Revista catalana de dret públic #65

www.rcdp.cat

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

Raül Ramos Fernández*

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.

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

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.

* Raül Ramos Fernández, advocat de l'Il·lustre Col·legi de l'Advocacia de Sabadell, doctorand en dret per la Universitat Autònoma de Barcelona en l'especialitat de dret i noves tecnologies. Departament de Dret Públic i Ciències Historicojurídiques, Facultat de Dret, Edifici B2, c. de la Vall Moronta, 08193 Bellaterra (Cerdanyola del Vallès). raulramos@icasbd.org.

Article rebut el 15.01.2022. Avaluació cega: 12.02.2022 i 23.02.2022. Data d'acceptació de la versió final: 21.03.2022.

Citació recomanada: Ramos Fernández, Raül. (2022). Reflexions sobre el projecte d'Identitat Digital Europea a la llum del certificat COVID digital i el moviment sobre la *self-sovereign identity*. *Revista Catalana de Dret Públic*, *65*, 179-193. https://doi.org/10.2436/rcdp.i65.2022.3777

Sumari

1 Introducció

A partir de l'1 de juliol de 2021, les autoritats sanitàries dels diversos països membres de la Unió Europea i altres països adherits van començar a emetre el denominat *certificat COVID digital* per demostrar la salut en relació amb la pandèmia, amb fiabilitat i comprovable sense centralització, d'acord amb un document verificable mitjançant un codi QR (*quick response*) en possessió del seu titular, que serveix de pont entre el digital i l'analògic, per acreditar bé la vacunació, bé la realització d'una prova negativa de la presència del virus SARS-CoV-2 en un moment determinat o bé la recuperació de la malaltia COVID-19.

Aquest certificat, simple en concepte, però complex en disseny, suposa una fita de la interoperabilitat en la triple dimensió organitzativa, tècnica i de continguts en l'àmbit de la Unió. Per a la seva implementació es va adoptar, el juny de 2021, el Reglament (UE) 2021/953[1] a fi de garantir l'acceptació del certificat en el territori comunitari i definir el seu funcionament. En paral·lel, la seva implementació tecnològica ve determinada per la Decisió d'Execució (UE) 2021/1073[2] i les especificacions tècniques publicades per la Xarxa Sanitària Electrònica[3] (eHealth Network), que descriuen els mecanismes per al reconeixement mutu i d'interoperabilitat dels certificats de vacunació, de recuperació i de prova diagnòstica.

Amb el certificat emès per l'autoritat sanitària competent, és l'individu qui el mostra, sense que hi hagi un arxiu de dades centralitzat, un registre de les vegades que s'empra o una constància de a qui es presenta. Al contrari, la verificació de l'autenticitat i la integritat del contingut de la credencial depèn del segell electrònic contingut en el codi QR de l'emissor, que queda enregistrat de manera centralitzada a la passarel·la del certificat COVID digital de la UE.[4] Passem del tradicional model en què es comparteixen dades a un nou sistema: la prova de l'existència de dades amb l'entrega al titular d'un testimoni que certifiqui determinats atributs sota la responsabilitat del seu emissor. Ja no són necessaris l'emmagatzematge centralitzat de dades ni la cessió d'aquestes a un tercer, amb el perill que suposen la seva compilació i transmissió. A tall d'exemple, en el sistema de salut nacional espanyol, són les disset comunitats autònomes, mitjançant els seus respectius sistemes de salut, i l'Administració general de l'Estat per al cas de Ceuta i Melilla, qui posseeixen les dades dels ciutadans a qui s'entrega el certificat en el seu respectiu àmbit competencial. Es tracta d'una emissió descentralitzada amb normes, formats comuns i credibilitat creuada entre els emissors i verificadors dins del sistema.

Per consegüent, la novetat del disseny conceptual subjacent al certificat anticipa el model que, amb ple encaix en el Reglament general de protecció de dades (RGPD),[5] pretén convertir-se en el vehicle habitual de fer arribar i usar certificacions emeses per una autoritat en l'àmbit de la Unió Europea: l'emissió de declaracions electròniques d'atributs per tal que l'individu es trobi en possessió de les seves dades i pugui escollir a qui les cedeix.

A hores d'ara, en el si del mercat digital únic europeu, els elements que permeten provar la identitat, fets, actes i situacions respecte a un individu determinat romanen en els tercers que els emeten per aplicació del Reglament (EU) 910/2014 del Parlament i del Consell[6] d'identificació electrónica i serveis de confiança (Reglament eIDAS).[7] Contràriament, en un model de gestió de la identitat com el que introdueix la creació

1 Reglament (UE) 2021/953 del Parlament Europeu i del Consell, de 14 de juny de 2021, relatiu a un marc per a l'expedició, verificació i acceptació de certificats COVID-19 interoperables de vacunació, de prova diagnòstica i de recuperació (certificat COVID digital de la UE) a fi de facilitar la lliure circulació durant la pandèmia de COVID-19. (DOUE L, núm. 211, 15.06.2021, p. 1-22).

2 Decisió d'Execució (UE) 2021/1073 de la Comissió, de 28 de juny de 2021, per la qual s'estableixen especificacions tècniques i normes relatives a l'aplicació del marc de confiança per al certificat COVID digital de la UE establert pel Reglament (UE) 2021/953 del Parlament Europeu i del Consell. (DOUE L, núm. 230, 30.06.2021, p. 32-53).

3 Per a més informació, vegeu el web de la Comissió Europea Sanitat electrònica i COVID-19 (data d'accés: 21.09.2021).

4 Annex IV de la Decisió d'Execució (UE) 2021/1073, de la Comissió, de 28 de juny de 2021.

5 Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) (DOUE L, núm. 119, 04.05.2016, p. 1-88).

6 Reglament (UE) 910/2014 del Parlament Europeu i del Consell, de 23 de juliol de 2014, relatiu a la identificació electrònica i als serveis de confiança per a les transaccions electròniques en el mercat interior i pel qual es deroga la Directiva 1999/93/CE (DOUE L, núm. 257, 28.08.2014, p. 73-114).

7 Acrònim d'*electronic identification authentication and trust services.*

de la Identitat Digital Europea, per mitjà de la proposta de reforma del Reglament eIDAS,[8] que al seu torn s'emmiralla en el moviment d'identitat autosobirana (*self-sovereign identity,* SSI),[9] els posseeix el seu titular en una cartera virtual. El certificat de vacunació COVID-19 es mostra així com el mitjà idoni per introduir les possibilitats que les noves tecnologies, aplicades a la gestió de la identitat a la xarxa, poden oferir al mercat únic digital. En definitiva, es palesa la relació entre el certificat COVID digital de la Unió Europea, la proposta d'identitat digital europea i el moviment SSI, essent aquesta la qüestió a tractar mitjançant la conceptualització i l'anàlisi del marc jurídic creat *ad hoc* per donar resposta a la necessitat de garantir la lliure circulació dins de la Unió arran de la crisi sanitària.

Per tal d'assolir l'objectiu marcat, s'haurà de contraposar el marc jurídic actual de la gestió de la identificació a la Unió Europea amb la proposta de creació de la cartera d'identitat digital europea. Tot seguit, conceptualitzarem els postulats del moviment SSI i les tecnologies que s'hi relacionen, com la *blockchain* –per a les quals s'inclou la determinació d'un règim jurídic inèdit en la proposta de modificació del Reglament eIDAS–, aturant-nos momentàniament a fer entenedor com aquesta aplicació tecnològica ha suscitat de nou el debat de la identitat a la xarxa. En l'últim tram de la nostra exposició mostrarem el funcionament tècnic del certificat COVID, amb especial atenció a la infraestructura de clau pública (*public key infrastructure*, PKI),[10] la qual esdevé la principal clau de volta de la seguretat en entorns electrònics. Acabarem l'article amb l'aportació del certificat COVID al projecte d'identitat digital europea i la seva interacció amb l'RGPD, sense entrar en altres aspectes ètics i socials, com l'adequació a dret d'emprar el certificat per a altres usos diferents del desplaçament transfronterer, tot indicant les mancances que per a la confiança dels usuaris presenta el certificat, en aquest cas, prenent en consideració el certificat emès pel Servei Català de la Salut, pel fet que suposa el de l'àmbit territorial de qui subscriu.

2 La transició cap a un nou model de gestió de la identitat digital a la Unió Europea

En just un any la pandèmia de la COVID-19 ha canviat radicalment la digitalització dels serveis. La demanda de mitjans d'identificació i autenticació en línia, així com l'intercanvi d'informació digital relacionada amb la identitat, atributs o qualificacions, amb seguretat i un alt nivell de protecció, han augmentat exponencialment i han desbordat l'instrument jurídic que, en forma de reglament, habilita els mecanismes d'identificació i de signatura i segell electrònics[11] en entorns digitals, delimita els seus efectes jurídics[12] i regula els serveis de confiança prestats dins de la Unió, erigint-se en elements fonamentals en bé de la cohesió del mercat interior per expressió dels articles 26 i 114 del Tractat de Funcionament de la Unió Europea.[13]

Conforme amb l'anterior, un dels objectius del Reglament eIDAS és habilitar el reconeixement transfronterer de la identificació electrònica emesa pels estats membres per a l'accés a serveis públics i establir un mercat únic de serveis de confiança qualificats,[14] amb independència de l'estat membre que els aprova d'acord amb

8 Proposta de Reglament del Parlament Europeu i del Consell pel qual es modifica el Reglament (UE) núm. 910/2014 pel que fa a establir un marc per a una Identitat Digital Europea. Brussel·les, 03.06.2021 COM(2021) 281 final.

9 Ateses les connotacions del terme i les diverses propostes de traducció per la seva comunitat, s'emprarà en aquesta anàlisi el terme en anglès.

10 Actualment és la tècnica més generalitzada a la xarxa per a la vinculació d'una clau pública amb una persona determinada mitjançant un certificat digital amb l'aval d'una autoritat de certificació en un context centralitzat i jeràrquic del model de confiança (Gisolfi, 2018). Es basa en el joc de dues claus vinculades matemàticament que s'usen per xifrar o desxifrar la informació que es transmet per canals no segurs de comunicació. Mentre que la clau privada mai es mostra o comunica, el que resol la PKI és el mode com es difon la clau pública.

11 Diferenciem *signatura electrònica*, quan la crea una persona física per declarar la seva conformitat amb un contingut, de *segell electrònic*, quan aquest és creat per una persona jurídica per garantir l'origen i la integritat de les dades (art. 3 eIDAS).

12 Mentre que tant la signatura electrònica com el segell gaudeixen de determinats efectes jurídics, recollits als articles 25 i 35 de l'eIDAS, respectivament, la signatura digital és més genèrica i fa referència a les operacions matemàtiques basades en algoritmes de xifratge.

13 Tractat de la Unió Europea i Tractat de Funcionament de la Unió Europea. Versions consolidades. Protocols. Annexos. Declaracions annexes a l'Acta Final de la Conferència intergovernamental que ha adoptat el Tractat de Lisboa. (DOUE, núm. 82, 30.03.2010, p. 1-388).

14 Actualment, nou són els serveis de confiança qualificats sotmesos al Reglament eIDAS, la qual cosa comporta el reconeixement dels seus efectes jurídics en qualsevol estat membre: 1) emissió de certificat qualificat de signatura electrònica; 2) emissió de

el principi del mercat interior[15] i amb el mateix estatut jurídic que els processos tradicionals equivalents en paper a l'efecte d'agilitzar processos i reduir traves burocràtiques, heretades d'una tradició fortament basada en l'arxiu i en el registre documental de les antigues administracions sobre les quals es construïren els actuals estats europeus (About i Denis, 2011).

En un món globalitzat i canviant, però, eines com el Reglament eIDAS i l'RGPD, que han posicionat la Unió Europea com a capdavantera en la defensa de la privacitat i la confiança en entorns digitals, no poden romandre impassibles a les innovacions tecnològiques que es van succeint en curts períodes de temps. Conscient d'aquesta realitat, la Comissió Europea, seguint els objectius compromesos en la Brúixola Digital 2030[16] perquè a les acaballes de la dècada els ciutadans de la Unió puguin beneficiar-se d'un ampli desplegament d'una identitat fiable que permeti a cada usuari controlar les seves interaccions i la seva presència en línia, ha presentat recentment la proposta per a la modificació del Reglament eIDAS.[17] Una de les fites de la proposta és la creació d'un marc per a una Identitat Digital Europea prenent com a punt de partida, en l'exposició de motius i context de la proposta, que un nou moviment centrat a posicionar l'usuari com a gestor de la seva pròpia identitat a la xarxa ha agafat embranzida, en el qual la perspectiva d'una gestió centrada en identitats digitals rígides dona pas a la provisió i la confiança d'atributs específics relacionats amb aquestes identitats.

La confluència de diversos moviments socials com l'SSI, o els que simplement demanen major privacitat en entorns digitals, es reflecteix en aquesta nova proposta que pretén servir com a base jurídica per al desenvolupament de noves tecnologies com les del registre distribuït (*distributed ledger technology*, DLT), entre les quals la *blockchain*, d'acord amb la nomenclatura de llibres majors electrònics (*electronic ledgers*), en la proposta de modificació. Aquestes tecnologies, en la seva funció de suport, presenten la possibilitat de garantir en aquests registres electrònics immutables de codi obert[18] l'autenticitat i la integritat de les dades que contenen, així com l'exactitud de la data, l'hora i l'ordre cronològic per tal de seguir la seqüència de les transaccions. D'aquesta manera s'assegura la certesa que un succés registrat a la cadena en un moment determinat ho fou en aquell moment, utilitzant l'efecte dels segells de temps de manera similar a com s'usa en les signatures electròniques.[19]

Aquestes propietats de les xarxes de *blockchain* són, pels seus defensors, l'eina per a la implantació d'una capa d'identitat inèdita a la xarxa, així com l'alternativa desitjable als serveis de conservació de signatures i segells electrònics per garantir-ne la integritat en el decurs del temps.[20] Aquests registres descentralitzats presenten la capacitat d'erigir-se en font confiable d'informació dels prestadors habilitats per a l'emissió de credencials, a la manera de l'actual passarel·la del certificat COVID. La millora que plantegen les tecnologies de *blockchain* vers la configuració actual de la passarel·la, que actua com a registre centralitzat de les claus públiques dels diversos sistemes de salut de cada estat membre que permeten verificar les signatures del certificat COVID, és la seguretat reforçada que es coneix com la *immutabilitat de blockchain*, mitjançant la replicació per redundància de la informació en diversos nodes.

certificat qualificat de segell electrònic; 3) validació de signatura electrònica qualificada; 4) validació de segell electrònic qualificat; 5) conservació de signatura electrònica qualificada; 6) conservació de segell electrònic qualificat; 7) generació de segell de temps electrònic qualificat; 8) emissió de certificat d'autenticació de lloc web qualificat, i 9) servei d'entrega electrònica qualificada.

15 Article 4 de l'eIDAS.

16 Comunicació de la Comissió al Parlament Europeu, al Consell, al Comitè Econòmic i Social Europeu i al Comitè de les Regions: Brúixola Digital 2030: l'enfocament d'Europa per al Decenni Digital. COM(2021) 118 final.

17 Proposta de Reglament del Parlament Europeu i del Consell per la qual es modifica el Reglament (UE) 910/2014 pel que fa a la determinació d'un marc per a una Identitat Digital Europea. COM(2021) 281 final.

18 La construcció de *software* en codi obert implica que: a) qualsevol pot descarregar lliurement i gratuïtament tant la base de dades generada com el programa complet per executar-los al seu propi equip i convertir-se en node de sistema, o bé descarregar el programa, més limitat, que permet actuar com a simple usuari; b) qualsevol pot conèixer i examinar tant el codi font com la totalitat de la base de dades que genera el programa, i c) qualsevol pot modificar el programa (González-Meneses, 2019, p. 128).

19 Considerant 34 de la proposta de modificació del Reglament COM(2021) 281 final.

20 El servei de conservació de signatures o segells permet ampliar la fiabilitat de les dades de validació de la signatura o segell qualificat més enllà del període de validesa tecnològica inicial (Alamillo Domingo, 2019b, p. 426). El que es vol garantir és la continuïtat de la validesa d'un document en el temps davant la inevitable producció de documents que simulin haver-se signat en un moment pretèrit de manera fraudulenta. El tracte successiu del registre en xarxes *blockchain* promet alleugerir aquesta tasca, tot i que la immutabilitat de les dades registrades obliga a ser més curosos en el seu ús, per la qual cosa no en totes les circumstàncies es podria recórrer a aquesta aplicació de les tecnologies de registre distribuït, ni seria desitjable.

L'important, però, rau en el mode, en com la tecnologia pot emprar-se en entorns regulats per atendre problemàtiques encarades amb velles solucions i les seves inherents limitacions, que, progressivament, s'han posat greument en evidència des de la perspectiva de la privacitat i la seguretat de les dades en la gestió de la identitat digital. No debades, la Unió Europea ha treballat en les últimes dues dècades en diversos instruments jurídics en aquest sentit, començant amb l'aprovació de la Directiva 1999/93/CE,[21] derogada per l'actual Reglament eIDAS, que regulava les signatures electròniques basades en l'actual marc de la infraestructura de clau pública que s'imposa com a sistema jeràrquic per a l'emissió de certificats d'acord amb l'estàndard tècnic UIT-T X.509, per tal de confirmar la identitat del signant.

2.1 Limitacions del Reglament eIDAS

El Reglament eIDAS, des de la seva aprovació l'any 2014, projecta una federació d'identitats digitals dels ciutadans de la Unió amb la intenció de fer possible la interoperabilitat dels diversos sistemes d'identificació dels estats per a l'accés transnacional de serveis públics i poder usar, en conseqüència, les solucions d'identitat que cada estat decidís sense cap altre requisit addicional (Llaneza González, 2021, p. 142); en altres paraules, la possibilitat de fer servir el DNI electrònic per identificar-se davant una administració pública comunitària de la mateixa manera que es fa dins del territori nacional sense haver de seguir un procediment auxiliar, sistema que, tot i constituir una important fita vers la consolidació del mercat únic digital, es mostrava ja des del seu inici com una tímida aproximació a aquest objectiu.

Els principals esculls que han perllongat la desfragmentació del mercat únic digital en aquest àmbit es redueixen a tres qüestions crítiques: l'ús residual dels sistemes d'identificació nacional per la seva complexitat, sacrificant experiència de l'usuari per seguretat; la voluntarietat dels estats d'estendre les seves solucions d'identitat més enllà del seu territori, i l'exclusió del sector privat com a actor dins d'aquest projecte d'abast europeu (Alamillo Domingo, 2019a, p. 15). Això últim es tradueix en el fet de deixar de banda els sistemes d'identificació nacionals per autenticar-se en plataformes de prestadors privats en línia, cosa que genera dependència envers aquests tercers, que, al seu torn, demanen la creació de nous comptes i la cessió moltes vegades no justificada de dades, amb el que això comporta, com el monitoratge i l'aprenentatge del comportament dels usuaris en disposar de les identitats digitals registrades o vinculades al dispositiu d'accés, posant com a exemple el cas de les *cookies* (Alamillo Domingo, 2020, p. 9-10).

Aquesta manca d'ús dels sistemes digitals d'identitat emesos pels estats membres, que, al seu torn, són un bé públic, amb la contradicció que suposa per al mercat únic digital no poder-les usar de manera efectiva, és el que empeny la Comissió Europea, en exegesi de l'exposició de motius de la proposta de modificació del Reglament eIDAS, a oferir un nou marc comú, una identitat digital europea que permeti també l'accés a un ampli catàleg de proveïdors de serveis en línia del sector privat amb l'emissió d'una cartera digital europea.

2.2 Conceptualització del projecte d'identitat sobirana europea

Com s'ha anticipat, amb la proposta de modificació del Reglament eIDAS ens trobem davant un instrument jurídic centrat en l'usuari que cerca dotar-lo d'eines per fer-se càrrec dels seus atributs d'identitat, delegats voluntàriament o forçosa a terceres parts: ja no és quelcom que es fa a l'usuari, sinó realitzat per l'usuari.

Per aquest motiu, l'aposta de la Comissió és en la creació de la denominada *cartera d'identitat digital europea* (*european digital identity wallet*), definida per la proposta com un producte i servei que permeti a l'usuari emmagatzemar dades, credencials i atributs vinculats a la seva identitat,[22] així com crear signatures electròniques qualificades.[23] Qüestió diferent de la cartera com a continent és el contingut, l'emissió de declaracions electròniques

21 Directiva 1999/93/CE del Parlament Europeu i del Consell, de 13 de desembre de 1999, per la qual s'estableix un marc comunitari per a la signatura electrònica. (DOCE L, núm. 13, 19.01.2000, p. 12-20).

22 Art. 6.*b* de la proposta de modificació del Reglament eIDAS.

23 De conformitat amb l'article 25.2 de l'eIDAS, s'equipara amb la signatura manuscrita. En la transposició a l'ordenament jurídic espanyol per mitjà de la disposició final segona de la Llei 6/2020, d'11 de novembre, reguladora de determinats aspectes dels serveis electrònics de confiança (BOE, núm. 298, 12.11.2020, p. 98821-98841), que modifica l'article 326 de la Llei 1/2000, de 7 de gener, d'enjudiciament civil (BOE, núm. 7, 08.01.2000), el legislador nacional va més enllà i estableix una presumpció probatòria quan s'empra un servei qualificat, i es dona la paradoxa que ofereix més garantia la signatura electrònica basada en certificat qualificat que no pas la signatura manuscrita.

d'atributs –en aquest cas, emeses no pels estats membres, sinó per prestadors de serveis de confiança (art. 3.16 eIDAS)– que es defineixen provisionalment com una declaració en format electrònic que permet l'autenticació d'atributs,[24] els quals, al seu torn, serien trets, característiques o qualitats d'una persona física o jurídica o d'una entitat en format electrònic, com seria el cas del certificat COVID digital.

L'evolució proposada per la Comissió Europea és l'obtenció derivada d'un mitjà d'identificació electrònica addicional al mitjà nacional emprat. Això és, el mandat que cada estat, dins de la seva sobirania, emeti els mitjans d'identificació que consideri adients i, com a mínim, un de nivell de seguretat alt conforme a les normes tècniques que despleguen l'actual Reglament eIDAS. La novetat en l'entrega al ciutadà d'aquesta cartera d'identitat digital és poder-se identificar i autenticar davant qualsevol tercer. Un exemple d'això, traslladat al certificat COVID digital, suposa la capacitat d'incrementar seguretat, usabilitat i control en poder mostrar amb tota certesa la prova de vacunació, recuperació de la malaltia o prova diagnòstica. Des de la cartera es realitzaria de manera automàtica la verificació de la credencial i de la identitat de qui la mostra.

En la configuració actual, amb el certificat COVID digital es demana que s'acompanyi del document nacional d'identitat, i, mitjançant una comprovació visual de la credencial que és el certificat amb el document d'identitat, en tant que coincideixen les dades en ambdós documents, es produeix la validació. Els dubtes sobre la privacitat que això genera, i que ha motivat el pronunciament de l'Autoritat Catalana de Protecció de Dades,[25] posicionant-se a favor de la proporcionalitat d'aquesta pràctica quant a l'accés a les dades necessàries per verificar la identitat del posseïdor del certificat, quedarien resolts per la cartera d'identitat digital, en tant que mitjà d'identificació amb capacitat de mostrar dades de manera selectiva.

Qüestió diferent de la cartera com a mitjà d'identificació és la seva capacitació per emmagatzemar credencials d'atributs vinculats a la identitat, com pot ser el certificat COVID. La diferència és que ja no es tracta d'una manifestació de la sobirania nacional, sinó de l'emissió de certificacions que rau en els tercers de confiança i, per tant, susceptible de regulació pel Parlament Europeu i el Consell en bé de la cohesió del mercat interior per expressió dels articles 26 i 114 del Tractat de Funcionament de la Unió Europea. En lloc de la voluntat d'harmonitzar el dret preexistent –en escapar-se de les competències de la Comissió la modificació de les condicions de forma del dret civil i mercantil dels estats membres–, entra en joc l'interès pels serveis de confiança, la creació de noves institucions jurídiques europees, d'un nou dret europeu, amb els mateixos efectes jurídics que els seus equivalents als estats membres.

L'anterior és el que s'introdueix amb la proposta de modificació del Reglament eIDAS: superposar a les institucions nacionals preexistents –que no són interoperables i que no tenen un règim jurídic garantit– unes de noves, igual com ha succeït amb el catàleg de serveis de confiança i que configuren un mercat de dades de caràcter personal. Per consegüent, parlem d'un model d'identitat descentralitzada, on múltiples operadors emetran credencials d'identitat en sentit ampli.

Crear un instrument comú i interoperable pels sectors públic i privat per primera vegada en territori de la Unió Europea; la possibilitat d'aconseguir declaracions electròniques d'atributs, combinar-les i compartir les dades necessàries per a cada servei; la supressió del paper amb la dificultat que suposa compartir selectivament dades d'un certificat en format físic; o la privacitat per disseny en entregar les dades a l'usuari sense el monitoratge del seu ús per l'autoritat certificadora, és la proposta de modificació del Reglament eIDAS i, en aquest sentit, el certificat COVID digital, un dels seus assajos.

3 El moviment sobre la *self-sovereign identity*

Els principis en què s'emmiralla el certificat de vacunació COVID-19, i, per extensió, els presents en la creació de la identitat digital europea, són els propugnats pel moviment sobre la *self-sovereign identity*, traduït lliurement com a *identitat digital autosobirana*. Aquest moviment, conduït per noves tecnologies, estàndards en criptografia, xarxes distribuïdes, computació en núvol i l'accés generalitzat a dispositius mòbils, planteja

24 Art.1.3.*i* de la proposta de modificació del Reglament eIDAS.

25 Autoritat Catalana de Protecció de Dades. 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. Dictamen CNS, núm. 57/2021, 18.01.2022.

un nou model alternatiu als actuals models descentralitzats i federats de gestió de la identitat digital a Internet on l'usuari, de manera excloent i en exclusiva, es trobi en ple control de les seves dades.

Aquest nou model, sintetitzat per Allen (2016), amb l'experiència que comporta haver treballat en el desenvolupament dels protocols SSL/TLS de seguretat a la xarxa, ofereix una nova perspectiva d'un dels reptes més importants de la societat de la informació: la gestió segura de la identitat digital. A més, planteja el problema subjacent al sistema d'identitat sobre el qual es basen les societats modernes: el necessari reconeixement jurídic d'aquesta pels estats per fer subjecte l'individu de drets i d'obligacions, fins a arribar a la perversió que una persona pugui perdre la seva identitat, això és, la negació d'un seguit de drets inalienables, en equiparar la identitat administrativa a l'existència de l'individu mitjançant credencials i identificadors emesos en forma de llicències o passaports que, en últim terme, com a elements protètics, esdevenen la persona a la qual identifiquen (Romero Bachiller, 2009).

3.1 La polèmica del terme *sobirà*

Tot i remuntar-se el seu inici formal entorn de l'any 2015, el moviment SSI, com a tecnologia i proposta ideològica, és encara recent i no aliè a la controvèrsia per les seves connotacions. El que ha fet consolidar el terme, segons Reed i Preukschat (2021, p. 10-11), fins al punt que actualment és la denominació estàndard per fer referència a aquest nou model d'identitat, és, certament, l'ideari que evoca. En aquest sentit, *sobirà* (*sovereign*) en una visió amplia del terme, fa referència a l'autonomia o la independència de l'individu, i *auto* (*self*) fa referència a la connotació d'exclusió de tercers en la intervenció de l'autonomia personal de l'individu per a la seva existència.

Ara bé, l'atractiu del terme per a un sector social genera, per contra, reticència i recel en l'avaluació de les propostes que en la seva visió més radical introdueix el moviment SSI. Si bé no nega el poder de l'Estat –encara menys evadir la responsabilitat de l'individu com a subjecte de drets i obligacions–, ans al contrari, enfortir la relació entre Administració i ciutadà (Ruff, 2018), té com a meta reduir tant com sigui possible la seva presència en les interaccions de l'individu relacionades amb la privacitat, la identitat i la gestió de les dades personals.

Aquesta noció d'autogestió i d'autosobirania que introdueix el terme *self-sovereign identity* troba en Marlinspike (2012), en el que va anomenar *capacitat sobirana* (*sovereign source authority*), un dels seus orígens més directes no en el concepte, sinó en la concepció del terme que s'ha consolidat per fer referència al model d'identitat digital descentralitzada amb l'objectiu de donar resposta a una problemàtica d'extrema senzillesa en la seva formulació però de notòria complexitat en la seva resolució. I és que Internet, com exposà l'arquitecte en cap d'identitat de Microsoft, Kim Cameron (2005), es va crear sense una capa nadiua d'identitat, sense una manera de conèixer amb qui o què interacciona un usuari en navegar per la xarxa, amb els consegüents riscos de seguretat i criminalitat en un entorn fortament dependent per a tota mena de negocis jurídics i relacions socials.

Per Marlinspike, aquesta capacitat sobirana és el reflex de la natura de tot ésser viu d'actuar per si mateix i de la condició prèvia abans d'integrar-se dins de la societat; això és, de definir-se en la interacció amb la resta d'individus i com serà vist per aquests. Així ho resumeix lúcidament en exposar com aquesta construcció social que és la identitat entra en conflicte en reduir la capacitat sobirana a una existència administrativa, on el necessari apunt censal de l'individu i la seva prova impliquen un procés administratiu per a l'existència de la identitat i, en últim terme, de la persona com a subjecte de drets i obligacions, com a membre d'una societat determinada. Aquest model d'identitat, que és el que fins ara ha triomfat per atorgar seguretat jurídica en les relacions socials, traspassa als mecanismes de gestió de la identitat i als seus productes, en forma de certificats i credencials rígides, l'existència del seu titular i la seva capacitat d'obrar dins d'un context determinat, de manera que l'individu esdevé l'extensió d'aquests artefactes (Romero Bachiller, 2009).

Heus aquí l'ambivalència de la necessitat de contenir tota una proposta de caràcter polític en un instrument legislatiu que demana la necessària intervenció dels poders públics que es volen reduir o escapçar. Justament per aquest motiu hi ha veus autoritzades, com Cameron (2018) recollint la visió de Ruff (2018), que plantegen la necessitat d'emprar un nou terme, com *identitat descentralitzada*, a fi de dotar-lo de major neutralitat política i allunyar idees preconcebudes d'un concepte de transcendental complexitat.

3.2 L'aportació de la *blockchain* al debat de la identitat

El problema de base de la identitat a la xarxa, precisament, té a veure amb l'arquitectura inicial d'Internet i el seu objectiu inicial de permetre la comunicació entre dispositius pels diversos organismes dels Estats Units en una data tan llunyana com el 1969 –en referir-nos en termes absoluts pel que fa als seus orígens– amb la creació de la xarxa ARPANET per tal d'interconnectar dispositius i compartir recursos a través de diversos equips (Reed i Preukschat, 2021).

No seria fins al 1983, amb la transició al protocol TCP/IP, que s'obriria Internet als interessos comercials. I, com explicava el professor de la Universitat de Stanford Lawrence Lessig (1999), la necessitat de la identitat i l'autenticació no era dels dispositius, que quedava resolta pel protocol esmentat, sinó dels seus usuaris. Amb el protocol TCP/IP d'Internet només es coneixia –i es coneix– l'adreça de la màquina a la qual es demana un recurs, com l'accés a un lloc web, i això és així perquè originalment les persones que empraven Internet eren majoritàriament acadèmics. La comesa principal fou dissenyar una xarxa descentralitzada sense cap node neuràlgic, "de tal manera que, en l'eventualitat d'un atac massiu –especialment nuclear, pel període històric–, la comunicació no pogués ser mai completament desactivada"(Gran Enciclopèdia Catalana, 1998).

Anys més tard, i havent pres contacte amb el treball dut a terme per Cameron, Lessig (2006, p. 50-51) aprofundí en la qüestió, que és la que el moviment SSI pren en el seu ideari i la que la identitat digital europea vol acollir. En el seu estudi, Lessig exposava que el sistema d'identitat proposat en aquell temps per Microsoft pretenia la creació d'un protocol per habilitar una cartera virtual de credencials, amb els mateixos atributs que les tradicionals credencials en paper, però amb una seguretat fins llavors inèdita, amb vocació d'evitar el frau i facilitar la recuperació en cas de pèrdua del suport físic. Aquest projecte de Microsoft no només donaria major confiança que el format paper, sinó que permetria major control i precisió quant a les dades que són revelades a un tercer que les demani, tot sense la centralització de les dades en un sol punt on la confiança hagués de raure en un tercer, sinó en la tecnologia subjacent a l'arquitectura tècnica, la criptografia.

La senzillesa d'aquesta formulació teòrica, no possible tècnicament en el seu inici, ha estat recurrent al llarg dels anys amb cada innovació informàtica i ha agafat de nou embranzida pel fenomen *bitcoin* i la seva base tecnològica, que és la *blockchain.* Aquesta col·lecció de tecnologies es defensa com a eina adient per a la formulació d'un sistema de gestió de la identitat descentralitzada (Gonz*á*lez-Meneses, 2019, p. 173 i seg.), sense la intervenció de tercers, resistent a la censura, que garanteixi la privacitat i, per tant, sense la possibilitat que una autoritat pública hi pugui accedir o suprimir-ne o monitorar-ne dades.

Precisament les possibilitats que les tecnologies de registre distribuït –de les quals la *blockchain* és una de les seves aplicacions– poden aportar en la gestió d'una identitat digital descentralitzada, amb vocació de substituir l'actual infraestructura de clau pública, és el que ha portat a associar indivisiblement la *blockchain* amb el moviment SSI, però res més lluny de la realitat. Si bé la qüestió que resol la *blockchain* amb les monedes virtuals té similituds amb la problemàtica exposada en la gestió de la identitat, aquesta no es resol només amb la tecnologia que ha donat peu a introduir de nou en el debat tècnic i legislatiu un canvi en els actuals sistemes d'identitat a la xarxa (Hughes, 2020); per aquest motiu, trobarem en la proposta de modificació del Reglament eIDAS que es parli de registres de dades verificables a fi de donar cabuda a diverses tecnologies segons el principi de neutralitat tecnològica per fomentar l'exploració de noves propostes dins d'un marc de seguretat jurídica.

4 El certificat COVID digital de la Unió Europea

Per bé que el certificat digital COVID-19 i, per extensió, la proposta de modificació del Reglament eIDAS s'emmirallen en el moviment sobre la *self-sovereign identity*, cap dels instruments europeus citats suposa l'habilitació legal dels seus postulats o, com a mínim, de la seva totalitat, en tant que, des del vessant ideològic més radical, s'oposa a la dependència del mateix estat membre per a la determinació de la identitat de l'individu. El que sí que fan els instruments europeus és adaptar als principis rectors de la Unió i a la seva coherència interna aquells elements que li són compatibles en la línia de les demandes cada vegada més creixents en matèria de privacitat i seguretat en la gestió de l'actual ecosistema d'identitat a la xarxa, amb la necessària existència sota el presidi de l'RGPD d'un responsable identificable, subjecte a deures i obligacions

de les dades a tractar (art. 3 RGPD) i del dret dels interessats a no ser objecte de decisions fonamentades únicament en el tractament automatitzat que produeixi efectes jurídics (art. 22 RGPD).

Des d'aquesta perspectiva, el certificat COVID i el projecte d'Identitat Digital Europea han d'entendre's com l'equilibri triangular entre les demandes socials de major privacitat en entorns digitals, les dels sectors econòmics per garantir seguretat jurídica i de compliment normatiu en les seves transaccions en línia, així com la necessària intervenció de l'Estat, garant de la seguretat pública i jurídica dins de la seva sobirania. Com en tota innovació tècnica, i en aquest cas el certificat COVID no n'és una excepció, els antecedents exposats a l'apartat anterior han d'entendre's com un fil discursiu de la successió, en moltes ocasions prolífica en un curt període de temps, de propostes i solucions tècniques –àdhuc les que s'han quedat pel camí–, a fi de comprendre la finalitat perseguida per la Comissió Europea amb el certificat COVID i la proposta d'identitat digital europea.

També de manera indirecta cal entendre aquests instruments, en la mesura que fomenten l'adopció i el desenvolupament de nous estàndards tècnics per a una efectiva col·laboració entre el sector públic i el privat. Un exemple d'això el trobem en els estàndards de credencials verificables i identificadors descentralitzats de l'ecosistema de la *self-sovereign identity* que es desenvolupen pel World Wide Web Consortium (W3C) i que estan essent treballats per la Infraestructura Europea de Serveis de Cadena de Blocs (European Blockchain Service Infrastructure, EBSI), que és una iniciativa de la Comissió Europea per explorar l'aplicació d'aquestes tecnologies a diversos casos d'ús, entre elles el d'identitat digital, mitjançant el Marc Europeu d'Identitat Sobirana (European Self-Sovereign Identity Framework, ESSIF).

Una de les millores substancials que presenta el projecte EBSI-ESSIF al marc europeu és la base per a la introducció de credencials verificables i l'autenticació mútua d'entitats, siguin persones físiques o jurídiques, juntament amb la possibilitat de crear canals segurs de comunicació per a l'intercanvi de missatges sense la necessitat d'un intermediari, com succeeix amb l'actual model PKI. A la vegada, una arquitectura basada en l'intercanvi de credencials verificables a partir d'identificadors descentralitzats donaria pas a la possibilitat de configurar criptogràficament que les dades no puguin ser cedides a un tercer ni per a una finalitat diferent d'aquelles per a les quals foren sol·licitades, esdevenint en aquests casos il·legibles o marcades com a invàlides (Reed i Preukschat, 2021, p. 183).

4.1 Elements tècnics del certificat digital COVID-19

El paradigma en l'evolució d'estàndards tècnics, i que constitueix l'actual model de seguretat a la xarxa, és la infraestructura de clau pública de què al llarg de la nostra exposició s'ha fet menció. Aquest és també el marc de confiança per a la seguretat, l'autenticitat i la validesa del certificat COVID; en particular, es tracta d'una cadena de confiança creada només per a la gestió dels segells electrònics dels certificats que comprèn des de les autoritats sanitàries dels estats membres o altres autoritats de confiança fins a cada entitat amb capacitat d'expedir aquests certificats. Per aquest motiu, la Comissió ha creat un sistema centralitzat que emmagatzema les claus públiques dels emissors dels certificats: la passarel·la del certificat COVID digital de la UE.

En escanejar el codi QR, el segell electrònic de l'autoritat emissora es verifica mitjançant la corresponent clau pública, emmagatzemada amb anterioritat a la passarel·la, cosa que permet corroborar la integritat i l'autenticitat de les dades. D'aquesta manera, la confiança rau en la verificació de la signatura digital en vincular el segell electrònic contingut en el certificat amb una autoritat capacitada per a la seva l'emissió. Consegüentment, es garanteix el principi de minimització de dades des del disseny i, per defecte, de l'article 25 de l'RGPD en no registrar-se dades de caràcter personal a la passarel·la; en el seu lloc, el que s'emmagatzemen són les claus públiques de les entitats capacitades per a l'emissió del certificat, sense la possibilitat d'identificar directament ni indirectament una persona física a la qual s'hagi entregat un certificat COVID digital a partir del segell electrònic.

La qüestió que resol la infraestructura de clau pública té a veure amb la creació d'un canal segur de comunicació xifrat matemàticament entre dues o més parts per garantir que ningú més que l'emissor és l'autor d'una pretesa informació i que, en la seva recepció pel destinatari, aquesta no s'ha modificat i, per al cas de destinatari únic, que només aquest tingui accés a les dades (Grassi et al., 2017)contractors, or private individuals. Es tracta, per tant, de la manera com s'intercanvia una peça d'informació concreta per desxifrar el missatge: la clau. En

lloc d'una sola clau per xifrar i desxifrar el missatge, la criptografia de clau pública n'empra dues, amb doble finalitat: d'una banda, garantir que una clau roman sempre en possessió del seu propietari, la clau privada; de l'altra, permetre l'intercanvi de missatges segurs en una xarxa no segura, on sense restricció es pugui difondre la que es coneix com a clau pública. Així, mentre que el xifratge simètric depèn completament del fet que emissor i receptor comparteixen la mateixa clau amb anterioritat a la comunicació, el xifratge asimètric proporciona un sistema més complex i a la vegada més segur, en existir una relació matemàtica única entre el parell de claus pública/privada, que, de fet, es considera com un dels motors del comerç electrònic global (Adams i Lloyd, 1999).

Aquesta complexitat del sistema, fora de l'envitricollada matemàtica que garanteix la seguretat en funció del nivell que se'n demani i de l'àmbit on s'apliqui, així com l'existència de múltiples algoritmes, tots ells amb una finalitat concreta (Wong, 2021), demana la necessària interdicció del dret per resoldre l'interrogant de com vincular una determinada clau pública a una entitat. L'anterior va comportar la introducció de la PKI per crear, administrar, distribuir, usar, emmagatzemar i revocar certificats digitals, atès que, com explicaven Adams i Lloyd (1999, p. 34), la premissa fonamental de la formulació original de la criptografia de clau pública fou la comunicació segura entre dues parts no relacionades prèviament, que es resolia amb la introducció d'un tercer en qui ambdós confiessin per a la funció de vincular les claus públiques a una identitat determinada, que són les denominades *autoritats de certificació*.

Seguint una jerarquia piramidal, la confiança neix d'una autoritat arrel, que, al seu torn, certifica autoritats intermèdies abans d'arribar a l'usuari final, amb la qual cosa dona flexibilitat a la infraestructura i la possibilitat que certificats emesos per una autoritat diferent puguin ser validats sense haver-hi un nexe comú entre ells. Simplificat a l'extrem, el funcionament de la PKI del certificat COVID-19[26] segueix la mateixa estructura que l'exposada, amb la diferència que la passarel·la gestionada per la Comissió Europea actua *ad hoc* com a punt neuràlgic de la centralització de les claus públiques de les autoritats de cada estat membre per a l'emissió del certificat COVID-19.

Així doncs, un certificat digital és un document electrònic xifrat amb la clau privada de l'autoritat de certificació on es recull la identificació de l'emissor del certificat, la identificació de l'entitat la clau pública de la qual es vincula, la clau pública que es vincula, informació addicional segons el certificat i una empremta digital o *hash*[27] que serveix d'identificador únic al document per garantir la seva integritat (Gisolfi, 2018). Nogensmenys, el terme *certificat* serveix per definir dos elements: d'una banda, el que és objecte de certificació, i, de l'altra, el mitjà electrònic per a la seva signatura, que també es denomina *certificat*. És a dir, l'autoritat en qüestió expedeix un document que hem anomenat *certificat* amb les dades a acreditar, i, per segellar-lo electrònicament –simplement xifrar el document amb la clau privada de l'emissor–, empra el que pròpiament és el certificat electrònic, que assegura que és qui diu ser, de manera que entren en joc dos certificats. Per a l'usuari, l'important és el primer, que acredita la dada que es demana, i per a qui l'ha de validar, el segon, per tal com atorga validesa al primer.

En resum, en el document que es fa arribar a l'interessat entren en joc quatre conceptes ja esmentats: el certificat digital, el *hash* o resum criptogràfic, el segell electrònic i el codi QR per garantir comprovació, autenticitat, integritat i validesa del certificat,[28] que a la vegada serveix de pont entre l'analògic i el digital i es pot reproduir en una imatge en pantalla o en paper i llegir amb una càmera d'un telèfon mòbil.

4.2 L'aportació del certificat digital COVID-19 al projecte d'identitat sobirana europea

La principal innovació que s'introdueix amb el projecte d'identitat digital europea, i que ens anticipa el certificat digital COVID-19, és la progressió a un model on l'important no és facilitar una dada per al seu

26 Annex IV de la Decisió d'Execució (UE) 2021/1073, de la Comissió, de 28 de juny de 2021.

27 Les funcions resum *hash* són algoritmes criptogràfics que presenten quatre grans característiques: a) permeten l'obtenció d'un codi alfanumèric d'una longitud de caràcters fixa amb independència del volum de dades processades; b) aplicat l'algoritme sobre les mateixes dades sempre s'obté el mateix resultat; c) la mínima variació en les dades modificarà totalment el codi, i d) el procés no és reversible, de manera que es pot conèixer el *hash* mitjançant les dades, però no les dades mitjançant el *hash* (González-Meneses, 2019, p. 125).

28 Per a més informació, vegeu el web de la Comissió Europea. Preguntes i respostes. Certificat COVID digital de la UE (data d'accés: 20.09.2021).

tractament, sinó acreditar la seva existència. Des del punt de vista dels principis del moviment SSI, això suposa donar més autonomia a l'usuari respecte a les seves dades i millorar el compliment tant del principi de minimització de dades per defecte i des del disseny (art. 25 RGPD) com del dret d'accés (art. 15 RGPD).

Quant als articles citats, amb el certificat digital COVID-19 l'usuari es troba en possessió d'una dada concreta, que és la informació continguda en el document en llenguatge natural. D'aquesta manera el posseïdor del certificat té la llibertat d'exhibir-la a qui decideixi, amb la qual cosa es compleix el dret d'accés. Pel que fa al certificat de l'emissor, que permet donar fiabilitat a les dades certificades, aquest es conté en el codi QR,[29] amb la qual cosa es respecta la minimització per defecte i des del disseny. Mitjançant aquest procediment, les autoritats sanitàries entreguen als interessats una declaració electrònica d'atributs on l'important ja no és la dada, sinó el certificat, que permet assegurar autenticitat emissora, així com integritat de contingut. Des del punt de vista de la protecció de dades, no hi ha cap tractament pel validador del certificat, ja que les dades que donen origen al certificat es troben en cada sistema de salut. Per la seva banda, la validació es produeix mitjançant la consulta a la passarel·la, la qual censa la capacitat d'emetre i signar. En cap cas s'enregistra el contingut dels certificats, per la qual cosa la passarel·la no conté dades personals.[30]

Ara bé, tot i l'aparent senzillesa del funcionament del certificat, s'amaguen en una anàlisi més profunda qüestions relacionades amb la seva transparència des del punt de vista del ciutadà, qui en últim terme es veu constret al seu ús. En el cas del Servei Català de la Salut, el document que es posa a disposició dels interessats en format PDF no conté altres metadades que permetin corroborar la validesa i la integritat del document perquè no es troba segellat ni protegit contra escriptura per l'emissor. Això vol dir que no pot garantir-se la integritat del document PDF ni la correspondència de les dades que s'hi contenen en llenguatge natural amb el codi QR, punt que es pot millorar amb el segell electrònic de Servei Català de la Salut per garantir no repudi, integritat de les dades i marca de temps.

L'anterior solució redueix substancialment el risc de falsificació dels certificats quan es tracta del format electrònic, cosa que deixa oberta la qüestió en el format paper. Així i tot, com han indicat el Comitè Europeu de Protecció de Dades (CEPD) i el Supervisor Europeu de Protecció de Dades (SEPD),[31] existeix un alt risc relacionat amb la falsificació i la venda il·lícita de proves diagnòstiques falses per obtenir un certificat COVID digital vàlid, fet que demana mesures per identificar i mitigar els riscos que puguin derivar-se de l'ús del marc d'emissió del certificat. De la mateixa manera, el CEPD i el SEPD han mostrat la seva preocupació sobre la minimització del conjunt de dades a incloure al certificat, així com les mesures tècniques i organitzatives que es puguin adoptar en consonància amb la protecció de dades des del disseny i per defecte.

Les consideracions realitzades pel CEPD i el SEPD apunten al marge de millora que la Identitat Digital Europea pot aportar amb la creació d'una cartera digital, des de la qual es puguin emprar proves criptogràfiques de coneixement nul (*zero knowledge proof*, ZKP)[32] per a la reducció de l'ús d'informació personal que porti a correlacionar una persona, com la direcció física, el codi postal, el nom o la data de naixement (European Union Agency for Cybersecurity, 2022, p. 10). Al seu torn, la possibilitat de fer una divulgació selectiva mitjançant tècniques ZKP és una opció que els actuals certificats X.509 sobre els quals es construeixen les tradicionals PKI no permeten, atès que el seu disseny depèn d'una arquitectura centralitzada per la qual només les autoritats de confiança poden signar certificats (Fedrecheski et al., 2020). D'aquesta manera, els certificats X.509 vinculen un nom i un identificador únic, com el DNI, a la clau pública que s'usa en el procés d'identificació o signatura electrònica, i que sempre porten associats dades de caràcter personal. Aquest disseny comporta necessàriament mostrar totes les dades contingudes als certificats, amb l'agreujament que suposa que l'autoritat de certificació tingui coneixement de les vegades que s'empra el certificat per a l'accés a un recurs electrònic.

29 Considerant sisè i annex I de la Decisió d'Execució (UE) 2021/1073.

30 Considerant novè de la Decisió d'Execució (UE) 2021/1073.

31 Dictamen conjunt 4/2021 del CEPD i el SEPD sobre la proposta de Reglament del Parlament Europeu i del Consell relatiu a un marc per a l'expedició, la verificació i l'acceptació de certificats interoperables de vacunació, de test i de recuperació per facilitar la lliure circulació durant la pandèmia de COVID-19 (certificat verd digital).

32 Una prova de coneixement nul és un algoritme criptogràfic que permet a l'usuari acreditar una informació sense divulgar-la i verificar que la informació és certa amb un alt valor de probabilitat (Bamberger et al., 2021).

Aquestes són algunes de les qüestions que l'experiència del certificat COVID digital suscita en el desenvolupament del projecte d'Identitat Digital Europea, però entre les millores apuntades n'hi ha una a la qual no s'ha fet referència, i és la que paradigmàticament garanteix el funcionament del certificat COVID digital: l'ús de plataformes de *blockchain* per gestionar la passarel·la del certificat. Precisament la fortalesa i a la vegada la debilitat de tot el sistema rau en aquest arxiu centralitzat que és la passarel·la: fortalesa en tant que el compromís de l'arxiu de l'emissor, o fins i tot l'adopció d'un disseny d'oblit per defecte, on no s'emmagatzemés una còpia de la dada certificada no suposaria cap obstacle per a la validació del certificat, en traslladar-se la custòdia de la dada al seu titular; debilitat davant la feblesa que suposa recollir en un sol punt el mecanisme que fa possible la interoperabilitat i el funcionament del sistema, que és la validació de les claus públiques dels emissors.

5 Conclusions

El certificat de vacunació COVID avança el canvi de model que planteja la creació de la Cartera d'Identitat Digital Europea en la forma com es poden compartir atributs d'identitat. Alhora, alleuja la càrrega de compliment normatiu de les autoritats emissores dels certificats i els tercers que, per un interès legítim, demanen la seva exhibició. Amb l'entrega als titulars d'un testimoni de les dades sota la responsabilitat del signant es fan innecessàries la cessió i la sortida del registre en què es contenen quan són demanades per un tercer: és el titular en possessió de la dada certificada qui fa entrega o exhibició d'aquesta.

En el marc vigent del Reglament eIDAS, la necessitat de solucions d'identitat que facilitessin l'accés dels ciutadans de la Unió a serveis públics amb els seus respectius mètodes nacionals a tot el territori comunitari fou l'objectiu primordial de la seva promulgació. La realitat, però, és que la dificultat en l'ús d'eines com el DNI electrònic fa que quedin desplaçades per altres prestadors de confiança del sector privat o plataformes del mateix sector públic, com Cl@ve en el cas espanyol, eines que no gaudeixen de la interoperabilitat transfronterera per a l'accés a serveis públics conforme a l'article 12 de l'eIDAS, per la qual cosa esdevenen una de les principals carències del reglament. Com a resposta a aquesta situació, la proposta de revisió del Reglament eIDAS planteja l'adaptació europea del moviment sobre la *self-sovereign identity* en la seva visió descentralitzada de les dades amb la creació de la Identitat Digital Europea. Els elements que farien funcionar aquest nou sistema són dos: l'emissió per part dels estats membres d'una cartera virtual com a producte i servei per demostrar la identitat, i l'emissió per part de prestadors de serveis de confiança de declaracions electròniques d'atributs que puguin ser emmagatzemades en aquesta cartera.

El principal repte a què s'enfronta la revisió d'un model d'identitat basat tradicionalment en la cessió de dades –enfront de l'acreditació de l'existència d'aquestes en l'observança de les propostes del moviment sobre la *self-sovereign identity*– no només és de base tecnològica. La problemàtica a la qual el moviment SSI pretén donar resposta rau en la mateixa concepció de la identitat i la negació de la necessitat de reconeixement jurídic de la seva existència; en entorns electrònics, suposa trencar amb la dependència de tercers per al desenvolupament de l'usuari a la xarxa. Amb aquest objectiu, s'ha vist el potencial que les xarxes de *blockchain*, amb iniciatives europees com EBSI-ESSIF, presenten per assolir un nivell alt de privacitat i a l'hora interoperable, amb vocació de substituir l'actual PKI jeràrquica per a la gestió de la identitat digital. En paral·lel, una de les millores substancials que presenta el projecte EBSI-ESSIF al marc europeu és la base per a la introducció de credencials verificables i l'autenticació mútua d'entitats, siguin persones físiques o jurídiques, juntament amb la possibilitat de crear canals segurs de comunicació per a l'intercanvi de missatges sense la necessitat d'un intermediari, com succeeix amb l'actual model PKI. Totes aquestes sensibilitats es recullen en la modificació de la proposta de modificació del Reglament eIDAS, perquè sigui cada estat el que decideixi sobre la base tecnològica que vol emprar per complir amb el mandat de la cartera d'identitat digital.

El certificat de vacunació COVID-19 esdevé així una aplicació lleugera del projecte d'Identitat Digital Europea, continuant el camí marcat per l'actual versió del Reglament eIDAS i l'RGPD, basats en la responsabilitat i la confiança que s'atribueixen normativament. Tanmateix, hi ha qüestions sobre les quals el Comitè Europeu de Protecció de Dades i el Supervisor Europeu de Protecció de Dades han mostrat la seva preocupació quant als riscos de possible falsificació de proves diagnòstiques o de vacunació per obtenir un certificat vàlid i sobre les dades a incloure al certificat. Mesures tècniques que es puguin adoptar per reduir el risc passen per implantar el pilot de la cartera d'identitat digital i el recurs a protocols criptogràfics de coneixement nul per acreditar

des de la cartera que l'usuari posseeix un document electrònic amb la dada que es demana, i, si escau, generar un arxiu derivat perquè el validador del document pugui acreditar davant el supervisor o l'autoritat que li demani que, certament, ha realitzat la verificació. D'aquesta manera es reforça la garantia pel validador del certificat sense que en el procés pugui processar cap dada de l'usuari.

En l'actual configuració del certificat COVID, una qüestió que afecta la transparència vers els interessats que deixa en segon pla la solidesa de la base tecnològica és la confiança que ve imposada normativament, cosa que a la vegada genera dubtes en la seguretat del sistema, tal com han indicat el CEPD i el SEPD. Millores en el disseny del certificat que contribueixin a aquesta transparència podrien passar per emfatitzar el mode de determinar si el seguit de punts del QR genèric contingut en el document electrònic o la imatge com a suport han estat alterats o no, així com la inclusió d'un *hash* que es pugui llegir i reproduir de qualsevol QR sense necessitat de conèixer el seu contingut per comprovar la seva integritat. Pel que fa a la seguretat de tot el sistema, la gestió d'un node de *blockchain* per cada estat membre permetria descentralitzar el principal punt crític, que és la passarel·la europea que conté les claus públiques que validen el certificat.

El camí a recórrer encara és llarg, però l'experiència del certificat COVID suposarà un valuós assaig de com conjugar seguretat i dades personals en un nou model de gestió de la identitat descentralitzada en entorns digitals basat en la lliure elecció dels particulars per emprar aquestes eines com a complement de les ja existents, la possibilitat d'integrar noves solucions d'identitat en el desplegament de l'Administració i la desfragmentació del mercat únic digital.

6 Referències

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

Adams, Carlisle, i Lloyd, Steve. (1999). *Understanding public-key infrastructure: concepts, standards, and deployment considerations*. Macmillian Technical Publishing.

Alamillo Domingo, Ignacio. (2019a). 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. Comissió Europea.

Allen, Christopher. (2016). The path to self-sovereign identity. *Coin Desk*.

Bamberger, Kenneth A., Canetti, Ran, Goldwasser, Shafi, Wexler, Rebecca, i Zimmerman, Evan. (2021). Verification dilemmas in Law and the promise of zero-knowledge proofs. *Berkeley Technology Law Journal*, *37*(1).

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

Cameron, Kim. (2018). 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*. https://doi.org/10.1109/MTAS.2004.1337889

Fedrecheski, Geovane, Ccori, Pablo C. Calcina, Pereira, William T., i Zuffo, Marcelo K. (2020). *Self-sovereign identity for IoT environments : A perspective*.

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

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

Gran Enciclopèdia Catalana. (1998). *Internet*.

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

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

Lessig, Lawrence. (1999). *Code and other laws of cyberspace* (1a ed.). 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* (1a ed.). Bosch.

Marlinspike, Moxie. (2012). What is "sovereign source authority"? *The Moxie tongue*

Reed, Drummond, i 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). 7 Myths of self-sovereign identity. *Evernym*.

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