impulse.
Digital Government Institute

Digital Identity

A new paradigm of relationship with citizens

Contents

Global context of the document

Digital transformation is driving a **new paradigm at all levels of society**. A constant change, in a highly dynamic environment, where the challenges are varied and innumerable.

The Public Administration is not far from this context, which offers a new **framework of relationship with citizens**, where face-to-face communication gives way to the digital world and all the challenges that this entails.

One of these challenges has to do with Digital Identity, a concept at the core of most of the challenges that arise in citizen-Public Administration interactions, under the premises of security, effectiveness and trust between the parts.

In order to address this issue, public-private partnership is proposed as one of the essential pillars to offer citizens a safe, scalable and quality solution. As a key partner in this environment, NTT DATA, analyzes in this Whitepaper on **digital identity** the main keys and current events, with the following objectives:

- **Get to know the origin, scope and purpose of the digital identity for citizens.**
- **Understand the current situation regarding digital identity in Europe (state of the art).**
- **Debate and define a fundamental roadmap for the implementation of digital identity by the AA.PP.**

1. What is digital identity?

The digital identity emanates from the needs that arise from the rapid process of digital transformation of society as a key element to meet the new needs of citizens.

> **When we talk about digital identity, we refer to the set of electronic attributes that represent a person, an organization or a thing in the digital world.**

Digital transformation is currently the driver for change at all levels of our lives. The concept of identity, as a key element of the social conception, requires to be part of it in order to overcome the current existing limitations, such as:

- People without a registered identity **(15% of the population), which sets a barrier to access to basic services.**
- Misappropriation of personal data, **a consequence of delegating such data to a third party.**
- Security issues **when data is deposited in different repositories and between different users.**
- Privacy **and data protection** issues **as the individual is not the manager of his/her data.**
- Information contained in different **information** repositories.
- **Disposal of** high costs.
- **Lack of** portability **in mechanisms, even if they are secure.**
- **Lack of** compulsion **in its use.**

It is possible to overcome many of these barriers thanks to the implementation of digital identity for citizens. It also helps us to move from the current model defined by "who you are" to a model based on the idea of **"what we can do"**.

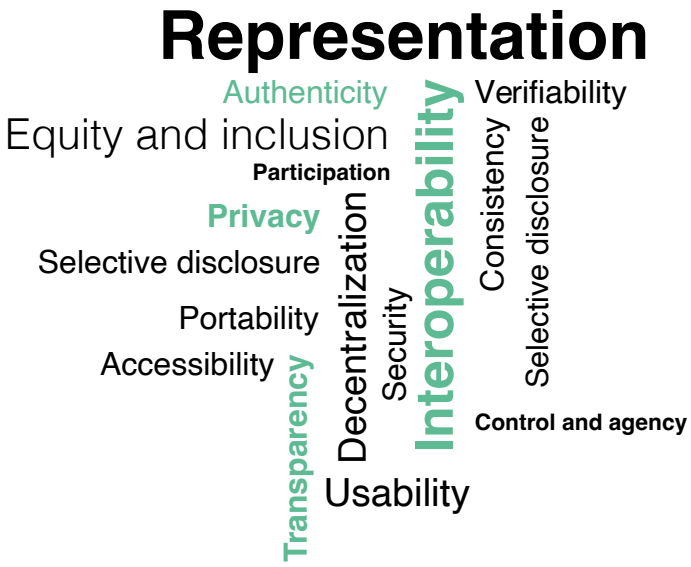
For example, in the current model it is necessary to share **each of the electronic attributes of the digital credential**, just as it happens in the physical world when we share the ID card where we are showing all the data, whether they are necessary or not. With **selective attribute disclosure**, the citizen is allowed to share only those attributes that are necessary and only if he/she wishes to do so.

According to this conceptualization, digital identity will not only be defined by personal data (name, age, etc.), but by **all those attributes that define and affect the capabilities of individuals**: university degrees, economic capacity, criminal records, etc.

This extension of the concept of identity also argues in favor of **self-sovereignty**, i.e., each person will be in control of his or her data, in other words, the user has autonomy and control. This way, each citizen limits and regulates the access of third parties to their information, obtaining benefits such as:

- Reduction of the risk **of massive theft.**
- Increase in privacy, **because the citizen is able to verify without having to access the source thanks to the settlement of trust frameworks and decentralized registries.**
- **The user can** choose the data to be shared **through selective disclosure of attributes and zero-knowledge proofs.**

Additionally, there are a number of principles that the digital identity must comply with, such as:



Digital identity, therefore, is a **concept that belongs in a greater whole**. It is not an individual concept, and it must be preceded and accompanied by a network of elements that make it possible to achieve an efficient, secure and reliable cross-border service.

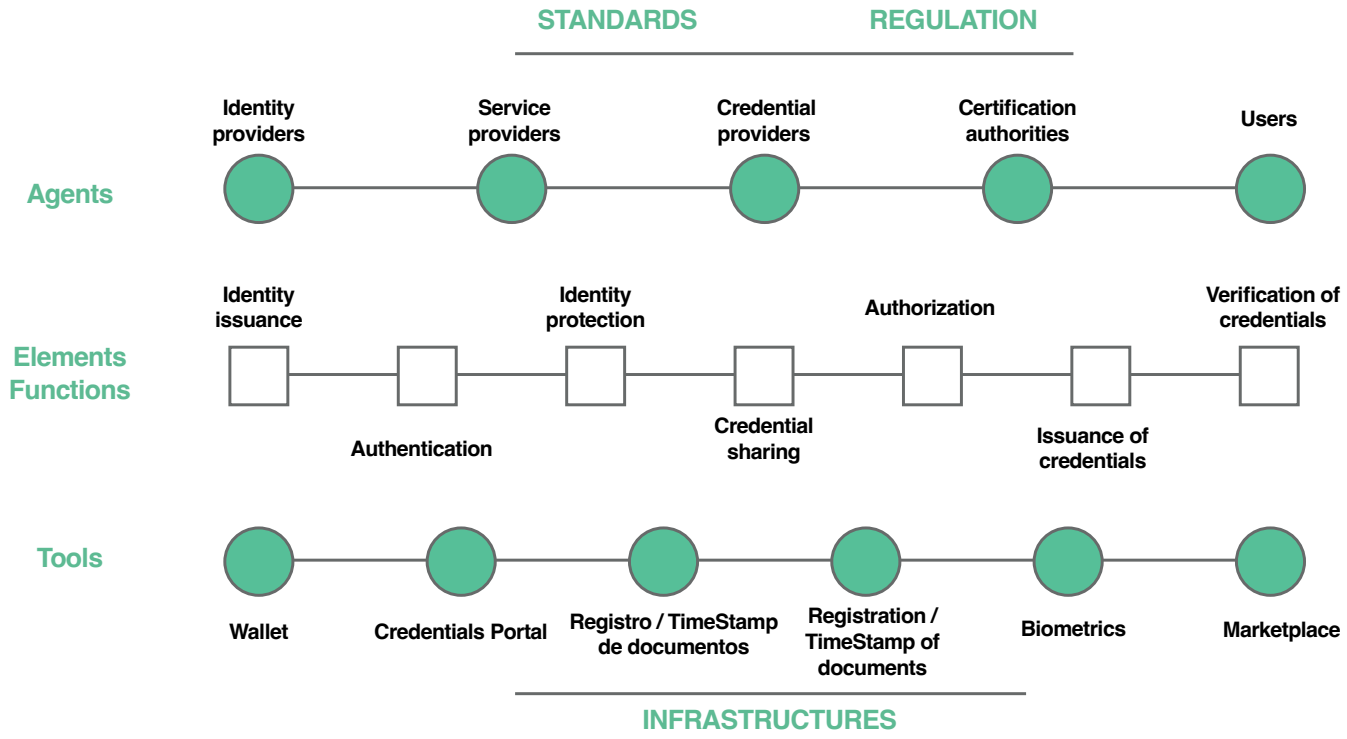
Therefore, to understand the implications of digital identity, its definition must be extended to the **ecosystem in which it is immersed** and to the different issues and agents that influence and affect its configuration.

1.1 Trust Framework: ecosystem of digital identity

The trust framework of digital identity is made up of all the **elements that, together, make digital identity possible, and is based on practices that guarantee privacy, security and proper functioning.**

The starting point for the understanding of all the elements that make up this ecosystem, is the trust framework, understood as those structures that are used to establish rules, procedures and technical requirements to ensure interoperability, privacy and security in the services offered by the digital identity. The following picture represents the ecosystem:

In the image, you can evaluate at a glance the different parts that make up the **Trust Framework of the digital identity ecosystem:**



There is a series of standards and specific regulations (eIDAS) that **harmonize and generate a safe and reliable environment** for the different parties. In addition, they make it possible to give legal validity to the model and comply with regulations related to GDPR, privacy, the right to be forgotten, consent, etc. In the regulatory field, issues of particular relevance to the functioning of digital identity, such as **signatures, transactions, certificates or electronic seals, among others, must be considered.**

Following these standards and regulations, the **different agents involved relate to each other** to make the concept of digital identity a reality. Authorized providers will offer Digital Wallet solutions and trusted issuers will issue citizens with electronic attestations of attributes (credentials).

As **functional elements**, we note the different processes and tasks involved in the use of digital identity: the issuance of credentials to users, the verification of credentials when shared with a third party, etc.

To support all the functionalities, the agents use **specific tools** to offer digital identity services to the user: **the wallet as the backbone**, biometrics as an authentication method, etc.

Therefore, technology is presented as the basis for facilitating the solutions aroused around digital identity, so that it can be developed in secure and reliable environments through the use of elements such as decentralized identifiers, credentials, decentralized registries or wallets, etc.

Finally, as the essentials of the framework, we find the **basic technological infrastructure** that makes possible the relationship between the agents, the decentralized data storage, etc.

1.2 Model of governance (interoperability)

Within the framework of this ecosystem is the set of specifications, rules and agreements that, with the objective of achieving a common purpose, gather mandatory requirements and allow transactions to be carried out among a community of participants.

As part of this governance model, interoperability, understood from its four perspectives, is framed as follows:

1 LEGAL

The European Interoperability Framework (EIF) or the Single Digital Gateway (SDG), among others.

2 SEMÁNTIC

This refers to the **analysis of the existing** initiatives aimed at harnessing models such as Core Vocabularies or highly reusable Ontologies, or even to existing standardized and interoperable models such as the EBSI educational credentials based on Europass.

3 ORGANIZATIONAL

It is responsible for defining the organizational **model or governance** model, with an emphasis on processes, data or decision-making bodies, among other aspects.

4 TÉCHNIQUE

It reuses **universal business languages** whenever possible (syntax of vocabularies) and creates interfaces necessary for the connection and exchange of information.

1.3 Case of use

Once we have understood what digital identity is and the agents that make up its ecosystem, we will present a specific use case. In this way, we illustrate in practice the tools, processes and agents we have learned about.

Case description:

It shows how to obtain a Proof of employment demand and its subsequent use to apply for a benefit.

The user accesses his Digital Wallet where he already has different credentials such as the Identification Card issued by FNMT or the Title of large family and from where he can apply for others.

They can also share their information securely with third parties to access digital services in remote scenarios or in person.

Digital wallet

#Portability, #Security, #Interoperability, #Utility, #Scalability

1- Initial screen of the Digital Wallet.

Credential application:

First, the user needs a Digital Wallet issued by an authorized issuer. When accessing the Digital Wallet, he/she has the option to request credentials from among those available.

The user requests a Proof of employment demand. The issuing entity (SEPE) must identify the user and requests the presentation of the identity credential issued by FNMT. After identifying the user and verifying the applicability of the request, the SEPE service issues the requested information.

2- Select Proof of employment demand.

3- Allows the SEPE service to verify your identity in order to issue the requested voucher.

4- Obtains the proof of employment demand requested.

Credential sharing:

Once the receipt has been obtained, the user can use it to carry out another procedure. In this case, it is used to apply for a benefit from the National Social Security Institute (INSS).

The user accesses a service that displays the option of initiating a benefit application process.

This is generally done by scanning a QR with the Digital Wallet. This QR leads the request to a service that asks the user for a large family certificate and proof of employment demand. The user agrees to share the information and the application is completed.

1- Scan the QR code that shows you the electronic headquarters.

2- Share the requested information with the INSS.

3- The INSS informs about the correct filing of the application form.

2. Digital identity: State of the art

After having analyzed the concept of digital identity, its implications and some cases of use, it is necessary to understand **the current state of the art in Europe.**

The EU, especially during the last few years and in an incremental manner, has laid the foundations for the implementation of digital identity as a fundamental right of citizenship. For this purpose, it has made use of:

- **A strategic framework with the European Digital Wallet at its core, based on key principles such as privacy and Portability.**
- **A sound regulatory framework based on the eIDAS2 regulation, which aims at harmonizing trust services across the continent.**
- **A technological framework that, in line with the above, makes it possible to offer quality and safety services.**

2.1 Strategic framework European digital wallet

At the heart of the digital transformation process throughout the continent and in the framework of the Digital Decade policy programme 2030, the **European Digital Wallet** is the backbone with which to face many of the challenges that will arise in the coming years.

In the current environment, a program is emerging to align the entire European public sector with the aim to converge towards a deep transformation of the digital world. Such transformation argues in favor of the recognition of a digital identity across Europe.

On the way to this momentum, the main objective is to ensure that all individuals and legal entities have secure, reliable and trusted access, while at the **same time being in control of their data**.

This means that digital identity will be universally available to all Europeans, and while its use will be voluntary for citizens, **for member states it will be obligatory** in order to guarantee the right of access and the protection of citizens' data.

Understanding this as the objective to be achieved at the European level with regards to digital identity, the European Digital Wallet emerges as:

(1) means of electronic identification *(2)* that allows the user to store and retrieve identity data *(3)* such as an individual's identification data and electronic attestations of attributes linked to the individual's identity.

(1) **From a social point of view, it is expected to be perceived as an equivalent to the identity card by virtue of its expected level of acceptance and its own legal regime: the data is held by the citizen, it is not in any repository.**

(2) **It returns control of the data to the citizen.**

(3) **They are intended to share information both remotely and in-person.**

Below we will define the strategic process by which we want to address the creation of the Digital Wallet, which includes four main lines of work:

- **The process begins with the creation of the legislative framework, which is based on the eIDAS2 regulatory framework.**
- **It would continue with the specification of the technical definition standards and the defined framework (called ARF), as drivers of its operation.**
- **Based on these technical standards and the reference framework, an iterative version of the Digital Wallet, a reference application, would be created.**
- **Finally, this application would enable the deployment of Large-Scale Pilots (LSPs) whose objective is to test the specifications and the reference implementation with real cases of use that will ultimately be the first ones to be made available to the citizen.**
- **Traceability must be null in order to guarantee the users' privacy, setting restrictions on the existence of data escrow services.**
- **The European Digital Wallet can be used to access all public and private digital services, as a supplement of the current means.**
- **It will be free and open source, without limiting the possibility of issuing attribute certificates; both the private and public sector will be able to monetize it.**
- **From its implementation, both the public and private sectors will be obliged to accept the European Digital Wallet.**

The Digital Wallet shall enable the following:

- **Information gathering and sharing in a user-friendly manner.**
- **Issuance and revocation of certificates.**
- **Qualified signature free of charge.**
- **Portability to another digital wallet and data downloading.**

2.2 Regulatory framework

In 2016, the EU Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market **(eIDAS)** came into force. However, the evolution of the environment and the constant commitment to digitalization in various aspects of daily life, **entail a need for an update of this regulation**, leading to cover the new demands that the digital transformation generates.

For this reason, work is currently underway on **eIDAS2**, a regulation that aims to face these new demands related to digital identity, with various objectives such as:

- **Harmonization and interoperability of trust services throughout the European Union.**
- **Make the provision of digital identity an obligation for the governments of member states.**
- **Expand the scope of regulation and digital identity to involve the private sector in partnership with the public sector.**
- **Regulate identity in the broadest sense of the term (not only who I am, but also what I can do).**
- **Improve the digital security of e-services and trusted service providers.**

In order to meet these objectives, eIDAS2 is positioned as the **central regulatory lever** for the development of the digital single market, from which to articulate the rest of the elements of the identity ecosystem. The major drivers of change arising from the regulation are:

- **Provision and use of the European digital wallet already addressed in this Whitepaper.**
- **Regulation of the DLT (Distributed Ledger Technology) as a reliable service.**
- **Creation of an interoperability framework to ensure that electronic identification systems and trust services are harmonized in the EU.**
- **Ongoing cooperation among EU members to share knowledge and assess best practices related to digital identity.**

2.2.1 Impact in AAPP

eIDAS2, within the framework of the regulation it is based on, has a profound impact on the way in which citizens relate to the Public Administrations, as well as on the **implementation of new technologies, processes and systems of trust** in the said administrations. As part of their implementation, Public Administrations must take into consideration the aspects described in this section as compulsory to comply with eIDAS2 regulations.

The use of the European Digital Wallet of digital identity is **mandatory** for all member states, with each of the administrations assuming this responsibility, as well as providing access to their sources and files to trusted service providers that issue electronic attestations of attributes.

Member States will be obliged to issue a digital wallet to citizens free of charge. On the other hand, Public Administrations will be obliged to accept the wallet as a means of electronic identification.

The impact on these will also be linked to the simplification of electronic signatures and seals, making everything available in the cloud and providing effective and reliable electronic communications.

Additionally, there will be a document archive that will incorporate electronically transmitted documents thanks to the blockchain.

2.3 Technological framework

Some of the most important aspects of the EUDI Wallet ecosystem that will support an interoperable digital identity model across Europe are the technology model and reference architecture.

Although the regulation lays the foundation for the issuance and recognition of electronic attestations of attributes, including the PID (digital identifier), a technological model is needed to support it and ensure proper implementation and interoperability. Although this is a work in progress, some major technological aspects are already known.

The main technological and safety elements are:

- **Architecture and Reference Framework (ARF):**

  The objective of this document is to provide all the specifications necessary to develop an interoperable European Digital Identity Portfolio (EUDI) solution based on common standards and practices.

  The ARF defines relevant aspects such as the trust model, protocols for issuing and exchanging information (OpenID and ISO 18013-5), data models, signature formats, types of flows and specifications for cases of use. The definition of the ARF is an **iterative process that is fed by the reference implementation and the work of the pilots.**

  Other aspects addressed in the RFA have to do with the implementation of mechanisms within the European Digital Wallet itself aimed at preserving privacy and ensuring security. Some of these are selective disclosure of information (Selective Disclosure) or the identification of issuers and third parties authorized to issue, request and consult information.

  The ARF will also serve as a guide for creating a reference implementation mechanism of the European Digital Wallet that can be reused.

- **Security certification scheme:**

  ENISA is currently leading the definition of a security certification scheme for the European Digital Wallet. This process will be aligned with national security schemes and with the EUCC certification scheme (based on Common Criteria). The objective **is to ensure**, through a common and certified process, the **security and privacy of the European Digital Wallet** regardless of which member state is responsible for issuing it.

- **Possibility of using DLT as a Trust Registry:**

  The potential regulation of DLT (distributed log technologies) as a trusted service in eIDAS2, like the development of the EBSI project, make it possible from both a regulatory and technical point of view to implement a Trust Framework based on this technology.

  This would enable the use of decentralized registries for verification during interactions and information exchanges through the European Digital Wallet would be possible. Currently EBSI already implements a chain of trust based on this model.

2.4 Time framework

After defining the strategic framework that encompasses the European Digital Wallet, as well as the key regulatory and technological aspects to be considered when creating the digital identity, below we present a timeline of each of the milestones that are marking the steps to follow until the constitution of a sovereign digital identity.

The **main technological and security points** are:

June 2021
Revision of the eIDAS regulation

February 2022
First Version of the ARF

Febrero 2023
Approval of ARF V1

December 2023
Approval of the eIDAS regulation

May 2024
Finalization of LSPs

2026
Deployment and Certification of the European Digital Wallet

3. Roadmap for implementing the digital identity:

At the European level, there is a need to adapt to a dynamic environment of digital transformation, which calls for the creation of a sovereign digital identity. As this Whitepaper shows, in this context, actions are being carried out to lay down the standards and regulatory norms on which it will be based and which must govern its implementation in the different member states.

In its implementation, each administration will regulate the aspects that must autonomously respond to the obligations, principles and premises arising from the eIDAS2 regulation, as well as to the technological requirements that will cover them.

They will have to comply with defined regulations and standards and will be a national challenge for governments and communities.

Below are some previous steps and areas of improvement that can be taken into consideration by the different Public Administrations, in order to enhance their services and prepare for this new model:

1. **Reducing bureaucratization and complexity of procedures by fostering administrative simplification.**
2. **Promoting the homogenization of platforms and the generation of simple interfaces.**
3. **Creating usable, secure and reliable technological solutions.**
4. **Eliminating entry barriers, as well as the different routes for performing procedures and redundant identification systems, so that this generates a single point of entry.**
5. **Focusing on the citizen experience to develop more effective and efficient services.**
6. **Knowing the technologies and their possibilities through continuous training, collaboration and communication.**
7. **Assessing the potential value-added services that the future wallet issued by the Public Administration may offer.**

ANNEX

Below are some key concepts for understanding the digital identity based on its characteristics:

Reliable services

A type of procedure that allows the user to trust the authenticity and veracity of a given transaction or information.

Credential

Set of one or more statements about an individual made by an issuer.

Verifiable credential

Credential with evidence of tampering whose authorship can be cryptographically verified.

Verifiable identity credential

A special form of verifiable credential that a natural or legal person can present as proof of who he or she is.

Holder

The actor in possession of the credential.

Verifier / Relying Party

The actor who requests the holder to present the credential, which can be verified in a centralized or decentralized way.

Issuer

The actor that issues the credential to the holder.

DID

Decentralized identifier based on W3C.

PID

Person Identification Data. The data that identifies the person and usually consists of the minimum eIDAS dataset.

(Q) EAA

Electronic attestation of attributes, qualified or not. For example, a verifiable credential.

Digital wallet

A storage where the holder stores its PID and credentials.

impulse.
Digital Government Institute

NTT DATA

www.impulsedigitalinstitute.es