Zero Trust Architecture for Legal Entities

Erwin Nieuwlaar
Distributed Systems EEMCS
Delft University of Technology
nieuwlaar@gmail.com

***Abstract*—The European Commission is developing a European Digital Identity (EDI) with the revised eIDAS regulation as its legal framework. Currently, the internet does not have a trust anchor for legal entities, and therefore it is challenging to validate company representatives. The EDI commercial closed reference wallet implementation is expected to be delivered in 2023. Once the EDI is established, it will provide legal digital proof of identity and create a plethora of opportunities with respect to online trust. Accordingly, we provide a Zero Trust Architecture making trust portable by providing irrefutable proof of a natural person acting as a legal representative of a company. In conjunction with, an open standard with open-source reference implementation which is fully extendable to the forthcoming EDI. Our reference implementation focuses on creating a peer-to-peer Power-of-Attorney protocol while integrating the Member State Chamber of Commerce Company Register of the Netherlands to serve as the root of trust. This work achieves a rigorous system change regarding the currently outdated Powers of Attorney by providing a framework that enables portable trust which is cross-border, decentralized, verifiable, has revocation, and enables management of legal delegation of authority. Accomplishing a legally binding delegation in a matter of seconds instead of weeks. Our Zero Trust Architecture aims to change the way we represent and delegate legal entities, making trust portable.**

***Index Terms*—Power of Attorney, European Blockchain Services Infrastructure (EBSI), Decentralized Zero Trust Architecture, Self-Sovereign Identity, IPv8, Legal Entities**

I. Introduction

Citizens must be able to comprehend their digital world, select how they want to interact with it, and act autonomously. At the moment, this is not obvious in the digital realm, correspondingly making online trust a challenge. Although technology is getting simpler to use, it is becoming more difficult to comprehend precisely how it operates and how data, whether personal or not, is used. This may be ameliorated by *i.a.* reducing data-collecting. In order to reduce the current data economy, the European Union, and accordingly, the Dutch government is striving to develop an alternative [1]. With the Data Act [2] and the Data Governance Act [3], the European Commission is pushing a data economy in which users are controlling their data. Reducing the dependence on organizations that do not adhere to European principles. With the European Data Act, the European Union is developing standards for fair access to and use of non-personal data, including the right to access data and the ability to readily transfer data to other parties. The new Data Act addresses genuine rights to the access and use of personal data, opposing Big Tech control on online identity [4] and the associated induced privacy issues [5]. A new, more privacy-friendly method of processing data and identification, does not spontaneously appear. Therefore, European citizens will have the ability to possess a digital identity in order to securely identify themselves in the digital world and have control over their own data - similar to using a passport in the physical world [6]. These means of identification enable us to establish our identity. By using digital identification, we can streamline interactions and save time. Although the European Commission has not set a strict release date for the new EDI, the first toolbox draft has not been officially published but is circulating since October 2022 [7, 8]. The most innovative aspect of the new regulation with regard to the new European digital passport is that everyone will be entitled to an EDI Wallet that is recognized by all Member States. However, there will not be any obligation either. The EDI intends to provide universal access for individuals and organizations to safe and reliable electronic identity and authentication while using a mobile phone [9]. The design of the EDI Wallet has the ambition to fully adhere to the principles of a Self-Sovereign Identity wallet where users choose to disclose their personal information with online services, enabling people to digitally identify themselves, as well as store and manage identity data and official documents in an electronic format [10]–[12]. These may include a driver's license, a prescription, educational certification, or proof of authority to act on behalf of a company. The latter is the focus of this thesis. With the wallet, users will be able to access internet services, transfer digital documents, or simply confirm a certain personality trait, such as age, without disclosing their identity or other personal information by means of zero-knowledge proofs. Economically, successful integration could lead to a 3 to 13% increase of GDP by 2030 [13]. One of such potential integration is implementing the Company Register from the Netherlands Chamber of Commerce (CoC) in combination with the Netherlands Personal Records Database (PRD). These institutions serve as an anchor for legal certainty for Dutch persons and businesses. Binding these anchors where the PRD provides proof of identity and the CoC the proof of authorized officers of a company is practical. It enables interactions by a representative on behalf of a company without the need for trust in the representative if designed properly. In this work, we will provide this design and how these registries can generate portable trust for legal entity representation within a zero-trust architecture. Furthermore,

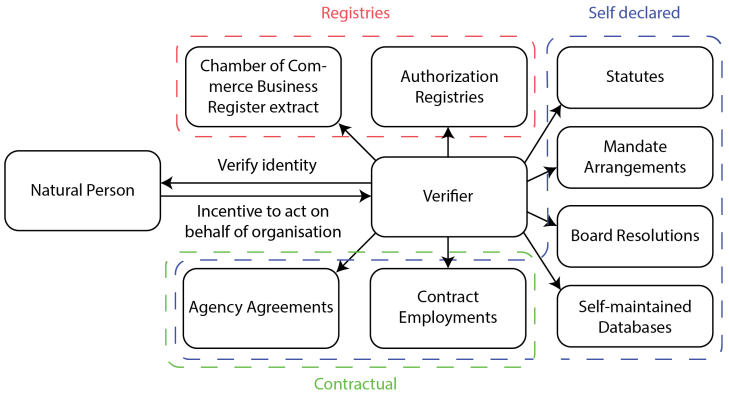

Fig. 1. Current situation of organization representation

we will show that this trust is well-founded, verifiable, profoundly portable, and widely applicable.

II. Problem Description

Presently, legal entity representation is done in various ways but does not adhere to the zero-trust architecture methodology [14], inflicting multiple problems specified further in this paragraph. With respect to demand, the Dutch government made eHerkenning mandatory for many entrepreneurs [15, 16] but is seeking alternatives [17], showing an insistence on PoA systems. At present, to transfer PoAs from a principal to an attorney-in-fact, the principal must create a PoA document that specifies the powers being granted and the scope of the attorney-in-fact's authority. The principal must then sign the document in the presence of witnesses or a notary public. The attorney-in-fact must accept the PoA and agree to act on behalf of the principal. Finally, the PoA document may need to be filed with the appropriate authorities to ensure that it is recorded[1] [20]. Examples of record-keeping are the PoA registry of Logius [21], eHerkenning [22], and the Business Registry of the Netherlands Chambers of Commerce [23]. These PoA registries have several benefits, such as increasing efficiency by including streamlined creation of PoA documents. Secondly, improved accessibility, through facilitating easy access and retrieval of PoA documents. Lastly, reducing the risk of disputes over authenticity or validity as these registers are considered authentic. Conversely, PoA registries come with numerous drawbacks. Namely, no cross-border interoperability, costly, publicly available, security concerns, and complexity. All previously mentioned PoA registries are barely implemented outside the borders of the Netherlands and registration is only available in the Netherlands. Furthermore, the PoA registries maintained by public companies are costly[2]. Further, the registries maintained by the private sector either do not include a PoA registry for legal entities (Logius' registry) or are publicly available (Business Registry of Netherlands Chamber of Commerce), raising privacy concerns. Additionally, the centralized nature of these registries imposes security vulnerabilities. Finally, the PoA document registration process is a cumbersome process that takes weeks. In this registration process, it is obligatory to be identified by a person or send a copy of your identification by post. Taken together, these drawbacks are responsible for the lack of trust in its portability. In our solution, we argue that we can make trust portable for legal entities by assuming the existence of the coming European Digital Identity and tackling each mentioned drawback by adhering to a decentralized zero trust architecture.

[1]Within legal entities it is almost never required to make a PoA document publically available [18]. However, exceptions do exist, such as the mandatory UBO registry in the Netherlands [19].

[2]The yearly price of eHerkenning level 3 (level 3 is required for using the PoA registry) is annually between 41 and 45 euros [24]. Creating or altering a PoA document is approximately 20 euros for each alteration [25].

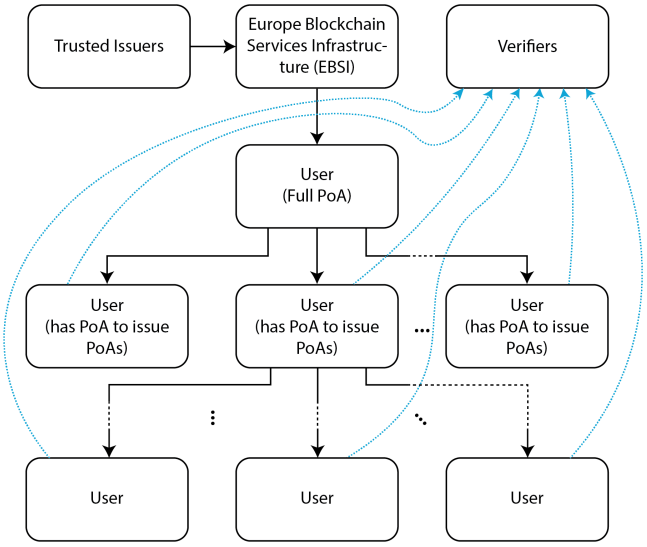

Fig. 2. System Architecture of the Zero Trust open standard for Legal Entities

III. System Architecture

This chapter examines the system architecture of our decentralized peer-to-peer PoA system. The system architecture is intended to be an open standard for European Union member states and the next chapter contains a reference open-source implementation to demonstrate the potential implications of this open standard and the including European Digital Identity.

In Figure 2, a visualization of the open standard system architecture is provided. This system consists of four main components: trusted issuers, the European Blockchain Services Infrastructure, users, and verifiers. The trusted issuers are responsible for placing verifiable credentials pertaining legal entities onto the European Blockchain Services Infrastructure. Thereafter, users are able to retrieve their PoA from EBSI, and if they do so directly, the PoA is considered a "full PoA". Users may also issue PoAs to other users provided their own PoA grants them the authority to do so, indicated by the black arrows. All users have the ability to present their PoA to a verifier, visualized by the blue arrows in Figure 2.

The whole chain from a trusted issuer to a verifier is called the zero trust chain, which we will prove as the irrefutable truth in Subsection III-E. Furthermore, all users may serve as a verifier if desired, as it is up to the presenter to accept the verifier. Contrarily, it is up to the verifier to specify their accepted PoA presentations. Each component in the system architecture will be described thoroughly below.

A. PoA

Subsequently, the representation by a natural person of a legal entity will be described as a type of Power of Attorney. A Power of Attorney (PoA) is a legal document that allows an individual or organization (the "principal") to appoint another person or organization (the "attorney-in-fact") to act on their or the companies' behalf. The attorney-in-fact is granted legal authority to make decisions and take actions on the principal's behalf, as specified in the PoA document. PoAs can be used for a variety of purposes, including financial matters, medical decisions, and legal affairs. The scope of the PoA is determined by the principal and can be as broad or narrow as they choose. In this work, all PoAs are limited to the boundaries of legal entities, and the person who is inherently authorized on behalf of a company (in the Netherlands this is the functionary enlisted in the Business Registry) is described to have full PoA over that company. There exists many similar interpretations of PoAs, e.g. delegation, mandate, authorization, and guardianship [26, 27]. The reason the term PoA is used in this work is because, firstly, delegation is used ambiguously and may not have legal effect [28, 29]. Secondly, mandating has an alternative definition in public law[3] and moreover the responsibility in our system should go with the attorney-in-fact, contrariwise to mandates. Thirdly, authorization is too vague and does not necessarily concern legal binding. Lastly, guardianship involves transferring power away from a person who is unable to make decisions for themselves [30], which is inapplicable in our system.

Regarding accountability, the attorney-in-fact is expected to use due diligence and good judgment in carrying out their duties. If they fail to fulfill their responsibilities or abuse their power, they may be held accountable for their actions [31] adhering to Zero Trust principles.

B. Trusted Issuers

In our Zero Trust system architecture, a trusted issuer is responsible for making the link between a natural person's identity and a legal person, such as a corporation or government agency. Correspondingly, trusted issuers play a critical role by providing the anchor of trust. The connection between an officer and the legal entity at which they operate is in most EU countries recorded at a chamber of commerce, commercial court, or ministry agency, [32] contains a complete list of such registries. These chambers, courts, and agencies are potential trusted issuers. Typically, trusted issuers only have a limited number of officers cataloged in their registry. For our architecture this is not an issue, provided that each legal entity has at least one, which is always the case.

C. European Blockchain Services Infrastructure

The European Blockchain Services Infrastructure is a network of blockchain nodes that aims to provide a secure, reliable, and scalable infrastructure for cross-border public services in all EU Member States, Norway, Liechtenstein, and Ukraine [33, 34]. The EBSI network is based on the Hyperledger Fabric platform and utilizes a permissioned consortium model [35] of which Delft University of Technology will maintain an operational node by the end of 2023. In our system, the EBSI will function as a distributed ledger for the input of trusted issuers. Trusted issuers are ought to register officers of legal entities in the EBSI. These registrations will become available on the EBSI in the W3C verifiable credentials format [36], achievable through the Trusted Issuer Registry API of EBSI [37]. The verifiable credential is a tailor-made credential available in EBSI's Trusted Schemas Registry [38]. In case a registration of an officer has to be revoked, this is made feasible by the Revocation and Endorsement Registry [39].

D. Users

As a user in our system, you will be required to complete an onboarding process[4] in pursuance of binding the EU Member States' Personal Record to the device used by the user. Correspondingly, the process involves identifying with an EU-recognized identification document such as a passport or ID card. The enrolment must meet the "high" Level of Assurance (LoA) proclaimed in the Architecture and Reference Framework[5] and outlined in the eIDAS regulation [41, 42]. The feasibility is a lively argument with respect to user's hardware concerns [43], privacy issues [44, 45], cross-border governmental distrust [46], and offline operability [47]. In the provided architecture we assume that personally identifiable data on LoA high is available. Nevertheless, this assumption is not strict, as the Zero Trust Architecture provided can still be operational with an already existing form of electronic identification. However, this will make the system more centralized and dependable on these services, e.g. MyGovID, SPID, FranceConnect and DigiD, altering the decentralized character of this work. Acquiring personally identifiable data on the LoA high in a decentralized manner has not yet been accomplished and is outside the scope of this research. Notwithstanding, the most obvious approach to achieving this is through linking the scanned identity document to the natural person and proving its integrity with biometrics [48, 49]. Once the personally identifiable data is

[3]Article 10:10 Awb

[4]Specified as "enrolment" in the eIDAS regulation [40]

[5]The official Architecture and Reference Framework has not been published yet. However, sequential draft versions include the following: *The mechanisms through which the PID is generated and provided to the EUDI Wallet are up to the Member State and are only constrained by legal requirements such as the requirements of LoA high, GDPR or any other national or union law*.

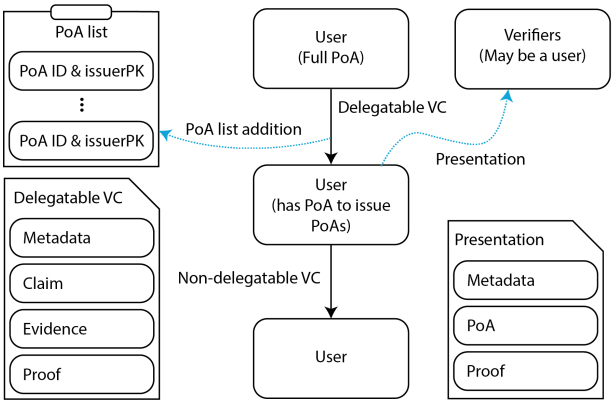

Fig. 3. Components of the Zero Trust Architecture

linked to the device of the user, the user can collect their link to a legal entity from the EBSI. Consequently, the user now possesses a digital proof of their identity and a proof of a full PoA of the legal entity they are an officer of. Combined, this empowers the user to act on behalf of the legal entity and the ability to issue PoAs to other users. Subsequently, a complete decentralized hierarchy of rights and obligations can be established, enabling any authorization connected to a legal entity anywhere at any time. While the users are in complete control of their own PoAs and their issued PoAs and are not required to trust one another. The system will contain branches and verifiable chains, which can be revoked or altered. Revocation is achieved by altering the Zero Knowledge PoA list of the corresponding legal entity. Transferring a whole branch of PoAs can be altered by the principal by modifying the PoA list with a signed message. Conclusively, the user will be able to provide a presentation of their PoA which a verifier can trust. Accordingly, enabling the user to irrefutably represent a legal entity where the user sees fit.

E. Verifiers

The presentation presented by a user can be verified by a verifier, and every user within the system can act as a verifier. However, a verifier can also be an entity outside the system which happen to accept presentation from our system. The format of a PoA is as delegatable verifiable credential which is added to the gossiped PoA list upon issuance [50]. The functionality of this list is to enable revocations and alterations of PoAs and its branches. Our Zero Trust Architecture system conjointly adheres to the Zero Knowledge Proof paradigm[6] [51]. Figure 3 provides more depth to the components within the Zero Trust Architecture.

[6]The only knowledge an adversary could obtain is the number of given PoAs corresponding to a public key.

IV. Evaluation

In this Chapter, we present the outcomes of implementing the Zero Trust Architecture for Legal Entities on top of Bambacht's Decentralized Societal Infrastructure [52]. The Decentralized Societal Infrastructure is a decentralized platform that is designed to provide identity, trust, money, and data services. It is made using the IPv8 protocol, which allows for post-quantum secure data sharing and communication among a network of peers [53]. In order to evaluate the performance and efficacy of this implementation in a real-world situation, we have augmented it with our own work. Our implementation enables us to evaluate the scalability and dependability of our system, in addition to identifying prospective use cases for the Zero Trust Architecture for Legal Entities.

A. European Blockchain Services Infrastructure

B. Trusted Issuer - Netherlands Chamber of Commerce

The implementation allows you to easily and securely verify your identity using your legal documents. Consecutively, the user is able to obtain their power of attorney from the Netherlands Chamber of Commerce. The requirement is that you are registered as an officer at that legal entity. This is achieved through connecting with the HR Dataservice from the Netherlands Chamber of Commerce. To receive a signed XML from which the officers of a legal entity can be deduced. In order to access this data, a fee for start-up costs of 1040 euros and 2.40 euros for each call is required[7] [54]. In our implementation the user interacts with a pre-production server of the HR Dataservice, switching to production is a matter of paying, adding the keys and adjusting one boolean [55]. Once successful, the user can issue PoAs to other users. Figure 4 visualizes how a root PoA can be obtained and verified by a verifier.

C. User

Figure 5 shows how a PoA is issued to another user.

V. Performance Analysis

[7]Expectation is that the price for each call will free of charge in the future.

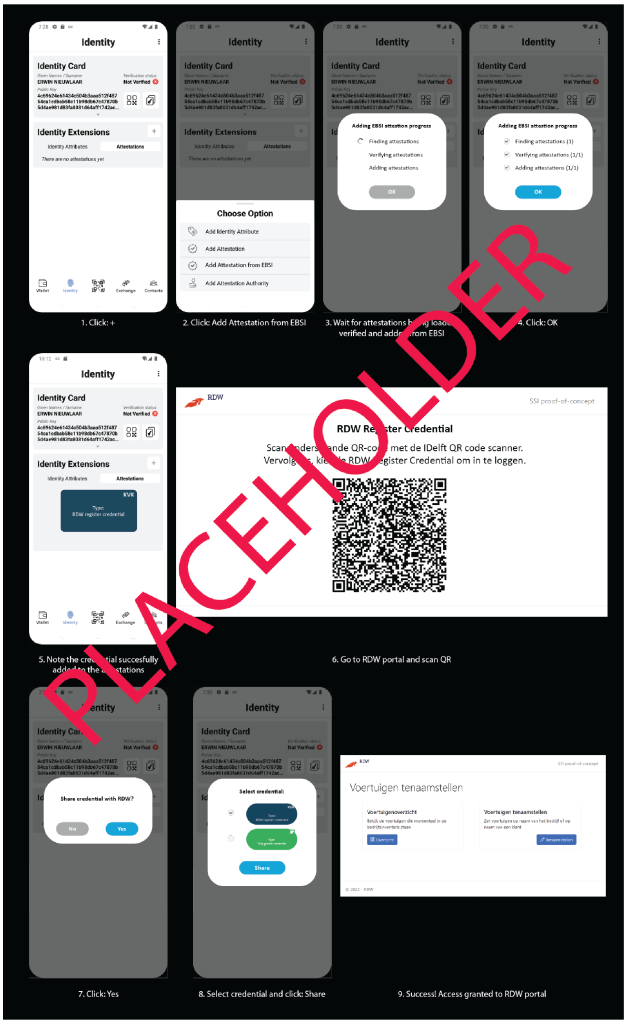

Fig. 4. Flow obtaining a Power of Attorney

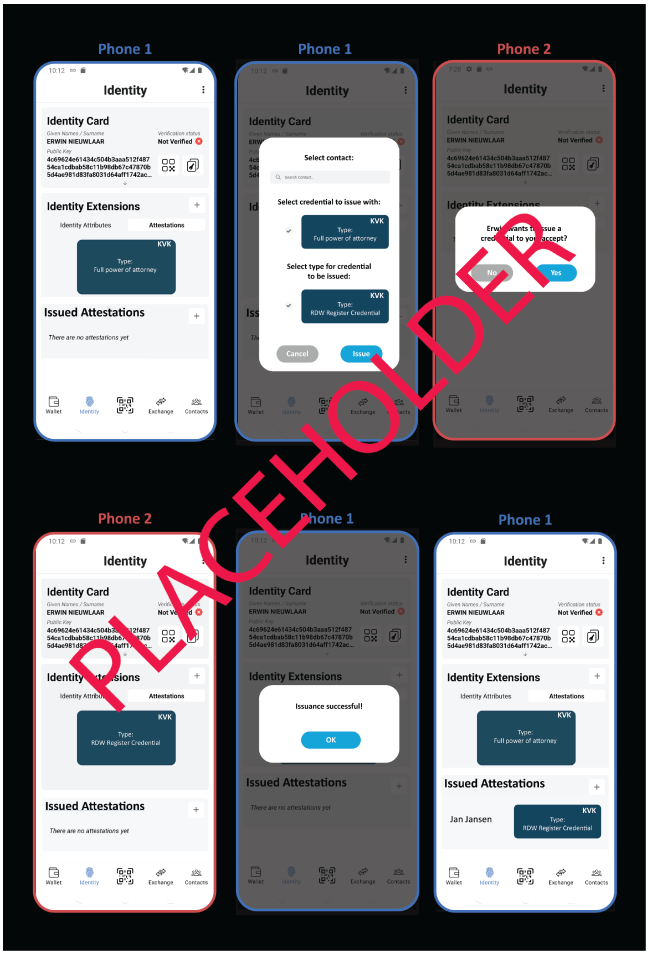

Fig. 5. Issuance of a Power of Attorney

REFERENCES

[1] A. van Huffelen, M. Adriaansens, and D. Yeşilgöz-Zegerius, "Kamerbrief hoofdlijnen beleid voor digitalisering." [Online]. Available: https://www.rijksoverheid.nl/documenten/kamerstukken/2022/03/08/-kamerbrief-hoofdlijnen-beleid-voor-digitalisering

[2] Feb 2022. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

[3] Nov 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[4] V. Mokshagundam, "Top social login tools compared," Jan 2017. [Online]. Available: https://medium.com/@Vamshi_Mokshagundam/top-social-login-tools-compared-b350eae26118

[5] O. Tene and J. Polonetsky, "Big data for all: Privacy and user control in the age of analytics," Apr 2013. [Online]. Available: https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/

[6] U. Leyen, "State of the union address by president von der leyen at the european parliament plenary," Sep 2020. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

[7] eIDAS Expert Group, "The toolbox process," 2021. [Online]. Available: https://webgate.ec.europa.eu/regdel/web/meetings/2409/documents/6690

[8] "The eudi wallet architecture & reference framework," https://www.gataca.io, may 18 2022, [Online; accessed 2023-01-26].

[9] D. Mammonas, "European digital identity (eID): Council makes headway towards EU digital wallet, a paradigm shift for digital identity in Europe," https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/, dec 6 2022, [Online; accessed 2023-01-26].

[10] P. Mart, "Is the EU Digital Identity Wallet an Implementation of Self-Sovereign Identity?" https://thepaypers.com/expert-opinion/is-the-eu-digital-identity-wallet-an-implementation-of-self-sovereign-identity–1257448, jul 13 2022, [Online; accessed 2023-01-26].

[11] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *The Sovrin Foundation*, vol. 29, no. 2016, p. 18, 2016.

[12] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013718301217

[13] D. Mahajan, O. Sperling, and O. White, "Digital id: The opportunities and the risks — mckinsey & company." [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/digital-id-the-opportunities-and-the-risks

[14] J. Kindervag *et al.*, "Build security into your network's dna: The zero trust network architecture," *Forrester Research Inc*, vol. 27, 2010.

[15] Jun 2022. [Online]. Available: https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:PHR:2022:553

[16] [Online]. Available: https://www.belastingdienst.nl/wps/wcm/connect/nl/ondernemers/werkt-eherkenning

[17] M. Van Rij, "Antwoordidsinga," Jul 2022. [Online]. Available: https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2022D33247&did=

[18] R. Kulas., "Must a power of attorney be registered or recorded?" Apr 2011. [Online]. Available: https://www.kulaslaw.com/power-attorney-registered-recorded/

[19] [Online]. Available: https://www.kvk.nl/inschrijven-en-wijzigen/ubo-opgave/

[20] S. Ryall, "Registeringapowerofattorney," Jun 2016. [Online]. Available: https://justuslaw.com/powers-attorney-implications-registration/

[21] Jul 2020. [Online]. Available: https://www.logius.nl/domeinen/toegang/machtigingenregister

[22] [Online]. Available: https://eherkenning.nl/nl/eherkenning-gebruiken/machtigen

[23] [Online]. Available: https://www.kvk.nl/english/registration/who-is-authorised-to-sign/

[24] [Online]. Available: https://eherkenning.nl/nl/leveranciersoverzicht

[25] Bram, "Ketenmachtiging bij eherkenning » digidienst," Oct 2019. [Online]. Available: https://www.digidienst.nl/ketenmachtiging-bij-eherkenning/

[26] A. Abdullah, S. den Breeijen, K. Cooper, M. Corning, O. Coutts, R. Cranston, H. Dahl, D. Hardman, N. Hickman, N. Neubauer, D. O'Donnell, P. Page, J. Phillips, D. Reed, C. Raczkowski, P. Simpson, J. Stirling, and S. Warner, "On guardianship in self-sovereign identity," *Sovrin Guardianship Task Force*, pp. 1–33, 11 2019.

[27] J. Moye, K. Stolzmann, E. J. Auguste, A. B. Cohen, C. C. Catlin, Z. S. Sager, R. E. Weiskittle, C. B. Woolverton, H. L. Connors, and J. L. Sullivan, "End-of-life care for persons under guardianship," *Journal of Pain and Symptom Management*, vol. 62, no. 1, pp. 81–90.e2, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0885392420308721

[28] B. G. ALI POULADI, JAHANBAKHSH GHOLAMI, "Delegation of power of attorney and identification of related legal works," *Journal of Contemporary Issues in Business and Government*, vol. 27, no. 2, pp. 1388–1390, 2021.

[29] J. Lamb-Ruiz, "Apoderamiento: "power of attorney" vs "delegation of authority"," https://www.proz.com/kudoz/spanish-to-english/law-contracts/702330-apoderamiento-%22power-of-attorney%22-vs-%22delegation-of-authority%22.html, [Online; accessed 2023-01-04].

[30] A. B. A. C. on Law, A. P. Association, and N. C. of Probate Judges (US), "Judicial determination of capacity of older adults in guardianship proceedings," in *Judicial determination of capacity of older adults in guardianship proceedings*. American Bar Association, 2006.

[31] M. Goetting, "Power of attorney," *Revised Mar*, 2013.

[32] "European business registers," https://www.kvk.nl/english/about-the-netherlands-chamber-of-commerce/foreign-registers-overview/european-business-registers/, [Online; accessed 2023-01-03].

[33] "ukraineebsi," https://thedigital.gov.ua/news/ukraina-priednalasya-do-evropeyskogo-blokcheyn-partnerstva-v-statusi-sposterigacha-1, jun 17 2022, [Online; accessed 2023-01-03].

[34] "Europeancountriesjoinblockchainpartnership," https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership, apr 10 2018, [Online; accessed 2023-01-03].

[35] M. Turkanović and B. Podgorelec, "Signing blockchain transactions using qualified certificates," *IEEE Internet Computing*, vol. PP, pp. 1–1, 09 2020.

[36] "Verifiable Credentials Data Model v1.1," https://www.w3.org/TR/vc-data-model/, mar 3 2022, [Online; accessed 2023-01-03].

[37] "Trusted Issuers Registry API v3 | EBSI developers hub," https://api-pilot.ebsi.eu/docs/apis/trusted-issuers-registry/latest, [Online; accessed 2023-01-03].

[38] "Trusted Schemas Registry API v2 | EBSI developers hub," https://api-pilot.ebsi.eu/docs/apis/trusted-schemas-registry/latest, [Online; accessed 2023-01-03].

[39] "Education Verifiable Accreditation Records - EBSI Specifications -," https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Education+Verifiable+Accreditation+Records, [Online; accessed 2023-01-03].

[40] The European Parliament and the Council of the European Union , "Regulation (eu) no 910/2014 of the european parliament and of the council," 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

[41] The European Commission, "The common union toolboxb for a coordinated approach towards a european digital identity framework - the architecture and reference framework," December 2022, 0.1.2 Draft Version.

[42] ——, "Article 8(3) of regulation (eu) no 910/2014 of the european parliament and of the council on electronic identification and trust services for electronic transactions in the internal market," 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=-CELEX:32015R1502&from=ES.

[43] E. Verheul, "Secdsa: Mobile signing and authentication under classical "sole control"," Cryptology ePrint Archive, Paper 2021/910, 2021, https://eprint.iacr.org/2021/910. [Online]. Available: https://eprint.iacr.org/2021/910

[44] M. Walsh, "The challenges facing the EU's new digital identitysystem - Raconteur," https://www.raconteur.net/technology/problems-identified-for-new-eu-digital-identity-wallet/, nov 7 2022, [Online; accessed 2023-01-05].

[45] J.-H. Hoepman, "Civil liberties aspects of the European Digital Identity Framework." https://blog.xot.nl/2022/01/31/civil-liberties-aspects-of-the-european-digital-identity-framework/index.html, jan 31 2022, [Online; accessed 2023-01-05].

[46] J.-S. ARRIGHI, J.-T. BATTESTINI, L. COATLEVEN, F. HUBLET, S. MARINI, and V. QUEUDET, "The Scale of Trust: Local, Regional, National and European Politics in Perspective - Groupe d'études géopolitiques," https://geopolitique.eu/en/2022/07/13/the-scale-of-trust-local-regional-national-and-european-politics-in-perspective/, 7 2022, [Online; accessed 2023-01-05].

[47] D. Mekinec, "Offline face recognition: why use it? - Visage Technologies," https://visagetechnologies.com/offline-face-recognition/, aug 12 2022, [Online; accessed 2023-01-05].

[48] A. Traichuk, "6 Best Open-Source Projects for Real-Time Face Recognition | HackerNoon," https://hackernoon.com/6-best-open-source-projects-for-real-time-face-recognition-vr1w34x5, apr 28 2021, [Online; accessed 2023-01-05].

[49] O. B. Maestro, "Biometrics in Identity," https://dis-blog.thalesgroup.com/identity-biometric-solutions/2022/10/27/biometrics-in-identity/, oct 27 2022, [Online; accessed 2023-01-05].

[50] J. Camenisch, M. Drijvers, and M. Dubovitskaya, "Practical uc-secure delegatable credentials with attributes and their application to blockchain," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 683–699. [Online]. Available: https://doi.org/10.1145/3133956.3134025

[51] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof-systems," in *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, ser. STOC '85. New York, NY, USA: Association for Computing Machinery, 1985, p. 291–304. [Online]. Available: https://doi.org/10.1145/22145.22178

[52] J. Bambacht, "Web3: A decentralized societal infrastructure for identity, trust, money, and data," https://repository.tudelft.nl/islandora/object/uuid%3A3ad68dbd-3444-4e01-94a2-d28044b0ba3f, feb 28 2022, [Online; accessed 2023-01-08].

[53] Tribler, "Ipv8 documentation," 2022. [Online]. Available: https://py-ipv8.readthedocs.io/_/downloads/en/latest/pdf/

[54] "Hoe bepalen wij onze tarieven?" https://www.kvk.nl/over-kvk/over-het-handelsregister/tarieven/, [Online; accessed 2023-01-08].

[55] M. Mayer, "Handleiding kvk bevoegdheden," https://bevoegdheden.mayersoftwaredevelopment.nl/, [Online; accessed 2023-01-08].