IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

ARTICLE

A la recerca del règim jurídic de les proves de coneixement nul en la construcció de la identitat digital europea

Raül Ramos Fernández
Universitat Oberta de Catalunya

Data de presentació: octubre 2022
Data d'acceptació: juliol 2023
Data de publicació: octubre 2023

Resum

Els protocols criptogràfics de prova de coneixement permeten acreditar l'existència, possessió o coneixement d'una dada revelant només que la declaració feta sobre ella és certa. Aquest article proposa un esquema d'investigació per definir el valor jurídic d'aquests protocols per al desenvolupament de sistemes d'identitat digital dins de la Unió Europea. La darrera esmena a la proposta de modificació del Reglament eIDAS, publicada el febrer de 2023, introdueix nous objectes jurídics: la cartera d'identitat digital europea, les declaracions electròniques d'atributs i les proves de coneixement nul, aquestes com a funcionalitat auxiliar dels dos objectes anteriors. El problema és que la proposta no estableix el règim jurídic adequat per garantir la validesa de les proves de coneixement nul davant de les autoritats supervisores. Amb l'objectiu de redreçar la situació, l'article analitza conceptes com les cadenes de blocs, la identitat digital sobirana, la proposta eIDAS 2.0 i la unió de tots aquests elements en la solució comercial d'identitat digital Hyperledger Indy. Concloem que un marc regulador de proves de coneixement nul amb tres pilars –una regulació de producte informàtic, una regla d'equivalència entre les declaracions i les dades de la cartera amb les seves transformacions matemàtiques i la possibilitat d'imposar l'acceptació d'aquestes proves– pot contribuir a obrir noves perspectives en la direcció que han de prendre els sistemes d'identitat digital de la Unió Europea i el rol que els estats han d'assumir per equilibrar seguretat pública, privacitat dels usuaris i liberalització del mercat.

Paraules clau

reglament eIDAS; proves de coneixement nul; identitat digital sobirana; cadenes de blocs; cartera d'identitat digital europea; declaració electrònica d'atributs

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

In search of the legal regime for zero-knowledge tests in the construction of the European Digital Identity

Abstract

Zero-knowledge proof cryptographic protocols allow to prove the existence, possession or knowledge of a data revealing only that the statement made about it is true. This article proposes a research scheme to define the legal value of these protocols for the development of digital identity systems within the European Union. The last amendment to the modification to the eIDAS Regulation, published in February 2023, introduces new legal objects: the European digital identity wallet, the electronic attestation of attributes and the zero-knowledge proofs protocols, these as auxiliary functionality of the two previous objects. The problem is that the proposal does not establish the appropriate legal regime to guarantee the validity of zero-knowledge attestations to the supervisory authorities. In order to address the situation, the article analyses concepts such as blockchain, Self-Sovereign Identity, the eIDAS 2.0 proposal and the union of all these elements in the Hyperledger Indy digital identity commercial solution. We conclude that a regulatory framework for zero-knowledge proofs with three pillars – a regulation of computer products, a rule of equivalence between declarations and wallet data with their mathematical transformations and the possibility of imposing acceptance of these tests – can help to open new perspectives in the direction that the European Union's digital identity systems must take and the role that states must assume in balancing public safety, user privacy and market liberalization.

Keywords

eIDAS regulation; zero-knowledge proofs; self-sovereign identity; blockchain; European digital identity wallet; electronic attestation of attributes

Introducció

Els protocols criptogràfics de prova de coneixement nul (ZKP, *zero-knowledge proof*) són objectes matemàtics que permeten demostrar el coneixement, l'existència, la possessió o la correcció d'una dada sense necessitat de compartir-la, tot complint així amb els principis rectors del Reglament general de protecció de dades, RGPD[1] (Agència Europea de Ciberseguretat, 2022a, pàg. 22). Aplicades a sistemes d'identitat digital, les ZKP proporcionen privacitat, seguretat i verificació en canals insegurs, la qual cosa redueix els riscos associats a l'emmagatzematge i a l'exposició de dades personals.

Proposades per Goldwasser, Micali i Rackoff (1985), les ZKP es van popularitzar en la comunitat *blockchain*[2] a partir del fenomen del bitcoin i de les monedes digitals com Zerocash (Ben-Sasson *et al*., 2014), amb l'objectiu de proveir de privacitat i fer anònimes les transaccions en un canal com són les cadenes de blocs, les quals proporcionen un registre replicat entre tots els membres que conformen la cadena sense autoritats centrals, transparència en les dades que s'ancoren i resistència a la manipulació. La possibilitat d'emprar les cadenes de blocs per crear sistemes d'identitat al marge de qualsevol proveïdor, inclòs l'Estat, i l'ús de les ZKP per garantir la privacitat va fer que el moviment d'identitat digital sobirana (*self-sovereign identity*, SSI) proposés el desenvolupament de sistemes d'identitat digital basats en aquestes tecnologies (Allen, 2016).

Les propostes SSI estan contingudes en solucions comercials d'identitat digital, com ara Hyperledger Indy, solució que empra cadenes de blocs per a la descentralització del sistema; en identificadors descentralitzats (*decentralized identifiers*, DID), per crear i gestionar les identitats digitals de manera independent sota el control de l'usuari; en credencials verificables (*verifiable credentials*, VC) a manera de certificats digitals, com podria ser el certificat COVID digital; en proves de coneixement nul per ancorar l'anterior informació a les cadenes de blocs, i en una cartera digital en format d'aplicació mòbil per gestionar, emmagatzemar i administrar les credencials, així com per interactuar amb la cadena de blocs.

Paral·lelament, amb motiu de la revisió prevista en l'article 49 del Reglament 910/2014 de 23 de juliol[3] –Reglament eIDAS–, es va introduir en la proposta de modificació[4] –Reglament eIDAS 2.0– la creació de nous objectes normatius semblants als introduïts per Hyperledger Indy, però totalment diferents d'aquests que es poguessin emprar per explorar nous models de gestió de la identitat sota el principi de neutralitat tecnològica. Aquests objectes van ser la cartera d'identitat digital europea (*European Digital Identity Wallet*, EUDIW), els llibres majors electrònics i les declaracions electròniques d'atributs. La darrera esmena[5] a la proposta de modificació del Reglament eIDAS 2.0 porta a la inclusió de les ZKP en el text legal, però només quant a la seva definició i la seva funcionalitat com a element de suport a l'EUDIW i a les declaracions electròniques d'atributs.

La problemàtica que tractem en el present article és la manca de desenvolupament en la proposta consolidada eIDAS 2.0 d'un marc legal que permeti emprar les ZKP per a la construcció de sistemes d'identitat digital a la Unió Europea, amb la garantia per al receptor de les dades de poder acreditar el compliment de les seves obligacions legals davant l'autoritat supervisora quan vulgui acceptar una prova de coneixement nul. Els autors Alamillo Domingo, I., Valero Torrijos, J., Fortune, D. i Martin, D. (2017) van demostrar la viabilitat d'emprar protocols ZKP en un projecte pilot dut a terme a l'aeroport de Leeds Bradford

1. 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* núm. 119, de 4 de maig de 2016, pàg. 1-88 (88 pàg.). DOUE-L-2016-80807.
2. Traduït com a cadena de blocs.
3. Reglament (UE) nº 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 al mercat interior i per la qual es deroga la Directiva 1999/93/CE. DOUE núm. 257, de 28 d'agost de 2014, pàg. 73-114 (42 pàg.). DOUE-L-2014-81822.
4. Brussel·les, 3.6.2021 COM(2021) 281 final 2021/0136 (COD) Proposta de reglament del Parlament Europeu i del Consell pel qual es modifica el Reglament (UE) n.º 910/2014 pel que fa a l'establiment d'un marc per a una identitat digital europea {SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}.
5. 2021/0136 (COD) 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 Rapporteur: Romana Jerković CONSOLIDATED TEXT - COMPROMISE AMENDMENTS (EPP, S&D, Renew, Greens, The Left) 7 February 2023.

per acreditar la possessió d'una targeta d'embarcament vàlida i en conseqüència deduir l'IVA dels establiments de la zona lliure d'impostos, però sense poder reproduir-ho posteriorment davant l'autoritat tributària per la manca d'efectes jurídics de les ZKP.

La nostra hipòtesi és que la problemàtica anterior pel que fa a la manca de valor legal de les ZKP es pot redreçar amb tres pilars: en primer lloc, una regulació de producte informàtic que pugui instal·lar-se a l'EUDIW o que actuï de manera autònoma; en segon lloc, la definició d'una regla d'equivalència entre una declaració electrònica d'atributs i la informació personal emmagatzemada a l'EUDIW amb les dades derivades en format ZKP, i, en tercer lloc, la imposició d'acceptar una prova de coneixement nul en determinades interaccions.

Per tal d'assolir l'objectiu anterior, exposarem els casos potencials d'ús de les ZKP i les problemàtiques que presenten; ens aturarem a conceptualitzar les cadenes de blocs i la seva relació amb les ZKP; examinarem l'encaix de les ZKP amb les propostes SSI i la translació d'aquestes en l'entorn europeu; introduirem la proposta eIDAS 2.0, juntament amb l'actual versió consolidada i analitzarem l'abast de la reforma; exposarem com Hyperledger Indy se situa per davant del debat que planteja la proposta eIDAS 2.0 mitjançant un sistema que actualment està en el mercat; tancarem amb els fonaments que han de permetre desenvolupar un règim adient per a les ZKP, i acabarem amb les conclusions més rellevants.

1. Antecedents

1.1. Proves de coneixement nul

Les proves de coneixement nul permeten demostrar el coneixement d'un valor determinat revelant només el fet que es coneix aquella informació, la qual cosa permet implementar tres mesures recollides en l'article 25 del RGPD, la seguretat, minimització i limitació a l'accessibilitat de les dades (Agència Espanyola de Protecció de Dades –AEPD–, 2020). D'aquesta manera, es podria acreditar des d'una cartera d'identitat digital, sota l'exclusiu control de l'usuari, que es disposa d'una credencial que certifica la majoria d'edat quan un servei en línia tingui l'obligació legal de demanar-ho, o bé per adquirir en un establiment físic productes que sol·licitin acreditació de l'edat, però no es comparteix el DNI, i per tant no es poden capturar dades que es puguin fer servir de manera espúria.

Exemples que poden aprofitar els anteriors avantatges són la implantació de sistemes de vot electrònic per garantir la confidencialitat i, alhora, el vot únic (Bamberger *et al*., 2021); presentar proves de vacunació (de Vasconcelos Barros; Schardong; Felipe Custódio, 2022); demostrar la possessió d'una targeta d'embarcament vàlida en un aeroport (Alamillo Domingo, I.; Valero Torrijos, J.; Fortune, D.; Martin, 2017) sense revelar la identitat, la construcció de sistemes d'identitat digital basats en cadenes de blocs (Hyperledger White Paper Working Group, 2018), o demostrar la inclusió o l'exclusió de certa informació en una base de dades (Ben-Sasson *et al*., 2018). Quant a això últim, podríem imaginar un sistema pel qual es pugui acreditar per part de l'Estat que determinat algorisme funciona d'acord amb la llei o reglament en què s'emmiralla, com ara la concessió d'ajudes públiques.

Tot i la seva versatilitat, dos elements clau limiten el desenvolupament d'aquests protocols. En primer lloc, cal estandarditzar la informació que s'ha de revelar sobre les dades i, en segon lloc, la informació que es vol acreditar s'ha de decidir d'antuvi. Aquests requisits tècnics mostren la dificultat d'implementar i d'entendre aquestes eines, ja que demanen un coneixement avançat en criptografia i una forta inversió econòmica per al seu desenvolupament (Bamberger *et al*., 2021).

Quant a les garanties addicionals que han d'acompanyar les ZKP, no són tècniques, sinó jurídiques. Formalment, les dades processades en la prova matemàtica són les mateixes que el valor d'entrada del protocol, per la qual cosa cal la presumpció que la prova matemàtica té el mateix valor que les dades originals abans de ser processades. De la mateixa manera, cal que els protocols i el format de les dades que s'han de tractar estiguin estandarditzats per tal de minimitzar els riscos d'error o de frau. No és estrany, doncs, que organismes d'estandardització com ISO/IEC 9798-5[6] hagin proposat el desenvolupament d'esquemes d'autenticació que incorporin aquests protocols per fer-los confiables.

6. ISO/IEC 9798-5:2009 Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge techniques https://www.iso.org/standard/50456.html

1.2. Cadenes de blocs

Les cadenes de blocs són un protocol de programari i un llibre de registre distribuït de transaccions, que pot actuar com a substrat computacional global per processar qualsevol tipus d'activitat digitalitzada (Swan, 2016). Jurídicament, en tractar-se de registres digitals, són per definició documents electrònics sota el Reglament eIDAS (Lyons, Courcelas i Timsit, 2019). Això vol dir que a la informació ancorada en les cadenes de blocs no se li pot denegar validesa jurídica pel simple fet de la seva naturalesa electrònica d'acord amb l'article 46 eIDAS.

Al seu torn, les cadenes de blocs són una aplicació de les anomenades tecnologies de registre distribuït (*distributed ledger technology*, DLT). La diferència és que DLT és un terme genèric que es refereix a qualsevol tecnologia que distribueix i sincronitza registres digitals entre múltiples nodes (ordinadors, servidors, telèfons intel·ligents, etc.), mentre que les cadenes de blocs són un tipus específic de DLT que utilitza una estructura de dades enllaçades criptogràficament i que funcionen a manera de registre de tracte successiu, on la informació només es pot anar afegint i queda vinculada a la darrera que s'ha incorporat (Ibáñez Jiménez, 2018); és el que es coneix com la immutabilitat de la cadena.

Al marge de la immutabilitat, hi ha dues propietats addicionals presents tant en les cadenes de blocs com en les DLT: la replicació per redundància de les dades entre tots els nodes i la transparència, la qual cosa implica que la informació ancorada és accessible sense restricció: qualsevol persona o dispositiu pot examinar les dades. Aquesta característica, clau per evitar el frau juntament amb la immutabilitat de les cadenes, és el que genera tensió amb el RGPD quant al principi de privacitat des del disseny i per defecte: article 25 RGPD, la minimització de dades, article 5 RGPD, i el dret de supressió, article 17 RGPD.

És en aquest escenari on es mostra la idoneïtat d'explorar l'ús de protocols ZKP per substituir les corresponents declaracions electròniques d'atributs per derivacions criptogràfiques que incrementin de manera efectiva la privacitat i redueixin els costos de compliment per als responsables del tractament. Així ho assenyalava Alamillo Domingo (2020, pàg. 129-130) en analitzar el règim jurídic aplicable en un esquema d'identitat digital descentralitzat amb suport en tecnologies de registre distribuït.

En l'àmbit europeu, les cadenes de blocs les treballa l'European Blockchain Services Infrastructure (EBSI), que és una iniciativa conjunta de la Comissió Europea i el Parlament Europeu per desenvolupar una xarxa de serveis que puguin millorar l'eficiència, la transparència i la confiança en els processos públics i privats.

1.3. Identitat digital sobirana

La identitat sobirana (*self-sovereign identity*, SSI) és un model de gestió d'identitat digital que neix dels entorns de cadenes de blocs, atès que aquestes permeten eliminar els intermediaris i actuar com a registres descentralitzats i immutables per disseny (Schwalm i Alamillo Domingo, 2021, pàg. 90). El principal postulat del moviment SSI és que els individus estiguin en possessió de les seves dades d'identitat i en conseqüència puguin escollir quines, amb qui, amb quina finalitat i durant quant de temps les comparteixen (Allen, 2016). Tot i això, els sistemes SSI no necessiten xarxes distribuïdes per a la seva construcció (Lyons, Courcelas i Timsit, 2019, pàg. 6).

El moviment SSI es presenta com una alternativa al model d'autenticació d'identitat federada o delegada en tercers, que al seu torn és el model més desplegat mundialment (Reed i Preukschat, 2021, pàg. 8). Aquests sistemes permeten que els usuaris emprin una sola identitat per accedir a múltiples recursos i serveis en diferents dominis o organitzacions. És el cas quan el registre en un lloc web es fa mitjançant el compte d'una xarxa social en lloc de crear-ne un de nou o s'empra un correu electrònic.

El model anterior presenta quatre inconvenients. El primer és que depèn d'un tercer que pot eliminar el compte si s'incompleix el contracte i fer perdre les dades dels serveis autenticats. El segon és que és vulnerable als atacs informàtics, ja que totes les dades estan en servidors centrals. El tercer inconvenient és que no és interoperable, perquè el proveïdor d'identitats estructura les dades segons el seu sistema. El quart és que permet el seguiment en línia, ja que el proveïdor d'identitats rep metadades cada vegada que s'accedeix a un recurs en línia. Com a resposta als models d'autenticació delegats sorgeix el model SSI, que a Europa es representa sota dues visions: una que adopta part dels seus postulats, l'anomenada identitat digital descentralitzada, i l'altra, que és la identitat sobirana.

La identitat descentralitzada, visió del Reglament eIDAS 2.0, fa referència a la introducció d'una cartera d'identitat digital, una aplicació mòbil amb una interfície gràfica que l'usuari pugui instal·lar-se en el dispositiu i amb la qual pugui interactuar (Schwalm i Alamillo Domingo, 2021). Aquesta aplicació és l'equivalent al servidor d'identitat, on l'usuari emmagatzema els documents declaratius de la seva identitat. El que es planteja és fugir d'una base de dades centralitzada i que cada usuari tingui els documents d'identitat sota el seu control. Aquest seria el cas del certificat COVID digital, on cada autoritat sanitària entregava a l'usuari les dades en relació amb la malaltia sense necessitat de connectar-se amb els servidors de l'autoritat sanitària per comprovar la validesa de les dades.

Per identitat sobirana (Allen, 2016) s'ha d'entendre la identitat en sentit ampli, més enllà del registre civil. Això vol dir que l'identificador, el compte d'usuari, no depèn de ningú més que d'ell. Per compte d'usuari ens referim a l'identificador base en qualsevol servei, que típicament serà un compte de correu electrònic; posteriorment, aquest compte es verificarà amb un telèfon, una signatura electrònica o per altres mitjans. Aquest identificador, en últim terme, no depèn de l'usuari i, per tant, pot ser eliminat pel prestador amb la pèrdua de les dades associades.

1.4. La proposta eIDAS 2.0

El Reglament eIDAS és una normativa de la Unió Europea que estableix un marc jurídic comú per a la identificació electrònica i els serveis de confiança en les transaccions electròniques. El seu objectiu és facilitar la interoperabilitat i la seguretat dels serveis digitals en el mercat únic europeu i fomentar la confiança dels ciutadans i de les empreses en l'ús de mitjans electrònics.

Així doncs, el Reglament eIDAS presenta dues parts molt diferenciades: una que té a veure amb els sistemes de gestió de la identitat transfronterers per garantir la interoperabilitat a tota la Unió i l'altra, els serveis de confiança. Els darrers són una col·lecció tancada de serveis públics que tracten una visió privatitzada de la prova electrònica: la signatura electrònica, el segell electrònic, el certificat digital, el registre electrònic i el lliurament electrònic certificat. Això explica per què els serveis de confiança tenen efectes jurídics fefaents i valor probatori, i, en conseqüència, que el règim jurídic de supervisió, de control i de contingut obligatori dels prestadors sigui estricte.

Ara bé, quant als sistemes d'identificació transfronterers, no hi ha cap obligació per part dels estats membre d'estendre'n els efectes fora del seu territori i, per extensió, de reconèixer els sistemes d'altres estats, la qual cosa implica un fre en la cohesió del mercat únic digital. Per aquesta raó, i amb motiu de la previsió continguda en l'article 49 del Reglament eIDAS, el 3 de juny de 2021 es va publicar la proposta de modificació eIDAS 2.0, que preveia la creació d'una cartera d'identitat digital europea a càrrec o per compte de l'Estat, l'EUDIW, i la infraestructura necessària per a la recopilació, emmagatzematge o divulgació de les dades d'identitat digital.

Altrament, el marc actual del Reglament eIDAS no cobreix la provisió d'atributs electrònics, com ara certificats mèdics o qualificacions professionals, la qual cosa dificulta garantir el reconeixement d'aquestes credencials en format electrònic en l'àmbit europeu.[7] Consegüentment, la proposta eIDAS 2.0 porta la inclusió d'un nou servei de confiança: les declaracions electròniques d'atributs. Aquestes són documents electrònics emesos i signats digitalment per una font de confiança, que es poden validar criptogràficament. Un exemple d'això és el certificat COVID digital, el QR del qual contenia la signatura de l'autoritat pública de salut corresponent.

A més a més, per respondre a la dinàmica dels mercats i a l'evolució tecnològica, la proposta amplia la llista vigent de serveis de confiança amb la prestació de serveis d'arxiu electrònic: els llibres majors electrònics. Aquests es plantegen com una combinació dels segells de temps de les dades i la seva seqüenciació, amb la certesa del creador de les dades, de manera similar a la signatura electrònica. Aquest servei de confiança es mostra com a element de suport per a la posada en comú de dades procedents de fonts descentralitzades per a solucions d'identitat descentralitzades i sobiranes.

És en aquest marc en què les ZKP s'interrelacionen amb els serveis de confiança ja existents, i els nous que la proposta eIDAS 2.0 introdueix per a la millora de la seguretat i privacitat, en permetre verificar la identitat o l'autenti-

7. Dicció literal de la proposta de modificació del Reglament eIDAS. Brussel·les, 3.6.2021 COM(2021) 281 final 2021/0136 (COD).

citat d'un document sense exposar dades sensibles, per exemple, demostrar que es té un certificat digital vàlid sense mostrar-lo, o per signar un document sense revelar el contingut d'aquest, tot això des de l'EUDIW, i a la vegada emprar els llibres majors electrònics per tal de disseminar el material criptogràfic i crear la prova. Sota aquesta visió, el febrer de 2023 la Comissió Europea va publicar la darrera esmena a la proposta de modificació del Reglament eIDAS, la qual preveu la incorporació de les ZKP com a suport a l'EUDIW i a les declaracions electròniques d'atributs.

Les proves de coneixement nul es defineixen en l'article 3 (5c) de l'esmena a la proposta de modificació com «aquells mètodes criptogràfics pels quals una tercera part pot validar que una declaració determinada, basada en una declaració electrònica d'atributs, que és en la cartera d'identitat digital europea de l'usuari, és vàlida, sense revelar al tercer cap dada relacionada amb aquella declaració electrònica d'atributs»; l'EUDIW es defineix com «un mitjà d'identificació electrònic que emmagatzema de manera segura, gestiona i valida dades relatives a la identitat i declaracions electròniques d'atributs per facilitar-les a terceres parts o a altres usuaris de l'EUDIW sota sol·licitud, i que permet la creació de signatures electròniques qualificades i segells», segons l'article 3 (42); les declaracions electròniques d'atributs es defineixen com «declaracions en format electrònic que permeten la presentació i l'autenticació d'atributs», segons l'article 3 (44).

D'altra banda, l'ús que es preveu de les ZKP és el que hi ha en l'article 6 bis 4 (6): «La cartera d'identitat digital europea haurà de facilitar, en particular, una interfície comuna per als seus usuaris o per a terceres parts, quan estigui disponible, per fer proves de coneixement nul a partir de les dades d'identificació personal o de les declaracions electròniques d'atributs». Fora de les anteriors previsions a la proposta consolidada de l'eIDAS 2.0, no es fa cap referència al seu règim jurídic, com tampoc no se'n fa a l'arquitectura i al marc tècnic de referència de la cartera europea d'identitat digital,[8] document adoptat pel grup d'experts eIDAS a finals de gener de 2023.

Les deficiències apuntades fins al moment –la manca de desenvolupament del règim jurídic i de la infraestructura tècnica de les proves de coneixement nul,– comporten un fre a la descentralització de la identitat digital pretesa per l'eIDAS 2.0 i a l'adopció de propostes com la del moviment d'identitat digital sobirana, les quals van més enllà del que planteja la proposta de modificació i que aquesta podria encloure.

1.5. El projecte Hyperledger Indy

El model Hyperledger Indy (Hyperledger White Paper Working Group, 2018) és un exemple de solució tecnològica d'identitat digital que, d'una banda, integra els principis del moviment SSI i, de l'altra, permet complir amb la proposta de modificació del Reglament eIDAS. Al seu torn, va un pas més enllà en les propietats que es desitgen per al nou sistema d'identitat digital europea en integrar en un mateix ecosistema una cartera d'identitat, les declaracions electròniques d'atributs sota la nomenclatura de credencials verificables, les tecnologies DLT i les proves de coneixement nul. La unió de tots aquests elements, interrelacionats amb el RGPD, aporten una visió de privacitat reforçada no prevista ni per la proposta eIDAS 2.0 ni per l'EBSI, visió que Hyperledger Indy integra en el seu sistema a partir de tres pilars tecnològics principals.

En primer lloc, les cadenes de blocs esdevenen el canal per transmetre la informació a internet sense que aquesta romangui sota el control o la custòdia d'una sola entitat. Així és com s'estableix la relació de confiança i es possibilita que la validació que fa el receptor tingui lloc sense la participació de l'emissor. D'aquesta manera es redueixen dos dels riscos dels sistemes actuals de delegació de l'autenticació d'identitats, entre els quals el node d'interoperabilitat eIDAS: la dependència d'un tercer per dur a terme la verificació i la traça de les metadades en els servidors del proveïdor d'identitats que es pugui emprar per a la creació de perfils de comportament.

En segon lloc, els identificadors descentralitzats, *decentralized identifier*, o DID (W3C, 2022a), permeten crear un identificador pseudònim ancorat a la xarxa sota l'exclusiu control de l'usuari i sense la dependència d'un registre centralitzat, proveïdor d'identitat o d'autoritat de certificació, a partir del qual es poden obtenir atributs d'identitat com ara una titulació universitària emesa directament a la cartera digital.

En tercer lloc, les credencials verificables, *verifiable credentials* o VC (W3C, 2022b), són documents electrònics que contenen una o més declaracions asseverades per

8. Versió 1.0.0 https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

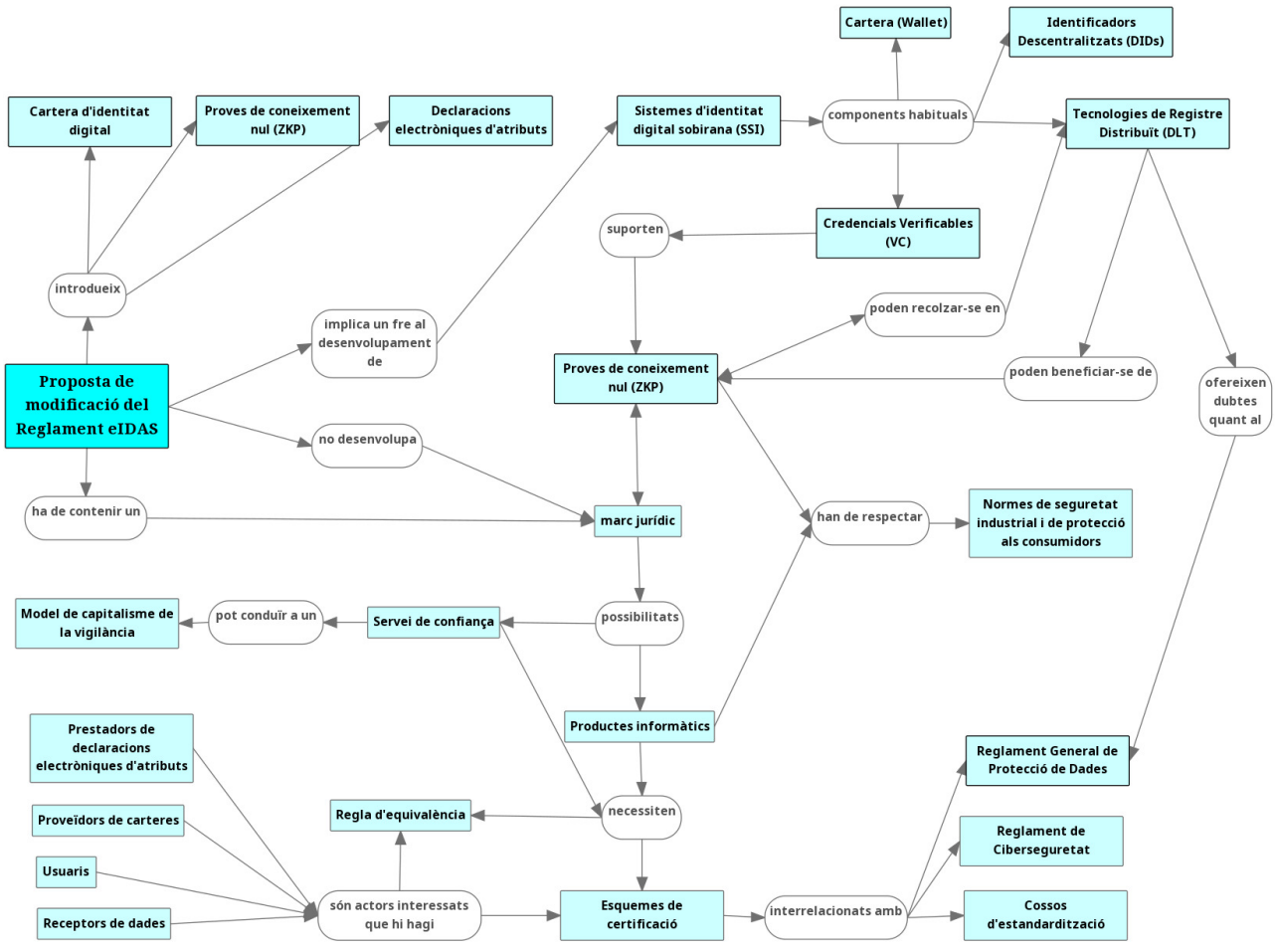
un emissor; en l'exemple anterior, seria el diploma acadèmic en format electrònic. En aquest cas d'ús, el Ministeri d'Universitats podria ser qui escrigués en una cadena de blocs quines universitats poden emetre títols.

Una característica de les credencials verificables, present en l'estàndard tècnic VC adoptat pel World Wide Web Consortium (W3C), i que incorpora Hyperledger Indy, és la seva emissió, control, gestió i compartició mitjançant proves de coneixement nul. Això permet combinar múltiples credencials de diversos emissors en una sola presentació verificable sense revelar la credencial o l'identificador, la possibilitat de mostrar de manera selectiva en una sola credencial atributs presents en diverses credencials, o bé crear una credencial verificable derivada d'acord amb el format establert per l'emissor, sense la necessitat de la seva participació una vegada emeses les credencials. Això últim permet que la prova de coneixement nul sigui susceptible d'ancorar-se en un registre distribuït, o bé només en el material criptogràfic generat per a la seva construcció.

2. El repte d'investigar el valor jurídic de les proves de coneixement nul

La proposta eIDAS 2.0 planteja dos reptes jurídics: regular les proves de coneixement nul i definir el seu paper com a suport per a les declaracions electròniques d'atributs i l'EUDIW. En la figura 1 es mostra un esquema amb la proposta eIDAS 2.0 i les proves de coneixement nul com a eixos principals. L'objectiu és establir el marc legal adequat per emprar protocols ZKP amb seguretat jurídica, la qual cosa ha de permetre el desenvolupament de nous sistemes d'identitat digital a la UE i facilitar la transició des de l'actual model on compartim dades fins a un model on es comparteixen proves de la seva existència.

Figura 1. Interacció de la proposta de modificació del Reglament eIDAS, els components d'identitat digital sobirana i les proves de coneixement nul



Font: elaboració pròpia

2.1. Règim de producte en front de règim de servei

El principal repte en l'anàlisi de les ZKP és determinar el marc regulador adequat per a aquests protocols. Un règim d'activitat en què només un proveïdor de serveis de confiança pugui emetre-les augmenta el risc de crear dependència en un prestador. Per tant, un pas inicial per definir el valor jurídic de les proves de coneixement nul és establir una regulació de producte que permeti a l'usuari generar aquestes proves.

Una altra qüestió és que l'elecció del tipus de prova de coneixement nul estigui imposada pel proveïdor de l'EUDIW, o que la declaració electrònica d'atributs només doni suport a un tipus de protocol criptogràfic. En aquests casos, la prova de coneixement nul quedarà absorbida per la regulació del servei sense perjudici de la responsabilitat del proveïdor, determinada per la seva elecció de la tecnologia. Tot i aquesta variable, el règim fonamental no canvia, que és la necessitat d'un règim que certifiqui la qualitat del producte mitjançant el control dels protocols criptogràfics que es fan servir per emetre la prova amb certificacions basades en la família de normes ISO 25000, relatives a la creació d'un marc de treball comú per avaluar la qualitat del producte programari.

2.2. Actors interessats

Aquest règim legal té impacte sobre el servei que doni l'Estat en l'emissió de l'EUDIW, però també pot passar que l'Estat no vulgui donar la funcionalitat de crear proves de coneixement nul. És així com prestadors de carteres no regulades i de declaracions electròniques d'atributs poden oferir en lliure concurrència competitiva aquest tipus de suport, però, en cas de no haver-hi un règim clar de producte, haurien de respondre del risc en la incorporació als seus serveis de proves de coneixement nul, o bé no donar aquest tipus de suport.

Així doncs, els proveïdors de carteres d'identitat digital i de declaracions electròniques d'atributs són actors interessats a definir un règim de producte, atès que per via d'elecció tecnològica, si és que decideixen incloure la funcionalitat d'emetre proves de coneixement nul o bé la seva escriptura en xarxes DLT, han de respondre per tal que criptogràficament el seu servei doni una seguretat mínima. Per això és important que els productes estiguin certificats, certificació que es pot plantejar, en el cas de la cartera, en relació amb les certificacions de ciberseguretat contingudes en la proposta eIDAS 2.0 i, en el cas de les declaracions electròniques d'atributs, vinculades a la utilització de sistemes i de productes fiables per part dels prestadors del servei de confiança.

2.3. Governança del model de certificació

Una certificació de producte amb avaluació criptogràfica ha d'estar en plena sintonia amb els cossos d'estandardització que es relacionen amb la proposta eIDAS 2.0 (ETSI, CEN i ISO), així com amb el reglament sobre ciberseguretat[9] i l'esquema de certificació de ciberseguretat candidat d'ENISA basat en criteris comuns, EUCC, perquè es pugui connectar posteriorment amb el RGPD i les certificacions en matèria de protecció de dades, d'acord amb el que disposen els articles 42 i 43 del RGPD. Només així estaria plenament justificada la intervenció pública per vetllar pel tràfic jurídic i garantir que el mercat únic no es fragmentarà, atesa la naturalesa de les proves de coneixement nul, on la confiança en la seva seguretat ha de descansar necessàriament en tota una sèrie de garanties i de controls previs per certificar que la tecnologia funciona correctament.

És amb aquest doble vessant, d'una banda una sòlida activitat reguladora per determinar les regles de control, fiabilitat i governança de les proves de coneixement nul, i de l'altra, el suport en instruments d'autoregulació de la indústria, que es pot assolir un marc de confiança amb les garanties adients per fomentar el seu ús entre tots els actors involucrats: Estat, prestadors de serveis, usuaris i receptors de proves de coneixement nul.

2.4. Determinació de regles d'equivalència

Definit el règim de producte i els mecanismes d'autoregulació, resta avaluar les implicacions per als receptors de les proves de coneixement nul. En última instància, són

9. Reglament (UE) 2019/881 del Parlament Europeu i del Consell, de 17 d'abril de 2019, relatiu a ENISA (Agència de la Unió Europea per a la Ciberseguretat) i a la certificació de la ciberseguretat de les tecnologies de la informació i la comunicació i pel qual es deroga el Reglament (UE) nº 526/2013 («Reglament sobre la Ciberseguretat»). *DOUE* núm. 151, de 7 de juny de 2019, pàg. 15-69 (55 pàg.). DOUE-L-2019-80998

els qui assumeixen un risc elevat en acceptar-les quan han de demostrar el compliment de les seves obligacions, com la d'identificar l'usuari a efectes de l'article 3 de la Llei 10/2010, de 28 d'abril, de prevenció de blanqueig de capitals i del finançament del terrorisme, o poder demostrar que s'està al corrent de les obligacions tributàries.

Amb l'objectiu de reforçar la protecció als receptors de les proves de coneixement nul, la clau de volta de tot el sistema és introduir en la proposta de modificació del Reglament eIDAS una regla d'equivalència substantiva, és a dir, l'equivalència entre l'efecte jurídic d'una credencial electrònica i la transformada criptogràficament en prova de coneixement nul, tal com proposaren Alamillo Domingo, I.; Valero Torrijos, J.; Fortune, D.; Martin (2017, pàg. 34). D'aquesta manera s'asseguren dos propòsits: primer, que la presentació de la dada en format ZKP mantingui la naturalesa de la credencial original perquè no pugui predicar-se'n una falsedat en document públic o privat (articles 392 i 395 CP); segon, que es pugui imposar l'obligació, en determinades circumstàncies, d'acceptar proves de coneixement nul o, en sentit negatiu, la prohibició de rebutjar proves de coneixement nul pel simple fet d'estar en aquest format o per estar recolzades en altres sistemes no regulats, com les DLT.

Totes aquestes regles del sistema han d'anar dirigides a construir un règim jurídic que permeti emprar proves de coneixement nul; consegüentment, tant la part de la proposta de l'eIDAS 2.0 relativa a l'EUDIW, com la del servei de confiança de declaracions electròniques d'atributs, han de tenir previsions normatives específiques a l'hora d'interrelacionar cadascun d'aquests objectes normatius, sense perjudici dels actes d'execució i de normalització tècnica que per raó de la seguretat i de l'interès públic pugui adoptar el legislador europeu.

Conclusions

La versió consolidada de la proposta eIDAS 2.0 aprovada el febrer de 2023 no conté un règim jurídic que permeti utilitzar proves de coneixement nul per a la construcció de sistemes d'identitat digital a la UE amb la garantia de la seva validesa, de tal manera que el receptor de les dades pugui acreditar el compliment de les seves obligacions legals davant de l'autoritat supervisora.

Per respondre a la problemàtica anterior, hem posat les bases per al desenvolupament d'un marc regulador recolzat per tres pilars: una regulació de producte informàtic que es pugui instal·lar a l'EUDIW o actuï de manera independent; la definició d'una regla d'equivalència funcional entre els efectes jurídics de la declaració electrònica d'atributs i les dades d'identificació de l'EUDIW amb la seva transformació a les ZKP, i la imposició d'acceptar l'ús de les ZKP en determinats escenaris que cal definir.

El règim que es desenvolupi facilitarà l'estímul de debats, com el paper que l'EBSI pot adoptar en el desplegament de solucions d'identitat digital sobirana basades en cadenes de blocs, o com les ZKP poden contribuir a la tensió que hi ha entre les cadenes de blocs i el RGPD. Al mateix temps, ha de participar a obrir noves perspectives sobre la direcció que han de prendre els sistemes d'identitat digital de la Unió Europea i el rol que els estats han d'assumir per no perdre la seva sobirania digital enfront del sector privat i equilibrar la seguretat pública, la privacitat dels usuaris i la liberalització del mercat.

Reconeixements

Aquest treball ha estat realitzat en el marc del programa de doctorat en Dret de la Universitat Autònoma de Barcelona.

Referències bibliogràfiques

AGÈNCIA ESPANYOLA DE PROTECCIÓ DE DADES (AEPD) (2020). «Cifrado y Privacidad IV: Pruebas de conocimiento cero» [en línia]. [Data de consulta: 26 febrer 2023]. Disponible a: https://www.aepd.es/es/prensa-y-comunicacion/blog/cifrado-privacidad-iv-pruebas-conocimiento-cero

AGÈNCIA EUROPEA DE CIBERSEGURETAT (ENISA) (2022). *Data protection engineering from theory to practice*. Publications Office of the European Union, 40 pàg. DOI: https://doi.org/10.2824/09079

ALAMILLO DOMINGO, I.; VALERO TORRIJOS, J.; FORTUNE, D.; MARTIN, D. (2017). «Legal requirements and analysis of ID legislation and law enforcement aspects». ARIES H2020 D2.3, 55 pàg [en línia]. Disponible a: https://www.aries-project.eu/content/legal-requirements-and-analysis-id-legislation-and-law-enforcement-aspects-0

ALAMILLO DOMINGO, I. (2020). *SSI eIDAS Legal Report*. Comissió Europea, 144 pàg. [en línia]. Disponible a: https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

ALLEN, C. (2016). «The Path to Self-Sovereign Identity». *Coin Desk* [en línia]. [Data de consulta: 23 maig 2023]. Disponible a: https://www.coindesk.com/path-self-sovereign-identity

BAMBERGER, K.A.; CANETTI, R.; GOLDWASSER, S.; WEXLER, R.; ZIMMERMAN, E. (2021). «Verification Dilemmas in Law and the Promise of Zero-Knowledge Proofs». *Berkeley Technology Law Journal*, vol. 37, núm. 1, 55 pàg. DOI: https://doi.org/10.2139/ssrn.3781082

BEN-SASSON, E.; BENTOV, I.; HORESH, Y.; RIABZEV, M. (2018). «Scalable, transparent, and post-quantum secure computational integrity». *Eprint.Iacr.Org*, 83 pàg., no. 693423, [en línia]. Disponible a: https://eprint.iacr.org/2018/046.pdf

BEN-SASSON, E.; CHIESA, A.; GARMAN, C.; GREEN, M.; MIERS, I.; TROMER, E.; VIRZA, M. (2014.) «Zerocash: Decentralized anonymous payments from bitcoin». *Proceedings - IEEE Symposium on Security and Privacy*, pàg. 459-474. DOI: https://doi.org/10.1109/SP.2014.36

DE VASCONCELOS BARROS, M.; SCHARDONG, F.; FELIPE CUSTÓDIO, R. (2022). «Leveraging Self-Sovereign Identity, Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass». *SSRN Electronic Journal*, vol. 5694, 10 pàg. DOI https://doi.org/10.2139/ssrn.4036226

GOLDWASSER, S.; MICALI, S.; RACKOFF, C. (1985). «Knowledge Complexity of Interactive Proof-Systems». *Conference Proceedings of the Annual ACM Symposium on Theory of Computing*, pàg 291-304. DOI https://doi.org/10.1145/22145.22178

HYPERLEDGER WHITE PAPER WORKING GROUP (2018). *An Introduction to Hyperledger. Hyperledger* [en línia]. [Data de consulta: 26 febrer 2023]. Disponible a: https://www.hyperledger.org/learn/white-papers

IBÁÑEZ JIMÉNEZ, J.W. (2018). *Blockchain: Primeras cuestiones en el ordenamiento español*. Dykinson, 1ª ed., 192 pàg. DOI: https://doi.org/10.2307/j.ctv346qc0

LYONS, T.; COURCELAS, L.; TIMSIT, K. (2019). «Blockchain and digital identity». *EU BLOCKCHAIN AND FORUM*, 27 pàg. [en línia]. Disponible a: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

REED, D.; PREUKSCHAT, A. (2021). *Self-Sovereign Identity*. Manning. 1ª ed., 465 pàg.

SCHWALM, S.; ALAMILLO DOMINGO, I. (2021). «Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0». *European Review of Digital Administration & Law - Erdal*, vol. 2, no. 2, pàg. 89-108. DOI: https://doi.org/10.53136/979125994752910

SWAN, M. (2016). «Blockchain Temporality: Smart Contract Time Specifiability with Blocktime BT - Rule Technologies. Research, Tools, and Applications». En: J.J. ALFERES, L. BERTOSSI, G. GOVERNATORI, P. FODOR i D. ROMAN (ed.). *Rule Technologies. Research, Tools, and Applications. RuleML 2016. Lecture Notes in Computer Science*, vol 9718. Cham: Springer International Publishing, pàg. 184-196. DOI: https://doi.org/10.1007/978-3-319-42019-6_12

W3C (2022a). «Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations». *W3C* [en línia]. [Data de consulta: 12 març 2023]. Disponible a: https://www.w3.org/TR/did-core/

W3C (2022b). «Verifiable Credentials Data Model v1.1». *W3C* [en línia]. [Data de consulta: 12 març 2023]. Disponible a: https://www.w3.org/TR/vc-data-model/.

Citació recomanada

RAMOS FERNÁNDEZ, Raül (2023). «A la recerca del règim jurídic de les proves de coneixement nul en la construcció de la identitat digital europea». *IDP. Revista de Internet, Derecho y Política*, núm. 38. UOC [Data de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i38.406131

Sobre l'autor

Raül Ramos Fernández
Universitat Autònoma de Barcelona
Departament de Dret Públic i Ciències Historicojurídiques
raulramos@icasbd.org
ORCID: https://orcid.org/0000-0001-7344-6140

Advocat de l'Il·lustre Col·legi de l'Advocacia de Sabadell. Graduat en Dret, màster universitari en Advocacia i doctorand en Dret per la Universitat Autònoma de Barcelona, i màster en *Blockchain i Smart Contracts* per la Universitat de Salamanca. Membre de la comissió de tecnologies de la informació i la comunicació de l'ICASBD, de l'àrea en Tecnologies en l'Advocacia del Consell de l'Advocacia Catalana i coordinador de la comissió de noves tecnologies de la Jove Advocacia de Catalunya. La seva línia d'investigació actual està centrada en l'anàlisi jurídica de les noves tecnologies aplicades a la identitat digital.