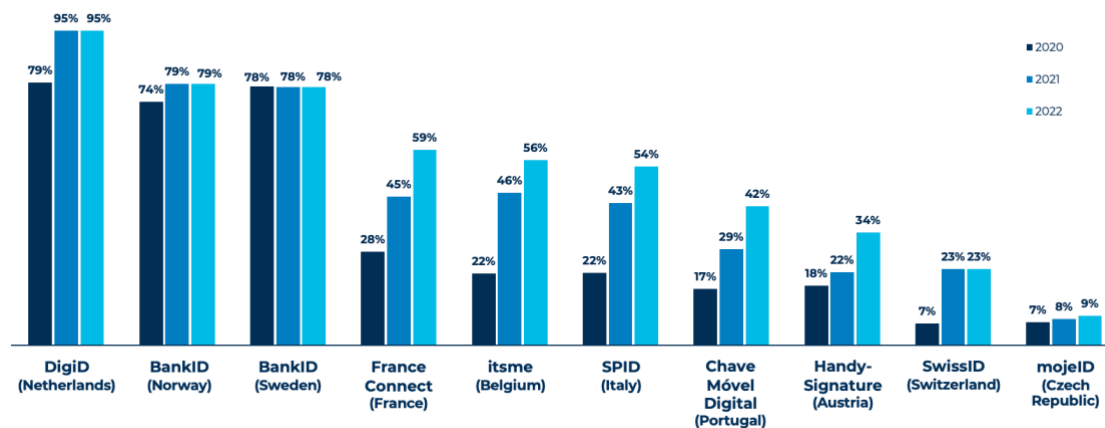


Figure 5.1 Population coverage in digital identity projects in the last three years

Following the analysis one by one per each of the projects in the Figure 5.1:

1. **DigiD (Netherlands):** It is a service that allows self-identify recognition and online arrangement of matters, primarily aimed at governmental and financial ecosystems. DigiD is similar to a digital passport. As a result, DigiD does everything possible to keep

DigiD accounts secure and to prevent fraud. DigiD has been notified by eIDAS. There are several ways to log in to DigiD¹¹:

- DigiD App, which eliminates the need to remember a password. All that is required is a PIN code selected by the user.
- SMS Verification, which enables secure login in two steps using an SMS code.
- Username and password, the most basic and least secure login method. When a user applies for a DigiD account, a username and password are generated.
- Identity Card, logging in with the identity card means granting access to particularly sensitive data. Data is fully safeguarded.

Today 16.7 million Dutch have a digiD. As it can be noticed from the Figure 5.1, digiD has grown by 16% from 2020 to 2021, while it kept stable in 2022. Obviously, the growth in 2021 is a consequence of COVID-19 pandemic, which accelerated a lot the adoption process of digital identity solutions by the population. Nevertheless, digiD was already significantly spread in Netherlands, since in 2020 it had a population coverage of 79%. Having reached one year ago an important result (95% of coverage of population), of course both in this year and in the next ones, the growth until reaching 100% is expected to be slower.

2. **Bank ID (Norway):** it is a personal and simple electronic ID for secure identification and online signing. BankID meets the official requirements for identity verification and binding electronic signatures. BankID is used by all the country's banks, public digital services, and a growing number of businesses in a variety of industries. BankID is eIDAS notified.¹²

Today 4.3 million Norwegians have a BankID. Looking the Figure 5.1, BankID has grown by 5% from 2020 to 2021, while it kept stable in 2022. Even the growth of BankID in 2021 is a consequence of COVID-19 pandemic. However, BankID was already quite spread in Netherlands, since in 2020 it had a population coverage of 74%. Having reached one year ago an important result (79% of coverage of population), in the next years BankID has the potential to grow by 10/15% more, since the digital identity trend does not stop to accelerate its penetration process in the IT industries and not only.

3. **Bank ID (Sweden):** it is the digital identity service used by Swedes to sign contracts, loan documents, and tax returns. People identify themselves in order to pay securely on the internet, log in with *försäkringskassan* (the Swedish Social Insurance Agency), or pick up packages from the postal service. BankID enables quick and secure identification, allowing society to progress without putting businesses or people's privacy at risk. BankID is used for identification and signatures at Sweden's largest banks, businesses, and government agencies. In terms of certification and management systems, the technical infrastructure, as well as its operation and maintenance, are ISO27001:2013 certified. BankID employs a risk-based management system in accordance with ISO 27001:2013, COBIT, and other electronic identification standards/best practices such as eIDAS and SEL.¹³

Today 8.2 million Swedes have a BankID. Considering the results of the Figure 5.1, BankID has not grown in 2021 and 2022. Very likely the effects of COVID-19 pandemic were more

¹¹ DigiD <https://www.digid.nl/en>

¹² BankID eIDAS notified <https://www.bankid.no/globalassets/dokumenter/apne-sider/bankid/bankid-certificate-profiles-for-eidas-3.0.pdf>

¹³ BankID <https://www.bankid.com/en/utvecklare/guider>

visible by comparing 2019 with 2020, since 78% of population coverage is a great result. Here a similar reasoning as for Norway can be done. Basically, in the next years BankID has the potential to grow more. Nevertheless, there is an important trend, looking at the first three results (Netherlands, Norway, Sweden). All these countries were investing more asset and money, with respect the European average, on digital solutions development a couple of years before the COVID-19 came. This is confirmed by the fact they have not grown that much in the last 2/3 years.

4. **France Connect (France):** it is the French government's solution for protecting and simplifying access to over 1,400 online services.¹⁴ France Connect provides digital services in the following categories: financial, citizenship, health, transportation, retirement, job, energy, renting, and family. France Connect also includes digital signature support and currently provides six different ways to connect using an existing account. There are several options, including impots.gouv.fr, ameli.fr, Identitié Numérique La Poste, MobileConnect et moi, msa.fr, and Yris. FranceConnect is eIDAS notified.

Today about 40 million French use FranceConnect. Observing the results of the Figure 5.1, FranceConnect had an amazing growth both from 2020 to 2021 (+17%) and from 2021 to 2022 (+14%). This means that in only 2 years 31% of France population started approaching, probably for the first time, a digital identity solution. In this case the effects of COVID-19 pandemic were a major cause. Of course, the push of European Union towards digital identity was present even before, but with the emergence of the pandemic, which prevented people to go out from home, France, and other nations as well, by investing on digital identity, killed two birds with one stone. Today, the population coverage for FranceConnect is equal to 59%. Since the pushing seems unstoppable, not only from EU, but also from citizens which increasingly want to manage and exploit services digitally, in a comfortable way, it is reasonable to expect a significant growth in the next years as well.

5. **itsme (Belgium):** is a digital identity that allows users to prove their identity in a secure manner. itsme provides services such as logging into a health insurance fund, confirming a payment to a bank, signing documents, applying to a local authority, and checking the pension online. It also offers a mobile app with the highest level of security for a wide range of applications. itsme provides two-factor authentication (MFA). The smartphone contains no data. To ensure maximum security, itsme encrypts user data for storage and communication with a partner. The user is the only person in the world who knows the 5-digit code because there is no database of itsme codes. Each itsme partner (banks, insurance companies, telecommunications companies, etc.) has a unique connection and employs asymmetric-key cryptography: one key to encrypt the data and another key to decrypt it. itsme is compliant with European regulations on security and privacy, such as eIDAS notified (both for the application and for the Qualified Electronic Signature), ISO/IEC 27001:2013 certified, EBA guidelines, PSD2 guidelines and GDPR guidelines.¹⁵

Today 6.5 million Belgians use itsme. Looking at the results of the Figure 5.1, itsme had a surprising growth from 2020 to 2021 (+24%) and another important increase from 2021

¹⁴ France Connect <https://franceconnect.gouv.fr/>

¹⁵ Itsme <https://www.itsme-id.com/>

to 2022 (+10%). This means that in only 2 years about 34% of Belgium population began using the itsme digital identity, overcoming the incredible French trend with FranceConnect. As per French case, the effects of COVID-19 pandemic made a difference as main trigger. Maybe, having in Brussels the capital of the European Union, influenced as well, as a minor trigger, on the adoption of digital identity. Today, the population coverage for itsme is equal to 56%. Even in this case for already mentioned reasons (see FranceConnect case at point 5), it is very likely that the spread of itsme inside Belgium population grow on.

6. **SPID (Italy):** the "Sistema Pubblico di Identità Digitale" (SPID) allows access to online public services. SPID is one of the identification tools for gaining access to the Public Administration's online services as well as the services of participating private individuals. The key to accessing online services is provided by the government in the form of a unique credential that is activated once and is always valid. Citizens can only submit online applications and declarations to the public administration using SPID, CIE, or CNS, according to Article 65 of the Digital Administration Code. Applications and declarations signed with a handwritten signature affixed in the presence of the employee in charge of the procedure are equivalent in this case. Citizens, businesses, and professionals can use any device to access services, including computers, tablets, and smartphones.

The National Recovery and Resilience Plan (NRP) includes among its goals the deployment of digital identity, with the goal of reaching 70% of the population by 2026. The SPID project, conceived and designed by the "Agenzia per l'Italia Digitale," is driven and coordinated by the Department (AgID).¹⁶ SPID is eIDAS notified.

Today about 32 million Italians use SPID. As it can be seen from the results of the Figure 5.1, SPID is almost as surprising as itsme. Indeed, SPID present an increase in terms of adoption from 2020 to 2021 of +21% and another important increase from 2021 to 2022 of +11%. This means that in only 2 years 32% of Italy population adopted SPID as digital identity, overcoming the amazing result of FranceConnect and getting closer to the one even more incredible of itsme. As per French and Belgian cases, the effect of COVID-19 pandemic played a fundamental role in triggering the digital identity innovation. Today, Italian population coverage for SPID is equal to 54%. Therefore, considering the objective of AGID – reaching 70% of population coverage – SPID seems to have all the makings of a +16% increase in the current percentage of Italian users who have adopted digital identity.

7. **Chave Móvel Digital (Portugal):** it is an authentication and digital signature method approved by the Portuguese government. With a single login, the user can access multiple public or private portals and sign digital documents. The Chave Móvel Digital links a mobile phone number to a Portuguese citizen's civil identification number and a foreign citizen's passport or residence permit/card number. The Chave Móvel Digital is a simple and secure authentication system for Public Administration portals and other websites that requires only two security steps¹⁷:
 - PIN Chave Móvel Digital (chosen at CMD activation).

¹⁶ Gov.it <https://innovazione.gov.it/progetti/identita-digitale-spide-cie/>

¹⁷ Autenticação.gov <https://www.autenticacao.gov.pt/web/guest/a-chave-movel-digital>

- A numeric and temporary security code obtained through one of the following channels:
 - o SMS notification
 - o notification via the Authentication.gov mobile application
 - o email
 - o Twitter direct message
 - o QR code scanning via the Authentication.gov mobile app

Today 4.4 million Portuguese use CMD. Analysing the results of the Figure 5.1, CDM is characterised by a significant growth in terms of digital identity adoption in the last 2/3 years. In fact, CDM increased by +12% from 2020 to 2021 and it had another significant growth from 2021 to 2022 of +13%. Having a rise of +25% in just 2/3 years is a superlative result. As per above cases, the effect of COVID-19 pandemic was a predominant consequence in pushing the digital identity innovation. Today, Portuguese population coverage for CDM is equal to 42%. Therefore, CDM has an enormous margin of spread for what concerns the future adoption of CDM.

8. **Handy-Signature (Austria):** It is a service that allows users to have their own online signature. It is analogous to a handwritten signature and serves as the user's digital identity on the internet. Handy-Signature provides access to over 200 business and government E-Services.¹⁸ Handy-Signature uses A-Trust qualified certificates to sign PDF documents. A valid certificate is required to use your digital ID card to renew mobile phone signature. For security reasons, this expires five years after activation and must be renewed or applied for again. Currently, 3 million Austrians use Handy-Signature. Considering the results of the Figure 5.1, Handy-Signature had a good growth in terms of digital identity adoption in the last 2/3 years. In fact, Handy-Signature increased by +4% from 2020 to 2021 and it had another significant growth from 2021 to 2022 of +12%. Having increased of +16% in just 2/3 years is a good starting point. COVID-19 pandemic was the main influencer, in pushing the digital identity innovation, in this case as well. Today, Austrian population coverage for Handy-Signature is equal to 34%. Therefore, Handy-Signature has a very high margin of diffusion that can be enhanced by pursuing investment for improvement of Handy-Signature thus having a bigger involvement of the potential users in the next years. Handy-Signature is eIDAS notified.
9. **Swiss ID (Switzerland):** is Switzerland's digital identity, allowing for simple and secure online access. Online transactions can also be legally completed with the digital signature SwissID Sign. Data can be encrypted and thus exchanged securely with the help of electronic certificates. SwissSign, as a Swiss Trust Service Provider (TSP), protects and stores all data in Switzerland in accordance with the highest security standards. Here are some of the reasons why Swiss ID is a trustworthy digital identity service¹⁹:
 - Cross-industry ecosystem, SwissID is present in all sectors, whether public authority, private company, or online shop.
 - higher conversion rates, no need to remember usernames or passwords, and thus higher completion rates

¹⁸ A Trust https://www.a-trust.at/de/produkte/Qualifizierte_Signaturservices/Handy-Signatur/#!infos/tour

¹⁹ SwissID <https://www.swissid.ch/signieren.html>

- Swiss precision, all data is stored in Switzerland.

Nowadays, more than 2 million users rely on SwissID thanks to an increasing number of online services. SwissID is eIDAS notified. Focusing on the Figure 5.1, SwissID had a partial growth in terms of digital identity adoption in the last 2/3 years. In fact, SwissID increased by +16% from 2020 to 2021 and no growth from 2021 to 2022. Having increased of +16% in just 2/3 years is a good starting point, but it worries that during the last year the growing trend has stopped. During the rise of 2020-2021, obviously the COVID-19 pandemic was the main pusher of the digital identity innovation. The fact that in 2020 the level of adoption of Swiss ID was at 7%, let understand that before the pandemic this innovation field was neglected. Today, Swiss population coverage for SwissID is equal to 23%. Therefore, as for Handy-Signature, SwissID has a very high margin of diffusion as well, that can be reached by investing more on digital identity. If this will be done, potential new users' adoption will become more likely in the next years.

10. **MojeID (Czech Republic):** It ensures a secure online identity. The mojeID account is safe, and it allows users to access thousands of private and public services. In a standard registration, the user's registration details are saved at the service provider, and the user has no assurance that the provider adheres to any security standards when handling this data. With mojeID, user information is stored under the same security conditions as the top-level domain CZ register. When users sign in with mojeID, the service provider never receives the user's password, eliminating the possibility of it being misused. Users need another authentication factor besides a password to access public administration services using mojeID, such as the *MojeID KI* app or another security key based on tokens and/or authentication keys.²⁰

Today, almost 1 million users rely on MojeID that is eIDAS notified. Focusing on the Figure 5.1, MojeID had a minimum growth in terms of digital identity adoption in the last 2/3 years. In fact, MojeID increased by +1% from 2020 to 2021 and the same occurred from 2021 to 2022. Having increased of +2% in just 2/3 years is a countertrend, since almost all the other European Countries had better growing results. In this specific case it seems that neither the COVID-19 pandemic was able to push and trigger in an effective way the digital identity innovation in Czech Republic. The fact that in 2020 the level of adoption of MojeID was at 7%, let understand that before the pandemic this innovation field was neglected as happened to SwissID. Unlike for SwissID, MojeID had not exploited the "pandemic chance" to improve digital identity technology and user involvement. Today, Czech population coverage for MojeID is equal to 9%. Therefore, in this case the potential margin of diffusion goes without every imagination, even if it must be supported by scientific enhancement and economic investment, otherwise the level of adoption of digital identity will not increase that much.

²⁰ MojeID <https://www.mojeid.cz/en/egovernment/>

Bibliography

1. Craig W. Thompson and Dale R. Thompson | University of Arkansas (2007) "Identity Management"
2. Robin Wilton (2008) "Identity and privacy in the digital age"
3. Sedlmeir J., Smethurst R., Rieger A., Fridgen G. (2021) "Digital Identities and Verifiable Credentials"
4. World Economic Forum Report (2018) "Identity in a Digital World"
https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf
5. World Economic Forum Report (2016) "A Blueprint for Digital Identity"
https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf
6. Wayman J.L. (2008) "Biometrics in identity management systems", IEEE Security and Privacy, vol.6, pp. 30-37. Doi: 10.1109/MSP.2008.28
7. IBM (1970) "The Consideration of Data Security in a Computer Environment, tech. report G5202169"
8. Hatef Rasouli and Changiz Valmohammadi (2019) "Proposing a conceptual framework for customer identity and access management: A qualitative approach"
https://www.researchgate.net/publication/334780101_Proposing_a_conceptual_framework_for_customer_identity_and_access_management_A_qualitative_approach
9. Digital Identity Observatory of Politecnico di Milano
10. PricewaterhouseCoopers (2022) "Digital Identity @ PwC"
<https://www.pwc.com/it/it/services/consulting/assets/docs/digital-identity.pdf>
11. Waldmann U., Vow S., Sven T. and Poller A. (2012) "Electronic Identity Cards for User Authentication: Promise and Practice", IEEE Secur., 10, 46–54.
12. US Dept. of Health Education and Welfare (1973), "Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems", available at: www.epic.org/privacy/hew1973report/
13. R., Pérez M., Ramírez G., Montes J. and Bouvarel L. (2020) "An architecture for biometric electronic identification document system based on blockchain", Future Internet, vol.12. Doi: 10.3390/Fi12010010
14. Dib O. and Toumi K. (2020) "Decentralized identity systems: Architecture, challenges, solutions and future directions", Annals of Emerging Technologies in Computing, vol.4, pp. 19-40. Doi: 10.33166/AETIC.2020.05.002
15. Sullivan C. (2018) "Digital identity – From emergent legal concept to new reality", Computer Law and Security Review, vol.34, pp. 723-731. Doi: 10.1016/j.clsr.2018.05.015
16. World Bank Group, GSMA and Secure Identity Alliance (2016) "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation"
17. World Bank Group (2016a) "Technical Standards for Digital Identity"
<https://thedocs.worldbank.org/en/doc/579151515518705630-0190022018/original/ID4DTechnicalStandardsforDigitalIdentity.pdf>

18. Armen Khatchatourov, Maryline Laurent & Claire Levallois-Barth (2015) "Privacy in Digital Identity Systems: Models, Assessment, and User Adoption" https://link.springer.com/chapter/10.1007/978-3-319-22479-4_21#Sec1
19. Clarissa Falcone Osservatori.net Digital Innovation (2020) "2020: un punto di discontinuità per l'identità digitale" https://blog.osservatori.net/it_it/identit%C3%A0-digitale-punto-discontinuit%C3%A0
20. Gartner (2019) "Critical Capabilities for Full Life Cycle API Management"
21. Skračić K., Pale P. and Jeren B. (2017) "A distributed authentication architecture and protocol", *Tehnicki Vjesnik*, vol.24, pp. 303-311. Doi: 10.17559/TV-20151114105745
22. Gerard Hartsink (2018) "The digital identity of legal entities: Current status and the way forward" https://scholar.google.it/scholar_url?url=https://www.gleif.org/_documents/blog/20180530-the-use-of-the-legal-entity-identifier-in-payment-systems/Gerard-Hartsink_The-Digital-Identity-of-Legal-Entities_Current-Status-and-Way-Forward_Journal-of-Payments-Strategies%26Systems_Volume12_Number1.pdf&hl=it&sa=X&ei=KDROY-LxMNqTy9YPuZmDwAY&scisig=AAGBfm32RgOraz2D14LT4guG1lbiw83PJA&oi=scholar
23. Jovanović B., Milenković I., Sretenović M.B. and Simić D. (2016) "Extending identity management system with multimodal biometric authentication", *Computer Science and Information Systems*, vol.13, pp. 313-334. Doi:10.2298/CSIS141030003J
24. Arner D.W., Zetsche D.A., Buckley R.P. and Barberis J.N. (2019) "The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities", *European Business Organization Law Review*, vol.20, pp. 55-80. Doi: 10.1007/s40804-019-00135-1
25. Hu P., Ning H., Qiu T., Xu Y., Luo X. and Sangaiah, A.K. (2018) "A unified face identification and resolution scheme using cloud computing in Internet of Things". *Future Gener. Comput. Syst.* 81, 582–592.
26. Ning H., Liu X., Ye X., Zhang J.H.W. and Daneshmand M. (2019) "Edge Computing Based ID and nID Combined Identification and Resolution Scheme in IoT", *IEEE Internet Things J.*, 6, 6811–6821.
27. Dhelim S., Ning H., Bouras M.A. and Ma J. (2018) "Cyber-enabled human-centric smart home architecture. In Proceedings of the 2018 IEEE SmartWorld", *Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBCom/IOP/SCI)*, Guangzhou, China, 8–12 October 2018; pp. 1880–1886.
28. Bouras M.A., Lu Q., Dhelim S. and Ning H. (2021) "A lightweight blockchain-based iot identity management approach", *Future Internet*, vol.13, pp. 1-14. Doi: 10.3390/fi13020024
29. Pöhn D. and Hommel W. (2020) "An overview of limitations and approaches in identity management. In Proceedings of the 15th International Conference on Availability", *Reliability and Security*, pp.1-10.
30. Srinivasa Reddy Modugula T.S., Vijaya Babu B., Pachala S., Rupa C. and Sumalatha L. (2018) "SAML based context aware IDM a fine-grained proxy re-encryption approach to improve the privacy of users identity data in cloud environment", *International Journal of Engineering and Technology (UAE)*, vol.7, pp. 108-113. Doi: 10.14419/ijet.v7i2.7.10274
31. Amoli G., Kala M. and Chaurasia J. (2019) "Comprehensive Security Analysis of Federated Identity Management", *Journal of Communication Engineering & Systems*, 7(1), pp.11-16.

32. Lin C., He D., Huang X., Khurram Khan M. and Choo K.-K.R. (2018) "A New Transitively Closed
33. Undirected Graph Authentication Scheme for Blockchain-Based Identity Management Systems", *IEEE Access*, vol.6, pp. 28203-28212. Doi: 10.1109/ACCESS.2018.2837650
34. Lin X. (2020) "New Innovations in eIDAS-compliant Trust Services: Blockchain" (Bachelor's thesis, Universitat Politècnica de Catalunya).
35. De Angelis F., Falcioni D., Ippoliti F., Marcantoni F. and Rilli S. (2016) "Federated identity management in e-government: Lessons learned and the path forward", *International Journal of Electronic Governance*, vol.8, pp. 22-38. Doi: 10.1504/IJEG.2016.076683
36. Shim S.S.Y., Bhalla G. and Pendyala V. (2005) "Federated identity management", *Computer*, vol.38, pp. 120-122. Doi: 10.1109/MC.2005.408
37. Sunyaev A. (2020) "Distributed ledger technology", In *Internet Computing*, pp. 265-299, Springer, Cham.
38. Patil A.S., Belhekar S.P., Burkul R.S. and Sambare M.V. (2019) "Review Paper on-Smart Wallet".
39. Andrew Tobin D.R. (2017) "The Inevitable Rise of Self-Sovereign Identity", White paper, Sovrin Foundation.
40. Lim S.Y., Fotsing P.T., Almasri A., Musa O., Kiah M.L.M., Ang T.F. and Ismail R. (2018) "Blockchain technology the identity management and authentication service disruptor: A survey", *International Journal on Advanced Science, Engineering and Information Technology*, vol.8, pp. 1735-1745. Doi: 10.18517/ijaseit.8.4-2.6838
41. Allen C. (2006) "The path to self-sovereign identity", available at: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>
42. Tobin A. and Reed D. (2016) "The inevitable rise of self-sovereign identity", Sovrin Foundation, available at: <https://sovrin.org/wpcontent/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf>
43. Andrew Tobin D.R. (2017) "The Inevitable Rise of Self-Sovereign Identity", White paper, Sovrin Foundation.
44. Sporny M. (2018) "Is Verifiable Credentials sufficiently different from Verifiable Claims?", available at: <https://github.com/w3c/vc-data-model/issues/112>.
45. Mühle A., Grüner A., Gayvoronskaya T. and Meinel C. (2018) "A survey on essential components of a self-sovereign identity", *Computer Science Review*, vol.30, pp. 80-86. Doi: 10.1016/j.cosrev.2018.10.002
46. World Bank Group (2017) "Technical Standards for Digital Identity Systems for Digital Identity" <https://thedocs.worldbank.org/en/doc/579151515518705630-0190022018/original/ID4DTechnicalStandardsforDigitalIdentity.pdf>
47. O'Gorman L. (2003) "Comparing passwords, tokens, and biometrics for user authentication", // *Proceedings of the IEEE*, 91, 12(2003), pp. 2021-2040. <https://doi.org/10.1109/JPROC.2003.819611>
48. Feng W., Zhou J., Dan C., Peiyan Z. and Li Z. (2017) "Research on mobile commerce payment management based on the face biometric authentication", *International Journal of Mobile Communications*, vol.15, pp. 278-305. Doi: 10.1504/IJMC.2017.083463
49. World Bank (2018a) "Private sector economic impacts from identification systems".

50. World Bank (2018b) "Public sector savings and revenue from identification systems: Opportunities and constraints".
51. M. Dabrowski and P. Pacyna (2008) "Generic and complete three-level identity management model", 2nd International Conference on Emerging Security Information Systems and Technologies
52. Netha in "National E-Health Transition Authority, [online] Available: <http://www.nehta.gov.au/>"
53. S.C. Lee, (2003) "An Introduction to Identity Management"
54. HP OpenView Identity Management solution Business blueprint, [online] Available: http://h41087.www4.hp.com/solutions/entreprises/grandes_entreprises/openview/pdf/im_bb.pdf
55. HP OpenView Identity Management Solution Whitepaper <http://www.cbnews.com/uploadfile/whitepaper/2007-01-30/30160032.pdf>
56. J. Li, Chang, C.X. Shen, H. Zhen, Y.Z. He and Y. Liu (2009) "Survey of research on identity management", Computer Engineering and Design, vol. 30, pp. 1365
57. H. Koshutanski, M. Ion and L. Telesca (2007) "Distributed Identity Management Model for Digital Ecosystems", Proc. The International Conference on Emerging Security Information Systems and Technologies (SecureWare 2007), pp. 132-138
58. Yuan Cao, Lin Yang (2010) "A survey of Identity Management technology" https://ieeexplore.ieee.org/abstract/document/5689468?casa_token=TZC-Q1oz_uUAAAAA:OPt-dIS6o4ILFdA_k-S0ZuTwJeBSyLvYc1lXgSJPmdCN7JldCUOKdbLQkvrSKDfFKBJNu1A
59. T. Ruff (2018) "The three models of digital identity relationships" <https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186>
60. P. Windley (2017) "Fixing the five problems of internet identity" https://www.windley.com/archives/2017/10/fixing_the_five_problems_of_internet_identity.shtml
61. A. Tobin and D. Reed (2016) "The inevitable rise of self-sovereign identity", The Sovrin Foundation, vol. 29
62. N. Naik and P. Jenkins (2016) "A secure mobile cloud identity: Criteria for effective identity and access management standards", 4th IEEE International Conference on Mobile Cloud Computing Services and Engineering (MobileCloud 2016), 2016
63. N. Naik and P. Jenkins (2017) "Securing digital identities in the cloud by selecting an apposite federated identity management from SAML OAuth and OpenID Connect", 11th International Conference on Research Challenges in Information Science (RCIS), pp. 163-174
64. N. Naik and P. Jenkins (2016) "An analysis of open standard identity protocols in cloud computing security paradigm", 14th IEEE International Conference on Dependable Autonomic and Secure Computing (DASC 2016)
65. N. Naik, P. Jenkins and D. Newell (2017) "Choice of suitable identity and access management standards for mobile computing and communication", 2017 24th International Conference on Telecommunications (ICT), pp. 1-6
66. Verifiable Credentials data model 1.0 (2019) <https://www.w3.org/TR/vc-data-model/>
67. A primer for Decentralized Identifiers (2019) <https://w3c-ccg.github.io/did-primer/>

68. Sovrin (2018) "A protocol and token for self-sovereign identity and decentralized trust"
<https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf>
69. Nitin Naik, Paul Jenkins (2020) "Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology"
https://ieeexplore.ieee.org/abstract/document/9126742?casa_token=X8K_HzL1fDoAAAAA:6A_1Exxp03WSvOyIW-vhNN-SliVBDgpre7dbBiAWaLYWDIbENjzGyyQS7hbMfc0WZZI27dM
70. World Bank Group (2018) "Technology Landscape for Digital Identification"
<https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf>
71. Nyst, C., Makin, P., Pannifer, S., & Whitley, E. (2016) "Digital identity: Issue analysis: executive summary" Consult Hyperion, Guildford
72. Alan Gelb, Julia Clark (2013) "Identification for Development: The Biometrics Revolution"
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2226594
73. World Bank Group (2014) "Digital Identity Toolkit"
<https://openknowledge.worldbank.org/bitstream/handle/10986/20752/912490WP0Digit00Box385330B00PUBLIC0.pdf?sequence=1&isAllowed=y>
74. World Bank Group (2016b) "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation"
<https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf>
75. OneSpan (2022) "Identity Verification" <https://www.onespan.com/topics/identity-verification>
76. Nancie Gunson, Diarmid Marshall, Hazel Morton, Mervyn Jack (2011) "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking"
https://www.sciencedirect.com/science/article/pii/S0167404810001148?casa_token=xjrHXnJZy4QAAAAA:wm6de3UhRoivj-6cQHMWteNIuBPNYqcFQpFV68LKXitnecntzrpT2ylXRz3PXBAZP56S3Wqr
77. L. O'Gorman (2003) "Comparing passwords, tokens and biometrics for authentication"
Proceedings of the IEEE, 91 (12) (December 2003), pp. 2021-2040
<https://www.scopus.com/record/display.uri?eid=2-s2.0-10044293457&origin=inward&txGid=a24c473e993b3dc11018d458aec79dde>
78. Murdoch S, Drimer S, Anderson R, Bond M. (2010) "Chip and PIN is Broken" 2010 IEEE Symposium on Security and Privacy; 2010. doi:10.1109/SP.2010.33
<https://ieeexplore.ieee.org/abstract/document/5504801>
79. Mannan M, van Oorschot PC. (2008) "Security and usability: the gap in real-world online banking" In: Proceedings New Security Paradigms Workshop (NSPW'07), New Hampshire, USA; 2007. p. 1–14. <https://dl.acm.org/doi/abs/10.1145/1600176.1600178>
80. Dipankar Dasgupta, Arunava Roy & Abhijit Nag (2017) "Multi-Factor Authentication"
https://link.springer.com/chapter/10.1007/978-3-319-58808-7_5
81. R. K. Konoth, V. van der Veen and H. Bos (2016) "How anywhere computing just killed your phone-based two-factor authentication", Proceedings of the International Conference on Financial Cryptography and Data Security, pp. 405-421
82. J. J. Kim and S. P. Hong (2011) "A method of risk assessment for multi-factor authentication", J. Inf. Process. Syst., vol. 7, pp. 187-198

83. Sanjar Ibrokhimov, Kueh Lee Hui, Ahmed Abdulhakim Al-Absi, hoon jae lee, Mangal Sain (2019) "Multi-Factor Authentication in Cyber Physical System: A State of Art Survey"
https://ieeexplore.ieee.org/abstract/document/8701960?casa_token=NXyJtlurAjIAAAAA:37-z-ULweu5xnlXmFZ4zOFdM6UZU6abEsvUaO-YMiA7h_Fg7QOq_BdivubhO_ALHosaHtHM
84. Mitek (2021) "What is multi-factor and risk based authentication?"
<https://www.miteksystems.com/blog/what-is-multi-factor-and-risk-based-authentication>
85. Mc Kinsey Global Institute (2019) "Digital Identification: A key to inclusive growth"
<https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>
86. Sylvia Klasovec Kingsmill, Partner KPMG (2022a) "The emergence of digital identity. Trust lies at the heart of today's digital economy"
<https://home.kpmg/xx/en/blogs/home/posts/2022/01/the-emergence-of-digital-identity.html>
87. Silvia Masiero & Savita Bailur (2020) "Digital identity for development: The quest for justice and a research agenda"
<https://www.tandfonline.com/doi/full/10.1080/02681102.2021.1859669?src=recsys>
88. World Development Report (2016) "Digital Identity"
<https://thedocs.worldbank.org/en/doc/822821519686607466-0050022018/original/9781464806711WDR2016Spot4RevOct2017.pdf>
89. KPMG (2022b) "Trust is key to unlocking digital identity, security and data insights"
<https://home.kpmg/xx/en/home/insights/2021/06/trust-is-the-key-to-unlocking-digital-identity-security-and-data-insights.html>
90. Mircea Zloteanu, Nigel Harvey, David Tuckett, Giacomo Livan (2018) "Digital Identity: The effect of trust and reputation information on user judgement in the Sharing Economy"
<https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0209071>
91. AR Friedman, LD Wagoner (2015) "The Need for Digital Identity in Cyberspace Operations"
https://www.jstor.org/stable/26487493?seq=2#metadata_info_tab_contents
92. Enrico Mentasti (2021) "Digital Identity in Italy: challenges and opportunities for the adoption in banking, insurance and utility sectors"
<https://www.politesi.polimi.it/handle/10589/189015>
93. AGID, Agenzia per l'Italia Digitale (2022) "The eIDAS regulation"
<https://www.agid.gov.it/en/platforms/eidas>
94. Marijana Petrović (2020) "PSD2 INFLUENCE ON DIGITAL BANKING TRANSFORMATION - BANKS' PERSPECTIVE"
<https://www.aseestant.ceon.rs/index.php/jouproman/article/view/28153/16218>
95. Steve Mansfield-Devine (2016) "Open banking: opportunity and danger, Computer Fraud & Security", 8-13. [https://doi.org/10.1016/S1361-3723\(16\)30080-X](https://doi.org/10.1016/S1361-3723(16)30080-X)
96. Mc Kinsey Global Institute (2018) "PSD2: Taking advantage of open-banking disruption"
<https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption>
97. Forester H., Rolfe A. & Brown A. (2017) "PSD2 and Europe's Open Banking Mandate – Challenges for Banks and FinTechs, Payments Cards and Mobile Research." NCR corporation.

- <https://www.paymentscardsandmobile.com/wp-content/uploads/2017/09/NCR-PSD2-Report-Final-1.pdf>
98. P.T.J. Wolters B.P.F. Jacobs (2019) "The security of access to accounts under the PSD2"
<https://doi.org/10.1016/j.clsr.2018.10.005>
 99. The Fintech Times (2019) "The State of European Fintech"
<https://thefintechtimes.com/european-fintech/>
 100. Piotr Kuszewski (2018) "Impact of the PSD2 directive and strategic use of costly innovation" <http://dx.doi.org/10.13140/RG.2.2.24263.55207>
 101. T. Vasiljeva & K. Lukanova (2016) "Commercial Banks and Fintech Companies in the Digital Transformation: Challenges for the Future, Journal of Business Management" No.11, 25-33
 102. G. Choi & M. Park (2019) "Reconnecting the Dots for the Payment Service Directive 2" -Compatible Asian Financial Network, East Asian Economic Review, vol. 23, (3), 285-309
<http://dx.doi.org/10.11644/KIEP.EAER.2019.23.3.364>
 103. I. Saarnilehto (2018) "Problems and possibilities of the payment services directive (PSD2)", ProCIEdings of the Seminar in ComputerScience: Internet, Data and Things (CS-E4000), 71-82.
 104. J.S.G Eide & S. Hallum (2018) "PSD2: A Strategic Perspective on Third-Party Payment Service Providers", Master Thesis, BI NorZegian Business School-campus Oslo.
<https://biopen.bi.no/bixmlui/bitstream/handle/11250/2578906/2040606.pdf?sequence=1&isAlloZEd=y>
 105. Forbes (2022) "What Does the Future of Digital ID Look Like?"
<https://www.forbes.com/sites/forbestechcouncil/2022/06/07/what-does-the-future-of-digital-id-look-like/>
 106. European Commission (2022) "European Digital Identity: Online consultation platform on European Digital Identity Wallets" <https://digital-strategy.ec.europa.eu/en/news/european-digital-identity-online-consultation-platform-european-digital-identity-wallets>
 107. International Peace Institute (2016) "Estonia PM: Country Saves 2% of GDP by Going Digital" <https://www.ipinst.org/2016/05/information-technology-and-governance-estonia>
 108. Juniper Research (2022) "USERS OF DIGITAL IDENTITY DOCUMENTS TO EXCEED 6.5 BILLION GLOBALLY IN 2026, ENABLING RAPID ADVANCES IN EGOVERNMENT SERVICES"
<https://www.juniperresearch.com/pressreleases/users-of-digital-identity-documents-to-exceed>
 109. e-Estonia (2022) "e-Residency, Mobile ID, Smart ID" <https://e-estonia.com/solutions/e-identity/mobile-id/>
 110. eIDAS Observatory (2016) "eIDAS Regulation (Regulation (EU) N°910/2014)"
<https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014.html>
 111. European Commission (2022), "Shaping Europe Digital Future" <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>
 112. Osservatori.net Digital Innovation (2021) "European Digital Identity Wallet: la carta d'identità a portata di wallet" https://blog.osservatori.net/it_it/digitale-wallet-identita

113. GDPR.EU (2020) "What is GDPR, the EU's new data protection law?"
<https://gdpr.eu/what-is-gdpr/>
114. Dow Jones (2022) "What is AMLD5 (5th EU Anti-Money Laundering Directive)?"
<https://www.dowjones.com/professional/risk/glossary/anti-money-laundering/amld5-definition/>
115. Cointelegraph (2022) "EU's Anti-Money Laundering Directive 5 (AMLD5)"
<https://cointelegraph.com/cryptocurrency-regulation-for-beginners/eus-anti-money-laundering-directive-5-amld5#:~:text=What%20is%20AMLD5%3F,illegal%20money%20cannot%20be%20laundered.>
116. Electronic Identification (2022) "5AMLD: A Unique Regulation for Europe's Digital Space" <https://www.electronicid.eu/en/blog/post/amld5-new-anti-money-laundering-directive/en>
117. Sullivan C. (2012) "Digital identity and mistake", *International Journal of Law and Information Technology*, vol.20, pp. 223-241. Doi: 10.1093/ijlit/eas015
118. Sullivan C. (2016) "Digital citizenship and the right to digital identity under international law", *Computer Law and Security Review*, vol.32, pp. 474-481. Doi: 10.1016/j.clsr.2016.02.001
119. Li Y., Y, W., L, X. and Yang Z. (2020) "Research on the evolution of global internet network interconnection relationships in 21 years", *China Communications*, 17(8), pp.158-167.
120. Atick J. (2016) "Digital identity: the essential guide", ID4Africa Identity Forum. 2016:1–3. Available at:
http://www.id4africa.com/prev/img/Digital_Identity_The_Essential_Guide.pdf
121. Rannenberg K., Camenisch J. and Sabouri A. (2015) "Attribute-based credentials for trust: Identity in the information society", *Attribute-Based Credentials for Trust: Identity in the Information Society*, pp. 1-391. Doi: 10.1007/978-3-319-14439-9
122. McKinsey Global Institute (2016) "Digital finance for all: Powering inclusive growth in emerging economies".

Acknowledgements

English Version

This Thesis marks the end of my university career. A path that I would have loved to live entirely as a student, but which instead has also seen me working full-time. In fact, concurrently with this Master's Degree, at the Politecnico di Milano (between March 2020 and December 2020), I worked in no less than three different companies: Ingenico, InfoCert and PricewaterhouseCoopers (PwC), the company where I am still employed today.

The Politecnico di Milano is a completely different reality compared to that of the University of Catania, where I obtained my Bachelor's Degree in Electronic Engineering.

I think I would have been much better off at the Politecnico di Milano than at the faculty in Catania if I had been able to attend classes and lead a normal university life.

On the other hand, starting work in 2019, about two months after graduating in Catania, allowed me to grow quickly in the world of work, which is highly valued in Milan.

Working and studying at the same time was not easy, in fact it has been a great burden these past two years. Nevertheless, it was a very formative experience, which I would repeat, during which I learnt many fundamental concepts, which I often found again in the working environment. But above all, the Master's Degree in Management Engineering at the Politecnico di Milano allowed me to meet many great girls and boys, who were an important reference point for me, and who played a primary role in leading me towards the completion of my studies. The best thing was to create friendships with these people. Relationships that I have the feeling will be long-lasting in the years to come.

In particular, I feel immensely grateful to three people: Alessia, Alessandro and Federico. Superlative young people who will graduate with top marks and who I am sure will also be able to impose themselves in the working environment. Not only for their professional qualities, but above all for their human qualities, which are the ones most appreciated and the ones everyone will remember.

Furthermore, I cannot help but thank my co-trainees, Clarissa, Diletta and Giorgia, who over the past eight months have been an example of helpfulness, kindness, and patience. I have probably been one of their most difficult cases to deal with, due to my busy work schedule. However, I hope that they have appreciated the commitment and dedication they have shown in carrying out this Thesis to the very end. I hope I have left them something positive, as they have left me.

I would also like to thank Prof. Luca Gastaldi, my Supervisor, who had also been my Professor for the subject Leadership & Innovation, which I appreciated very much. I always saw Prof. Gastaldi as a person not far from the student dimension. This was one of the factors that made me choose him as the Rapporteur for my Thesis.

Last but not least, as the good ones say, I thank from the bottom of my heart my family, my Mum (Sara), my Dad (Johnny) and my brother (Alessio) for always being there for me, even in times that were not at all pleasant. They have always instilled in me the strength and the will to go on to fight, achieve and realise my dreams.

Mum, Dad, Ale, my dreams are slowly coming true.

Today, 20 December 2022, the Master's Degree in Management Engineering (aka Laurea Magistrale in Ingegneria Gestionale), at the renowned Politecnico di Milano.

This will only be the beginning of an interminable series of satisfactions that I will continue to give you.

With affection,
Simone

Versione italiana

Questa Tesi sancisce la fine del mio percorso universitario. Un percorso che avrei tanto voluto vivere interamente da studente, ma che invece mi ha visto anche lavoratore a tempo a pieno. Infatti, in concomitanza con questo percorso di Laurea Magistrale, presso il Politecnico di Milano (tra Marzo 2020 e Dicembre 2020), ho lavorato in ben tre aziende diverse: Ingenico, InfoCert e PricewaterhouseCoopers (PwC), azienda dove sono tuttora impiegato.

Il Politecnico di Milano è una realtà completamente diversa rispetto a quella dell'Università di Catania, presso la quale avevo conseguito la Laurea Triennale in Ingegneria Elettronica.

Credo che al Politecnico di Milano mi sarei trovato molto meglio rispetto alla facoltà catanese se avessi potuto frequentare le lezioni e condurre una normale vita universitaria.

D'altra parte, cominciare a lavorare nel 2019, circa due mesi dopo essermi laureato a Catania, mi ha permesso di crescere velocemente nel mondo del lavoro, che a Milano è assai valorizzato.

Lavorare e studiare contemporaneamente non è stato facile, anzi è stato un grande fardello in questi ultimi due anni. Ciononostante, è stata un'esperienza molto formativa, che ripeterei, durante la quale ho appreso molti concetti fondamentali, che spesso e volentieri ritrovavo anche in ambito lavorativo. Ma soprattutto, la Laurea Magistrale in Management Engineering presso il Politecnico di Milano, mi ha permesso di conoscere tante ragazze e ragazzi in gamba, che hanno rappresentato per me un punto di riferimento importante, il quale ha giocato un ruolo primario nel condurmi verso il completamento del percorso di studi. La cosa più bella è stata creare dei rapporti di amicizia con queste persone. Rapporti che ho la sensazione saranno duraturi negli anni a venire.

In particolare, mi sento immensamente riconoscente verso tre persone: Alessia, Alessandro e Federico. Ragazzi superlativi che si laureeranno con il massimo dei voti e che sono sicuro che saranno capaci di imporsi anche nell'ambito lavorativo. Non solo per le loro qualità professionali, ma soprattutto per quelle umane, che sono quelle più apprezzate e quelle di cui tutti si ricorderanno.

Inoltre, non posso fare a meno di ringraziare le mie Correlatrici, Clarissa, Diletta e Giorgia, che negli ultimi otto mesi sono state un esempio di disponibilità, gentilezza e pazienza. Probabilmente sarò stato uno dei loro casi più difficili da gestire, a causa del mio impegno lavorativo. Tuttavia, spero che di me abbiano apprezzato l'impegno e la dedizione adoperati nel realizzare questa Tesi fino all'ultimo. Spero di aver lasciato loro qualcosa di positivo, così come loro hanno fatto con me.

Un ringraziamento anche al Prof. Luca Gastaldi, mio Relatore, che era anche stato il mio Professore per la materia Leadership & Innovation, che avevo apprezzato moltissimo. Ho sempre visto il Prof. Gastaldi come una persona non distante dalla dimensione dello studente. Questo è stato uno tra i fattori che mi ha fatto propendere a sceglierlo come Relatore per la mia Tesi.

Last but not least, come dicono quelli bravi, ringrazio dal profondo del mio cuore la mia famiglia, mia Mamma (Sara), mio Papà (Johnny) e mio fratello (Alessio) per essermi sempre stati vicino, anche nei momenti per niente piacevoli. Mi hanno sempre infuso la forza e la voglia di andare avanti per lottare, raggiungere e concretizzare i miei sogni.

Mamma, Papà, Ale, i miei sogni si stanno pian piano realizzando.

Oggi 20 Dicembre 2022 è toccato al Master Degree in Management Engineering (alias Laurea Magistrale in Ingegneria Gestionale), presso il rinomato Politecnico di Milano.
Questo è solo l'assaggio di una serie interminabile di soddisfazioni che continuerò a darvi.

Con affetto,
Simone