Revista catalana de dret públic #65

www.rcdp.cat

REFLECTIONS ON THE EUROPEAN DIGITAL IDENTITY PROJECT IN LIGHT OF THE DIGITAL COVID CERTIFICATE AND THE SELF-SOVEREIGN IDENTITY MOVEMENT*

Raül Ramos Fernández**

Abstract

What is anticipated from the European Digital Identity project is being able to prove possession of a COVID-19 vaccination certificate without submitting any personal data. The introduction of this project through the draft amendment of the Regulation on electronic identification and trust services (eIDAS) has established for the first time the creation of a Digital Identity Wallet that could be used as a means of identification and a container of identity credentials, without depending on centralised files or tracking who they are presented to, with the premise of security and privacy of personal data by design as a fundamental objective. This vision, which is strongly influenced by the self-sovereign identity movement, together with the creation of the European Blockchain Services Infrastructure (EBSI) on which the European Self-Sovereign Identity Framework (ESSIF) depends, is reflected in the amendment of the eIDAS Regulation, and, indirectly, in the EU Digital COVID Certificate. As a result of the pandemic, the need to create a reliable, secure, interoperable system with full respect for the General Data Protection Regulation (GDPR) to certify health in relation to the disease led to the adaption of the European Digital Identity project to the COVID certificate. The opportunity presented by the study of the technical functioning of the certificate means that the assessment of improvements to be introduced can be transferred to the European Digital Identity project, including the blockchain resource as an alternative to the traditional public key infrastructure (PKI). In this respect, the certificate represents a firm step towards a decentralised digital identity model to ensure that individuals have full control over their data.

Keywords: COVID-19; eIDAS Regulation; self-sovereign identity; blockchain; interoperability; key public infrastructure.

REFLEXIONS SOBRE EL PROJECTE D'IDENTITAT DIGITAL EUROPEA A LA LLUM DEL CERTIFICAT COVID DIGITAL I EL MOVIMENT SOBRE LA SELF-SOVEREIGN IDENTITY

Resum

Acreditar la possessió d'un certificat de vacunació contra la COVID-19 sense lliurar cap dada de caràcter personal és el que s'anticipa del projecte Identitat Digital Europea. La introducció d'aquest projecte mitjançant l'esborrany de modificació del Reglament d'identificació electrònica i serveis de confiança (eIDAS) planteja per primera vegada la creació d'una cartera d'identitat digital que es pugui emprar com a mitjà d'identificació i com a contenidor de credencials d'identitat, sense la dependència d'arxius centralitzats ni traça davant qui es presenten, amb la premissa de la seguretat i la privacitat de les dades personals per disseny com a objectiu fonamental. Aquesta visió, fortament marcada pel moviment sobre la self-sovereign identity*, –junt amb la creació de la Infraestructura Europea de Serveis de Cadena de Blocs (European Blockchain Services Infrastructure, EBSI), de la qual depèn el Marc Europeu d'Identitat Sobirana (European Self-Sovereign Identity Framework, ESSIF)– es veu reflectida en la modificació del Reglament eIDAS, i, de retruc, en el certificat COVID digital de la UE. La necessitat, arran la pandèmia, de crear un sistema fiable, segur, interoperable i amb ple respecte pel Reglament general de protecció de dades (RGPD) per acreditar la salut en relació amb la malaltia ha portat a adaptar part del projecte d'identitat digital europea al certificat COVID; l'oportunitat que s'introdueix amb l'estudi del funcionament tècnic del certificat permet que l'avaluació de les millores a introduir siguin traslladables al projecte d'identitat digital europea, com el recurs a xarxes de cadenes de blocs (*blockchain*) a manera d'alternativa a la tradicional infraestructura de clau pública (PKI). En aquest sentit, el certificat suposa un pas ferm cap a un model d'identitat digital descentralitzat per garantir que l'individu tingui ple control sobre les seves dades.*

Paraules clau: COVID-19; Reglament eIDAS; identitat autosobirana; cadena de blocs; interoperabilitat; infraestructura de clau pública.

* This article is a translation of an original one in Catalan.

** Raül Ramos Fernández, lawyer of the Il·lustre Col·legi de l'Advocacia de Sabadell (Bar Association of Sabadell), doctoral student of Law at the Universitat Autònoma de Barcelona (UAB), specialisation in Law and New Technologies. Department of Public Law and Legal History Studies, Faculty of Law, Building B2, c. de la Vall Moronta, 08193 Bellaterra (Cerdanyola del Vallès). raulramos@icasbd.org.

Article received 15.01.2022. Blind review: 12.02.2022 and 23.02.2022. Final version accepted: 21.03.2022.

Recommended citation: Ramos Fernández, Raül. (2022). Reflections on the European Digital Identity project in the light of the Digital COVID Certificate and the self-sovereign identity movement. *Revista Catalana de Dret Públic*, *65*, 179-193. https://doi.org/10.2436/rcdp.i65.2022.3777

Contents

1 Introduction

From 1 July 2021, the health authorities in various European Union member countries and other adhering countries began to issue what was called the Digital COVID Certificate. The aim was to demonstrate health in relation to the pandemic reliably and in a way that could be checked without centralisation, according to a document verifiable through a quick response (QR) code held by its holder. The certificate serves as a bridge between analogue and digital, to confirm either vaccination, a negative result for a SARS-CoV-2 virus test at a certain time, or recovery from the COVID-19 illness.

This certificate, which is a simple concept with a complex design, represents a milestone in interoperability in the three dimensions of organisation, technology and content in the European Union area. To implement it, in June 2021, Regulation (EU) 2021/953[1] was adopted to ensure acceptance of the certificate in the EU territory and to define its functioning. At the same time, its technological implementation is determined by Implementing Decision (EU) 2021/1073[2] and the technical specifications published by the eHealth Network,[3] which describe mechanisms for mutual recognition and interoperability of vaccination, recovery and diagnostic test certificates.

The certificate is issued by the relevant health authority but it is the individual who displays it. There is no centralised data file, record of the number of times the certificate is used or record of who it is presented to. Instead, verification of the authenticity and integrity of the content of the credential depends on the electronic seal contained in the issuer's QR code, which is centrally recorded in the EU Digital COVID Certificate gateway.[4] Consequently, we have moved from a traditional model in which data are shared to a new system: proof of the existence of data by submitting to the holder a certificate that confirms certain attributes under the responsibility of the issuer. Centralised data storage and data transfer to a third party are no longer necessary, with the risks that their compilation and transmission represent. For example, in the Spanish health system, it is the seventeen autonomous communities through their respective health systems, and the General State Administration (Administración General del Estado) in the case of Ceuta and Melilla, that hold the data on the citizens who are issued the certificate in their respective area of competence. The issuance of the certificate is decentralised with standards and common formats and the credibility cross-checked between issuers and verifiers within the system.

Consequently, the novelty of the conceptual design underlying the certificate anticipates a model that is fully in line with the General Data Protection Regulation (GDPR)[5] and aims to become the standard vehicle for delivering and using certificates issued by an authority within the European Union: the issue of electronic attestations of attributes so that individuals are in possession of their own data and can choose who to transfer them to.

In the European Digital Single Market today, the elements that enable proof of the identity, facts, actions and situations of a certain individual are in the hands of the third parties that issue them through application of Regulation (EU) 910/2014 of the European Parliament and of the Council[6] on electronic identification and trust services (eIDAS Regulation).[7] In contrast, in a model of identity management such as that introduced by

1 Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic (OJ L, no. 15.06.2021, 211, pp. 1-22).

2 Commission Implementing Decision (EU) 2021/1073 of 28 June 2021 laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate established by Regulation (EU) 2021/953 of the European Parliament and of the Council (OJ L, no. 30.06.2021, 230, pp. 32-53).

3 For more information, see the website of the European Commission eHealth and COVID-19 (accessed on: 21.09.2021).

4 Annex IV of the Commission Implementing Decision (EU) 2021/1073 of 28 June 2021.

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L, no. 119, 04.05.2016, pp. 1-88).

6 Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L, no. 257, 28.08.2014, pp. 73-114).

7 An acronym of electronic identification, authentication and trust services.

the creation of the European Digital Identity, through the proposal to amend the eIDAS Regulation,[8] which in turn is based on the self-sovereign identity (SSI) movement, data are held by their subject in a virtual wallet. The COVID-19 vaccination certificate is therefore the ideal means to introduce the possibilities that new technologies, applied to identity management on the internet, can offer to the Digital Single Market. In short, the relationship between the EU Digital COVID Certificate, the European Digital Identity proposal and the SSI movement is clear. This is the question to address through the conceptualisation and analysis of the legal framework created ad hoc to respond to the need to guarantee free movement in the European Union given the health crisis.

To achieve the above objective, the current legal framework for identification management in the European Union should be compared with the proposal to create the European Digital Identity Wallet. Then, we will conceptualise the postulates of the SSI movement and related technologies, such as blockchain, for which the determination of an unprecedented legal regime has been included in the proposal to amend the eIDAS Regulation. We will pause momentarily to explain how this technological application has again sparked debate on identity on the internet. In the last section of our article, we will describe the technical functioning of the COVID certificate, with a focus on the public key infrastructure (PKI),[9] which is the main base of security in electronic environments. We will conclude the article with an explanation of how the COVID certificate has contributed to the European Digital Identity project and its interaction with the GDPR. We will not discuss other ethical and social aspects, such as the suitability of using the certificate for purposes other than cross-border movement, indicating the shortfalls of the certificate in terms of user confidence and in this case considering the certificate issued by the Catalan Health Service (CatSalut), since it represents the territorial scope of the author.

2 The transition to a new model of managing digital identity in the European Union

In just a year, the COVID-19 pandemic has radically changed the digitalisation of services. There has been an exponential increase in the demand for online identification and authentication and the exchange of digital information on identity, attributes or qualifications with a high level of protection and security. This demand has overwhelmed the legal instrument that, in the form of a regulation, enables the mechanisms of identification and electronic signature and seals[10] in digital environments, delimits their legal effects[11] and regulates the trust services provided within the EU, based on fundamental elements for the good of cohesion in the internal market as described in Articles 26 and 114 of the Treaty on the Functioning of the European Union (TFEU).[12]

In accordance with the above, one of the objectives of the eIDAS Regulation is to establish cross-border recognition of electronic identification issued by Member States to access public services and establish a single market of qualified trust services,[13] regardless of the Member State that approves them, in accordance

8 Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) no. 910/2014 as regards establishing a framework for a European Digital Identity. Brussels, 03.06.2021 COM(2021) 281 final.

9 Currently, this is the most widespread technique on the internet for associating a public key with a specific person by means of a digital certificate with the approval of a certifying authority in a centralised, hierarchical context of the trust model (Gisolfi, 2018). It is based on the play between two mathematically associated keys that are used to encrypt or decrypt the information transmitted through insecure communication channels. While the private key is never displayed or communicated, the PKI resolves the mode by which the public key is disseminated.

10 We differentiate between an *electronic signature*, which is created by a natural person to declare their agreement with content, and an *electronic seal*, which is created by a legal entity to guarantee the origin and integrity of data (Article 3, eIDAS).

11 While the electronic signature and seal have certain legal effects, which are described in Articles 25 and 35 of the eIDAS, respectively, the digital signature is more general and refers to mathematical operations based on encryption algorithms.

12 Treaty of the European Union and Treaty on the Functioning of the European Union. Consolidated versions. Protocols. Annexes. Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon (OJ, no. 82, 30.03.2010, pp. 1-388).

13 Currently, nine qualified trust services are subject to the eIDAS Regulation, which leads to recognition of their legal effects in any Member State: 1) issue of a qualified electronic signature certificate; 2) issue of a qualified electronic seal certificate; 3) validation of a qualified electronic signature; 4) validation of a qualified electronic seal; 5) conservation of a qualified electronic signature; 6) conservation of a qualified electronic seal; 7) generation of a qualified electronic time stamp; 8) issue of a qualified website authentication certificate, and 9) a qualified electronic delivery service.

with the principle of the internal market[14] and with the same legal status as equivalent traditional processes on paper. The aim is to streamline processes and reduce bureaucratic obstacles, inherited from a tradition strongly based on files and documentary records of the former administrations on which the current European States were constructed (About & Denis, 2011).

However, in a globalised, changing world, tools such as the eIDAS Regulation and the GDPR, which have positioned the European Union as a leader in the defence of privacy and trust in digital environments, could not remain unaffected by the technological innovations that have arisen in short periods of time. Aware of this situation, the European Commission is following the objectives established in the 2030 Digital Compass[15] so that, by the end of the decade, EU citizens could benefit from extensive deployment of trusted identity that enables each user to control their online interactions and presence. This has led to the recent presentation of a proposal to amend the eIDAS Regulation.[16] One of the aims of the proposal is to create a framework for European digital identity taking as a starting point, in the explanatory memorandum and context of the proposal, the new movement that has gained pace and is focused on making users managers of their own identity on the internet. In this movement, the perspective of management centred on rigid digital identities gives way to the provision of and trust in specific attributes related to these identities.

The confluence of various social movements, such as SSI or those that simply demand greater privacy in digital environments, is reflected in this new proposal. It is designed to serve as the legal basis for the development of new technologies such as distributed ledger technology (DLT), including blockchain, in accordance with the nomenclature of electronic ledgers in the proposal for amendment. The supporting function of these technologies provides the opportunity to guarantee in these open source, immutable electronic records[17] the authenticity and integrity of the data that they contain, and the accuracy of the date, time and chronological order so that the sequence of transactions can be followed. This guarantees that an event registered in the chain at a given time was carried out at this time. The system uses the effect of a time stamp in a similar way to the use of time stamps in electronic signatures.[18]

According to their supporters, these properties of blockchain networks are a tool for implementing an unprecedented layer of identity on the internet, and a desirable alternative to the services of preservation of electronic signatures and seals to guarantee their integrity over time.[19] These decentralised registers have the capacity to become a reliable source of information for providers authorised to issue credentials, like the current COVID certificate gateway. The improvement made by blockchain technologies over the current configuration of the gateway, which acts as a centralised register of public keys from the various health systems of each Member State enabling the verification of COVID certificate signatures, is the reinforced security known as blockchain immutability, achieved by redundancy through replication of information in various nodes.

However, what is important lies in the mode, in how the technology can be used in regulated environments to address problems faced with old solutions and their inherent limitations. These have been revealed progressively from the perspective of privacy and data security in digital identity management. In the last two

14 Article 4 of the eIDAS.

15 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 2030 Digital Compass: the European way for the Digital Decade. COM(2021) 118 final.

16 Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) no. 910/2014 as regards establishing a framework for a European Digital Identity. COM(2021) 281 final.

17 The construction of open source software means that: a) anyone can freely download the database that is generated or the full program to run it on their own equipment and make it a node of the system or download the more limited program that enables you to act as a basic user; b) anybody can discover and examine the source code and all the databases that the program generates, and c) anybody can modify the program (González-Meneses, 2019, p. 128).

18 Considering Article 34 of the proposal to amend Regulation COM(2021) 281 final.

19 The service of preservation of signatures and seals enables the reliability of the validation data for the qualified signature or seal to be extended beyond the initial period of technological validity (Alamillo Domingo, 2019b, p. 426). The aim is to guarantee the continuity of the validity of a document over time, given the inevitable production of documents that simulate that they have been signed at some point in the past in a fraudulent way. The successive processing of records in blockchain networks should make this task easier, although the immutability of the registered data means that greater care is required in their use. Therefore, this application of distributed ledger technologies can neither be resorted to nor is it desirable in all circumstances.

decades, the European Union has worked on various legal instruments in this area, starting with the approval of Directive 1999/93/EC,[20] repealed by the current eIDAS Regulation, which regulated electronic signatures based on the current framework of public key infrastructure imposed as a hierarchical system for the issue of certificates in accordance with technical standard UIT-T X.509, to confirm the identity of the signatory.

2.1 Limitations of the eIDAS Regulation

Since its approval in 2014, the eIDAS Regulation has established a federation of digital identities of EU citizens in order to make interoperability of the various States' identification systems possible for cross-border access to public services and thus to be able to use the identity solutions that each Member State has chosen without any additional requirement (Llaneza González, 2021, p. 142). In other words, the Regulation offers the opportunity to use electronic ID to identify yourself before an EU public administration in the same way as within national territory, without requiring an additional procedure. Although this system constitutes a major milestone in the consolidation of the Digital Single Market, since its launch it has been seen to be a timid approach to this objective.

The main obstacles that have prolonged the defragmentation of the Digital Single Market in this area can be summarised as three critical issues: the residual use of national identification systems due to their complexity, so that the user experience is sacrificed for security; the willingness of States to extend their identity solutions beyond their territory; and the exclusion of the private sector as an actor within this project of a European scope (Alamillo Domingo, 2019a, p. 15). This last factor leads to national identification systems being overlooked. Instead, online private providers' platforms are used for authentication. This generates dependence on these third parties, which require the creation of new accounts and often unwarranted data transfer, with everything that this involves, such as the monitoring and learning of users' behaviour as digital identities are recorded or associated with the access device. One example is the case of cookies (Alamillo Domingo, 2020, pp. 9-10).

This lack of use of digital identity systems issued by Member States, which are a public asset, with the contradiction that their ineffective use represents for the Digital Single Market, is what has driven the European Commission to offer a new common framework, a European Digital Identity, as stated in the explanatory memorandum of the proposal to amend the eIDAS Regulation. This will also allow access to an extensive catalogue of private online service providers with the issuance of a European Digital Identity Wallet.

2.2 Conceptualisation of the sovereign European identity project

As pointed out above, the proposal to amend the eIDAS Regulation is a user-centred legal instrument. It is designed to give users the tools required to take charge of their own identity attributes, delegated voluntarily or out of necessity to others. This is no longer something that is done to the user, but something done by the user.

For this reason, the Commission is committed to creating the European Digital Identity Wallet, defined in the proposal as a product and service that enables the user to store data, credentials and attributes associated with their identity,[21] and to create qualified electronic signatures.[22] A different aspect to that of the wallet as a container is its content: the issue of electronic statements of attributes, in this case by providers of trust services rather than by Member States (Article 3.16 eIDAS). These statements are defined provisionally as attestations in electronic format that allow the authentication of attributes.[23] In turn, these would be traits, characteristics or qualities of a natural person or legal entity in electronic format, as in the case of the Digital COVID Certificate.

20 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ L, no. 13, 19.01.2000, pp. 12-20).

21 Art. 6.*b* of the proposal to amend the eIDAS Regulation.

22 In accordance with Article 25.2 of the eIDAS, this is equivalent to a handwritten signature. In the transposition to Spanish legal regulations by means of the second final provision of Law 6/2020, of 11 November, regulating certain aspects of electronic trust services (Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza) (BOE, no. 298, 12.11.2020, pp. 98821-98841), which amends Article 326 of Law 1/2000, of 7 January, on civil procedure (Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil) (BOE, no. 7, 08.01.2000), the national legislator has gone further and established an evidentiary presumption when a qualified service is used. The paradox arises that there is greater guarantee of an electronic signature based on a qualified certificate than on a handwritten signature.

23 Art. 1.3.*i* of the proposal to amend the eIDAS Regulation.

The development proposed by the European Commission is to obtain an additional means of electronic identification from the national means that is used. The mandate is that each State, within its own sovereignty, issues the means of identification that it deems appropriate and at least one means with a high level of security in accordance with the technical standards specified in the current eIDAS Regulation. The novelty in the handing over of this Digital Identity Wallet to citizens is that they can identify and authenticate themselves before any other party. One example of this, transferred to the Digital COVID Certificate, is the capacity to increase security, usability and control to be able to demonstrate with certainty proof of vaccination, recovery from disease or diagnostic test results. From the wallet, verification of the credentials and identity of whoever shows the certificate will be carried out automatically.

In the current configuration, the Digital COVID Certificate must be accompanied by a national identity document. The certificate is validated when a visual check of the credential, that is, the certificate, and the identity document shows that both documents coincide. This generates concerns about privacy. The Catalan Data Protection Authority (APDCAT)[24] released a statement in favour of the proportionality of this practice in terms of access to the data required to verify the identity of the certificate holder. Such concerns would be resolved by the Digital Identity Wallet, as it is a means of identification that can display data selectively.

Another aspect of the wallet as a means of identification is its capacity to store the credentials of attributes associated with identity, such as the COVID certificate. The difference is that this is no longer an expression of national sovereignty, but of the issue of certificates through trust service providers. Therefore, it is subject to regulation by the European Parliament and the Council for the good of cohesion in the internal market through the expression of Articles 26 and 114 of the Treaty on the Functioning of the European Union. There is no desire to harmonise existing law, as the amendment of conditions in the form of Member States' civil and commercial law is outside the competences of the Commission. Instead, the interest in trust services comes into play, with the creation of new European legal institutions and new European legislation, with the same legal effects as its equivalents in the Member States.

This is what is introduced with the proposal to amend the eIDAS Regulation: to supersede existing national institutions, which are not interoperable and do not have a guaranteed legal regime, with some new institutions. This has occurred with the catalogue of trust services that comprise the personal data market. Therefore, we are talking about a decentralised identity model in which numerous operators issue identity credentials in a broad sense.

The proposal to amend the eIDAS Regulation involves creating a common, interoperable instrument for the public and private sectors for the first time in European Union territory; providing the opportunity to attain electronic attestations of attributes, combine them and share the data required for each service; eliminating paper and the difficulty in selectively sharing data on a certificate that is in physical format; and introducing privacy by design as data is handed over to users without monitoring their use by the certifying authority. Hence, the Digital COVID Certificate is a trial of the proposal.

3 The self-sovereign identity movement

The principles underlying the COVID-19 vaccination certificate, and by extension the principles present in the creation of the European Digital Identity, are those supported by the self-sovereign identity movement. This movement, driven by new technologies, cryptography standards, distributed networks, cloud computing and widespread access to mobile devices, proposes a new, alternative model to the current decentralised, federated models of digital identity management on the internet. In the new model, only users are in full control of their data.

This new model, summarised by Allen (2016), with the experience of having worked on the development of the SSL/TLS internet security protocols, provides a new perspective on one of the greatest challenges of the

24 Catalan Data Protection Authority. Statement relating to a consultation formulated by an association of collegiate members on whether the use of the COVID certificate in different sectors in Catalonia and the identity card requirement by establishments was in accordance with data protection regulations (Dictamen en relació amb la consulta formulada per una associació de col·legiats relativa a la conformitat a la normativa de protecció de dades de l'ús del certificat COVID a diferents àmbits a Catalunya i el requeriment del DNI per part dels establiments). Statement CNS, no. 18.01.22, 2021/57.

information society: safe management of digital identity. In addition, it addresses the underlying problem in the identity system on which modern societies are based: the necessary legal recognition of this identity by States to make the individual subject to rights and obligations. This problem can even lead to a person losing their identity, that is, the negation of a series of unalienable rights, by equating administrative identity with the existence of the individual through credentials and identifiers issued in the form of licences or passports that, ultimately, as prosthetic elements, become the person that they identify (Romero Bachiller, 2009).

3.1 Controversy over the term *sovereign*

Although its formal beginnings date back to around 2015, the SSI movement as a technology and an ideological proposal is still recent and not without controversy due to its connotations. According to Reed and Preukschat (2021, pp. 10-11), what has consolidated the term, to the extent that it is currently the standard name used to refer to this new model of identity, is clearly the ideology that it evokes. In this respect, *sovereign* in a broad view of the term refers to the individual's autonomy or independence, and *self* refers to excluding others from intervening in the individual's personal autonomy in relation to their existence.

However, although the term is attractive to a certain social sector, it also generates reservations and distrust in the evaluation of proposals introduced by the most radical vision of the SSI movement. It does not deny the power of the State, and even less so does it evade the responsibility of the individual as subject to rights and obligations. In contrast, it strengthens the relationship between government and citizens (Ruff, 2018). However, one of its goals is to reduce as much as possible State presence in the interactions of the individual related to privacy, identity and personal data management.

The notion of self-management and self-sovereignty that is introduced in the term *self-sovereign identity* is found in Marlinspike (2012), in what he called *sovereign source authority*. This is one of the most direct origins, not of the concept, but of the conception of the term that has been consolidated to refer to a decentralised digital identity model to respond to a problem that is extremely easy to formulate but notoriously difficult to resolve. This problem is that the internet, as described by Microsoft's leading identity architect, Kim Cameron (2005), was created without any native identity layer, without a way of knowing who or what a user is interacting with when they are on the internet, with the resulting security and criminality risks in an environment that is strongly dependent on all kinds of legal transactions and social relations.

Marlinspike considers that this sovereign capacity reflects the nature of all living beings to act for themselves and is a precondition for integration into society. That is, it is a precondition for defining interaction with other individuals and how you will be seen by them. He sums this up clearly by describing how this social construction that is identity comes into conflict when sovereign capacity is reduced to an administrative existence. In this case, the necessary census entry of the individual and its proof involves an administrative process for the existence of identity and, ultimately, of the person as subject to rights and obligations, as a member of a certain society. This model of identity, which is the one that has triumphed up to now to provide legal security in social relations, goes beyond mechanisms for managing identity and its products, in the form of rigid certificates and credentials, the existence of their holder and their capacity to operate within a certain context, so that the individual becomes an extension of these devices (Romero Bachiller, 2009).

There is ambivalence in the need to contain an entire political proposal in a legislative instrument that calls for the necessary intervention of public powers that are to be reduced or cut entirely. Precisely for this reason, authoritative voices such as those of Cameron (2018), who describes the vision of Ruff (2018), propose the need to use a new term such as *decentralised identity* to give it greater political neutrality and distance preconceived ideas from a concept of considerable complexity.

3.2 The contribution of blockchain to the identity debate

The underlying problem of internet identity is associated with the original internet architecture and its initial objective of permitting communication between the devices of various United States bodies as far back as 1969, if we refer in absolute terms to its origins. It began with the creation of the ARPANET network to interconnect devices and share resources through different equipment (Reed & Preukschat, 2021).

It was not until 1983, with the transition to TCP/IP protocol, that the internet opened up to commercial interests. As explained by University of Stanford professor Lawrence Lessig (1999), the need for identity and authentication was not for the devices, as this was resolved by the aforementioned protocol, but for the users. The TCP/IP internet protocol only gives the address of the machine from which a resource is requested, such as access to a website. This is because originally the people who used the internet were mainly academics. The main task was to design a decentralised network without any key node, "so that, in the event of a mass attack, especially a nuclear attack in this historical period, communication could never be entirely deactivated" ("Internet," 1998).

Years later, having come into contact with the work carried out by Cameron, Lessig (2006, pp. 50-51) investigated the issue in greater depth, which is where the SSI movement gets its ideology from and what European Digital Identity wants to embrace. In his study, Lessig explained that the identity system proposed at that time by Microsoft was designed to create a protocol to establish a virtual wallet of credentials with the same attributes as traditional credentials on paper, but with a level of security that had not been obtained before, with the aim of preventing fraud and facilitating recovery in the case of loss of physical medium. This Microsoft project would provide greater trust than the printed format. It would also enable greater control and precision of the data that are revealed to the party that has requested them without the centralisation of data in a single point where the trust must lie in another party. Instead, data are in the technology underlying the technical architecture, the cryptography.

The simplicity of this theoretical formulation, which was not technically possible when it was first devised, has been repeated over the years with each computer innovation. It has gained new impetus with the bitcoin phenomenon and its technological foundation, blockchain. This collection of technologies are promoted as a suitable tool for the formulation of a decentralised identity management system (González-Meneses, 2019, p. 173 et seq.) without the intervention of third parties that can withstand censorship and guarantees privacy. There is no possibility that a public authority can access, delete or monitor the data.

Distributed ledger technologies – of which blockchain is one of the applications – can provide opportunities for decentralised digital identity management, with the aim of replacing the current public key infrastructure. Hence, blockchain has been inseparably associated with the SSI movement. However, this association could not be further from the truth. The issue that blockchain resolves with virtual currency has similarities to the identity management problem explained here. However, it is not only resolved with the technology that has led to the reintroduction of a change in current network identity systems in the technical and legislative debate (Hughes, 2020). For this reason, in the proposal to amend the eIDAS Regulation, verifiable data registers are mentioned to include various technologies according to the principle of technological neutrality to promote the exploration of new proposals within a framework of legal security.

4 The European Union's Digital COVID Certificate

Although the COVID-19 digital certificate and, by extension, the proposal to amend the eIDAS Regulation reflect the self-sovereign identity movement, none of the aforementioned European instruments represent the legal recognition of its postulates or at least of its entirety. On its more radical ideological side, the movement opposes the dependency on each Member State to determine the identity of the individual. However, the European instruments do adapt the elements that are compatible with it to the EU's guiding principles and internal consistency, in line with the increasing demands for privacy and security in the management of the current network identity ecosystem, with the necessary existence under the governance of the GDPR of an identifiable responsible entity. The entity must abide by the duties and obligations of the data to be processed (Art. 3 GDPR) and the right of those concerned not to be subject to decisions based only on automated processing that has legal effects (Art. 22 GDPR).

From this perspective, the COVID certificate and the European Digital Identity project should be considered a triangular balance between the social demands for greater privacy in digital environments, the demands of the economic sectors to ensure legal security and regulatory compliance in their online transactions, and the necessary intervention of the State to ensure public and legal security within their sovereignty. As in all technical innovations, and in this case the COVID certificate is no exception, the background described in the

previous section should be interpreted as a discussion on the succession of technical proposals and solutions (even those that have not been applied), often in a short period of time, so as to understand the purpose sought by the European Commission with the COVID certificate and the European Digital Identity proposal.

In addition, these instruments should be interpreted indirectly according to the extent that they promote the adoption and development of new technical standards for effective collaboration between the public and private sector. One example of this can be found in the verifiable credentials standards and the decentralised identifiers of the self-sovereign identity ecosystem that are being developed by the World Wide Web Consortium (W3C) and worked on by the European Blockchain Service Infrastructure (EBSI), which is a European Commission initiative to explore the application of these technologies to various use cases, including digital identity, through the European Self-Sovereign Identity Framework (ESSIF).

One of the substantial improvements in the EBSI-ESSIF project in the European framework is the basis for introducing verifiable credentials and mutual authentication of entities, whether they are natural persons or legal entities, along with the opportunity to create secure communication channels for the exchange of messages with no need for an intermediary, as occurs with the current PKI model. In turn, an architecture based on the exchange of verifiable credentials using decentralised identifiers would lead to the possibility of cryptographically configuring the data so that they cannot be transferred to a third party or used for a purpose other than that for which they were requested. In these cases, data would become unreadable or marked as invalid (Reed & Preukschat, 2021, p. 183).

4.1 Technical elements of the COVID-19 digital certificate

The paradigm in the evolution of technical standards, which constitutes the current model of network security, is the public key infrastructure that has been mentioned throughout this article. This is also the framework for trust in the security, authenticity and validity of the COVID certificate. It is a chain of trust created only to manage electronic seals of certificates ranging from those of Member States' health authorities or other trusted authorities to each entity with the capacity to issue the certificates. For this reason, the Commission has created a centralised system that stores the public keys of the issuers of certificates: the EU Digital COVID Certificate gateway.

When a QR code is scanned, the issuing authority's electronic seal is verified via the corresponding public key, stored previously in the gateway. This corroborates the integrity and authenticity of the data. In this way, trust lies in the verification of the digital signature when the electronic seal contained in the certificate is linked with an authority that is qualified for its issue. Then, the principle of data minimisation is guaranteed in the design and, by default, in Article 25 of the GDPR, as personal data are not registered in the gateway. Instead, what are stored are the public keys of the entities that are responsible for the issue of the certificate. There is no opportunity to identify directly or indirectly the natural person who has received the Digital COVID Certificate based on an electronic seal.

The issue that public key infrastructure resolves is related to the creation of a secure communication channel that is mathematically encrypted between two or more parties to ensure that nobody other than the issuer is the author of certain information, the information has not been modified when it is received by the recipient, and the data can only be accessed by the specific recipient when it is sent to a sole recipient (Grassi et al., 2017), whether this is a contractor or private individual. This is the way that a specific piece of information is exchanged to decrypt the message: the key. Instead of a single key for encrypting and decrypting the message, public key cryptography uses two keys for two purposes: first, to ensure that a key always remains in the possession of the holder, the private key; and second, to enable the secure exchange of messages on an insecure network, where what is known as the public key can be disseminated without restrictions. Thus, while symmetric encryption depends completely on the fact that the issuer and receptor share the same key prior to the communication, asymmetrical encryption provides a more complex and, at the same time, more secure system, as there is a unique mathematical relationship between the public/private key pair that, in fact, is considered one of the drivers of global electronic trade (Adams & Lloyd, 1999).

This complexity of the system, apart from the complicated mathematics that guarantee the security depending on the level that is requested and the area in which it is applied, and the existence of many algorithms all with

a specific purpose (Wong, 2021), calls for the necessary interdiction of the law to resolve the question of how to link a certain public key to an entity. This led to the introduction of PKI to create, administer, distribute, use, store and revoke digital certificates, given that, as Adams and Lloyd (1999, p. 34) explained, the fundamental premise of the original formulation of public key cryptography was secure communication between two parties that were not previously related. This was resolved by the introduction of a trusted third party for the function of linked public keys to a certain identity. The third parties are known as *certification authorities*.

Following a pyramidal hierarchy, trust arises in a root authority, which in turn certifies intermediate authorities before reaching the end user, thus giving flexibility to the infrastructure and making it possible that certificates issued by a different authority be validated without having a common link between them. Simplified to the extreme, the functioning of the PKI of the COVID-19 certificate[25] follows the same structure as that described here. The difference is that the gateway managed by the European Commission acts *ad hoc* as a crucial point in the centralisation of the public keys of the authorities of each Member State for the issue of the COVID-19 certificate.

Therefore, a digital certificate is an electronic document encrypted with the private key of the certifying authority that includes the identification of the issuer of the certificate, the identification of the public key entity with which it is associated, the associated public key, additional information depending on the certificate and a digital stamp or hash[26] that serves as a unique identifier of the document to guarantee its integrity (Gisolfi, 2018). However, the term *certificate* serves to define two elements. The first is the subject of certification and the second is the electronic means for signing it, which is also called a *certificate*. That is, the authority in question issues a document that we have called a certificate with the data to be accredited. To seal it electronically (simply encrypting the document with the issuer's private key), it uses what is strictly speaking the electronic certificate that guarantees that it is what it claims to be. Therefore, two certificates come into play. For the user, the first is important, as it confirms the data that have been requested. For those who validate the data, the second is important to give validity to the first.

To sum up, the document sent to the interested party includes the four aforementioned concepts: the digital certificate, the hash or cryptographic summary, the electronic seal and the QR code to guarantee the certificate's proof, authenticity, integrity and validity,[27] which in turn bridges analogical and digital and can be reproduced on an on-screen or printed image that can be read with the camera of a mobile phone.

4.2 The contribution of the COVID-19 digital certificate to the sovereign identity project

The main innovation introduced by the European Digital Identity certificate, which is anticipated by the Digital COVID Certificate, is the progression from a model in which what is important is not the provision of an item of data for its processing, but to prove its existence. From the perspective of the principles of the SSI movement, this means giving more autonomy to the user regarding their data and improving compliance with the principle of data minimisation by default and design (Article 25 GDPR) and the right of access (Article 15 GDPR).

In terms of the above articles, the COVID-19 digital certificate means that the user holds a specific item of data, which is the information contained in the document in natural language. In this way, the holders of the certificate are free to display it to whoever they want. Consequently, the right of access is met. The certificate of the issuer, which gives reliability to the certified data, is contained in the QR code.[28] This respects data minimisation by default and design. Through this process, the health authorities provide interested parties with an electronic attestation of attributes in which what is important is no longer the item of data, but the

25 Annex IV of Commission Implementing Decision (EU) 2021/1073 of 28 June 2021.

26 The hash functions are cryptographic algorithms that have four main characteristics: a) they enable an alphanumerical code to be obtained with a fixed longitude of characters regardless of the volume of data processed; b) by applying the algorithm on the same data, the same result will always be obtained, c) the slightest variation in data will totally modify the code, and d) the process is not reversible, so the hash can always be determined through the data, but not the data through the hash (González-Meneses, 2019, p. 125).

27 For more information, see the website European Commission. Questions and Answers – EU Digital COVID Certificate (accessed on: 20.09.2021).

28 Recital six and Annex I of Implementing Decision (EU) 2021/1073.

certificate, which allows the authenticity of the issuer to be checked as well as the content integrity. From the perspective of data protection, there is no processing by the certificate validator, as the data that give rise to the certificate are already in each health system. In turn, validation is produced by consulting the gateway, which registers the capacity to issue and sign. In no case is the content of the certificates recorded, so the gateway does not contain personal data.[29]

However, despite the apparent simplicity of the functioning of the certificate, a deeper analysis reveals issues associated with its transparency from the perspective of the citizen, who is ultimately constrained to use it. In the case of the Catalan Health Service (CatSalut), the document that is made available to interested parties in PDF format does not contain other metadata to corroborate the validity and integrity of the document, because it is not sealed or protected against writing by the issuer. This means that the integrity of the PDF document or the correspondence of the data that it contains in natural language with the QR code cannot be guaranteed. This point could be improved with the electronic seal of the Catalan Health Service to guarantee no repudiation, data integrity and a time stamp.

The above solution considerably reduces the risk of falsification of certificates when they are in electronic format, which leaves the issue open in printed format. However, as indicated by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS),[30] there is a high risk associated with the falsification and illegal sale of false diagnostic tests to obtain a valid Digital COVID Certificate. This calls for measures to identify and mitigate the risks that may arise from the use of the certificate's issuing framework. Similarly, the EDPB and the EDPS have shown their concern about minimisation of the dataset to include in the certificate, and about the technical and organisational measures that could be adopted in line with data protection by design and default.

The considerations of the EDPB and the EDPS indicate the room for improvement that the European Digital Identity can bring with the creation of a digital wallet, from which it can use cryptographic tests of zero-knowledge proof (ZKP)[31] to reduce the use of the personal information that is included to correlate a person, such as physical address, postcode, name or birth date (European Union Agency for Cybersecurity, 2022, p. 10). In turn, the opportunity for selective disclosure through ZKP techniques is an option that current X.509 certificates on which the traditional PKI are constructed do not allow, given that their design depends on a centralised architecture whereby only trusted authorities can sign certificates (Fedrecheski et al., 2020). In this way, X.509 certificates associate a name and a unique identifier, such as the identity card, with the public key that is used in the identification process or electronic signature. They are always associated with personal data. This design necessarily involves showing all the data contained in the certificates, with the aggravation that the certifying authority always knows how many times the certificate has been used to access an electronic resource.

These are some of the issues that have arisen in the development of the European Digital Identity project as a result of the experience of the Digital COVID Certificate. However, among the improvements described, there is one that has not been mentioned. This is the improvement that paradigmatically ensures the functioning of the Digital COVID Certificate: the use of blockchain platforms to manage the certificate gateway. The strength and at the same time weakness of the entire system lies in this centralised file that is the gateway. The strength lies in the fact that the commitment of the issuer's file, or even the adoption of a default forgetting design so that a copy of the certified data is not stored, does not represent an obstacle for the validation of the certificate, as the custody of the data is transferred to the holder. The weakness is due to bringing together in one point the mechanism that makes the interoperability and functioning of the system possible. This mechanism is the validation of the issuers' public keys.

29 Recital nine of Implementing Decision (EU) 2021/1073.

30 Joint Opinion 4/2021 of EDPB and EDPS on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free circulation during the COVID-19 pandemic (Digital Green Certificate).

31 A zero-knowledge proof is a cryptographic algorithm that enables a user to accredit information without disseminating it and to verify that the information is true with a high level of probability (Bamberger et al., 2021).

5 Conclusions

The COVID vaccination certificate advances the change in model that the creation of the European Digital Identity Wallet envisions in the way that identity attributes can be shared. At the same time, it lightens the burden of regulatory compliance for authorities that issue the certificates and others that, for a legitimate interest, demand presentation of the certificate. As holders are given proof of the data under the responsibility of the signatory, it is no longer necessary to transfer data from the register that contains them when they are requested by a third party. It is the holder of the certified data who submits or displays the data.

In the current framework of the eIDAS Regulation, the need for identity solutions that would facilitate EU citizens' access to public services with their respective national methods in the entire European Union territory was a fundamental objective of the Regulation's enactment. However, the reality is that the difficulty in using tools such as the electronic identity card means that they are displaced by other trust service providers from the private sector or public sector platforms, such as Cl@ve in Spain, tools that do not enjoy cross-border interoperability to access services in accordance with Article 12 of the eIDAS Regulation. This is one of the main shortfalls of the Regulation. In response to this situation, the proposal to amend the eIDAS Regulation focuses on the European adaptation of the self-sovereign identity movement in its decentralised vision of data with the creation of the European Digital Identity. Two elements would enable this new system to function: the issue by Member States of a virtual wallet as a product and service to demonstrate identity, and the issue by trust service providers of electronic attestations of attributes that could be stored in this wallet.

The main challenge facing the revision of an identity model that was traditionally based on data transfer, compared to accreditation of the existence of data in compliance with proposals in the self-sovereign identity movement, is not only one of technological basis. The problem that the SSI movement aims to respond to lies in the conception of identity and negation of the need for legal recognition of its existence. In electronic environments, this means breaking with the dependence on third parties for users' activity on the internet. With this objective, the potential of blockchain networks has been seen, with European initiatives such as EBSI-ESSIF. They have a high level of privacy, are interoperable and could replace the current hierarchical PKI to manage digital identity. At the same time, one of the main improvements presented by the EBSI-ESSIF project in the European framework is the basis for the introduction of verifiable credentials and the mutual authentication of entities, whether they are physical people or legal entities, along with the opportunity to create secure communication channels for the exchange of messages without the need for an intermediary, as occurs with the current PKI model. All these factors are gathered in the proposal to amend the eIDAS Regulation, so that each State decides on the technological basis that it wants to use to comply with the mandate of the Digital Identity Wallet.

The COVID-19 vaccination certificate thus became a light implementation of the European Digital Identity project, continuing the path marked by the current version of the eIDAS Regulation and the GDPR, based on the responsibility and trust that are normatively attributed. The European Data Protection Board and the European Data Protection Supervisor have shown concerns about some areas in terms of the risks of potential falsification of diagnostic tests or vaccination to obtain a valid certificate, and on what data to include in the certificate. Technical measures that can be adopted to reduce risks involve implementing the pilot test of the Digital Identity Wallet and resorting to zero-knowledge cryptographic protocols to prove from the wallet that the user has an electronic document with the data that is requested and, if necessary, generating a derived file so that the document validator can accredit before the supervisor or the authority that makes the request that the verification has certainly been made. In this way, the guarantee of the validator of the certificate is reinforced without any user data needing to be processed.

In the current configuration of the COVID certificate, one question that affects the transparency for interested parties and that puts the soundness of the technological basis in the background is the trust that is imposed by legal norms. This sometimes generates concerns about the security of the system, as indicated by the EDPB and the EDPS. Improvements in the design of the certificate that contribute to this transparency could involve emphasising the way of determining whether the series of generic QR dots contained in the electronic document or the supporting image have been altered or not, and the inclusion of a hash that could be read and reproduced from any QR without the need to understand the content to check its integrity. Regarding

the security of the entire system, the management of a blockchain node by each Member State would enable decentralisation of the main critical point, which is the European gateway that stores the public keys used to validate the certificate.

There is still a long way to go, but the experience of the COVID certificate will be a valuable test of how to combine security and personal data in a new model for decentralised identity management in digital environments based on the free choice of individuals to use these tools as a complement to existing ones, the possibility of integrating new identity solutions in the deployment of the administration, and the defragmentation of the Digital Single Market.

6 References

About, Ilsen, & Denis, Vincent. (2011). *Historia de la identificación de las personas*. Ariel.

Adams, Carlisle, & Lloyd, Steve. (1999). *Understanding PKI: concepts, standards, and deployment considerations*. Macmillan Technical Publishing.

Alamillo Domingo, Ignacio. (2019a, March). El uso de los sistemas de identidad auto-soberana en el sector público español y en la Unión Europea. *Blockchain Intelligence*.

Alamillo Domingo, Ignacio. (2019b). *Identificación, firma y otras pruebas electrónicas*. Aranzadi.

Alamillo Domingo, Ignacio. (2020). SSI eIDAS legal report. European Commission.

Allen, Christopher. (2016, April 27). The path to self-sovereign identity. *CoinDesk*.

Bamberger, Kenneth A., Canetti, Ran, Goldwasser, Shafi, Wexler, Rebecca, & Zimmerman, Evan. (2021). Verification dilemmas in law and the promise of zero-knowledge proofs. *Berkeley Technology Law Journal*, *37*(1). http://dx.doi.org/10.2139/ssrn.3781082

Cameron, Kim. (2005, November 5). The laws of identity. *Kim Cameron's Identity Weblog*.

Cameron, Kim. (2018, November 4). Let's find a more accurate term than "self-sovereign identity". Kim *Cameron's Identity Weblog*.

European Union Agency for Cybersecurity. (2022). *Digital identity: Leveraging the self-sovereign identity (SSI) concept to build trust*. European Union.

Fedrecheski, Geovane, Rabaey, Jan, Costa, Laisa, Calcina-Ccori, Pablo, Pereira, William T., & Zuffo, Marcelo K. (2020, June 3). Self-sovereign identity for IoT environments: A perspective [Conference presentation]. 2020 Global Internet of Things Summit (GIoTS), virtual event.

Gisolfi, Dan. (2018, June 13). Self-sovereign identity: Why blockchain? *IBM Blockchain.*

González-Meneses, Manuel. (2019). *Entender blockchain: Una introducción a la tecnología de registro distribuido* (2nd edition). Aranzadi.

Internet. (1998). In Enciclopèdia.cat. https://www.enciclopedia.cat/gran-enciclopedia-catalana/internet

Grassi, Paul A., Garcia, Michael E., & Fenton, James L. (2017). Digital identity guidelines. *NIST Special Publication*, 1–48.

Hughes, Riley. (2020, September 23). Blockchain is the least interesting thing about self-sovereign identity. Medium.com.

Lessig, Lawrence. (1999). *Code and other laws of cyberspace* (1st edition). Basic Books.

Lessig, Lawrence. (2006). *Code 2.0.* Basic Books.

Llaneza González, Paloma. (2021). *Identidad digital. Actualizado a la Orden ETD/465/2021, de 6 de mayo (sobre métodos de identificación remota) y a la propuesta de Reglamento eIDAS2* (1st edition). Bosch.

Marlinspike, Moxie. (2012, February 15). What is "sovereign source authority"? The Moxy Tongue.

Reed, Drummond, & Preukschat, Alex. (2021). *Self-sovereign identity*. Manning.

Romero Bachiller, Carmen. (2009). Documentos y otras extensiones protésicas, o cómo apuntalar la "identidad". *Política y Sociedad*, *45*(3), 139–157.

Ruff, Timothy. (2018, October 30). 7 Myths of Self-Sovereign Identity. *Evernym*.

Wong, David. (2021). *Real-world cryptography*. Manning.