Zero Trust Architecture for Legal Entities

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

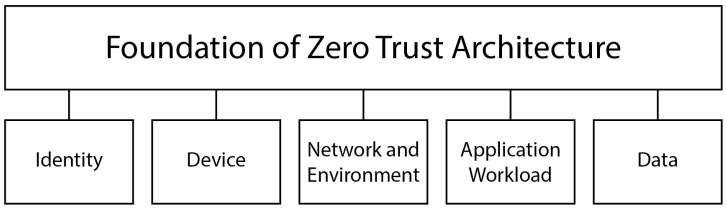


Fig. 1. Foundation of Zero Trust Architecture

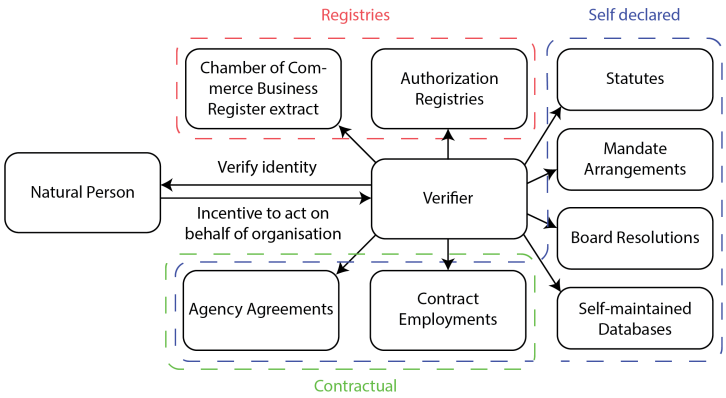


Fig. 2. Current situation of organization representation

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

I. Introduction

Figure 1 in introduction

II. Problem Description

Figure 2 in problem description

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.

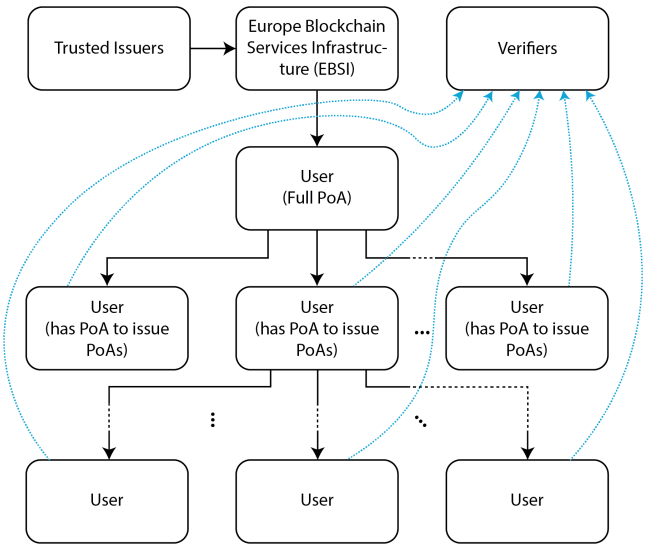


Fig. 3. System Architecture of the Zero Trust open standard for Legal Entities

In Figure 3, 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 3. 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. Power of Attorney

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 [1, 2]. The reason the term PoA is used in this work is because, firstly, delegation is used ambiguously and may not have legal effect [3, 4]. Secondly, mandating has an alternative definition in public law[1] 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 [5], 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 [6].

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, [7] 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.

[1] Article 10:10 Awb

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 [8, 9]. The EBSI network is based on the Hyperledger Fabric platform and utilizes a permissioned consortium model [10] 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 [11], achievable through the Trusted Issuer Registry API of EBSI [12]. The verifiable credential is a tailor-made credential available in EBSI's Trusted Schemas Registry [13]. In case a registration of an officer has to be revoked, this is made feasible by the Revocation and Endorsement Registry [14].

D. Users

As a user in our system, you will be required to complete an onboarding process[2] 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[3] and outlined in the eIDAS regulation [16, 17]. The feasibility is a lively argument with respect to user's hardware concerns [18], privacy issues [19, 20], cross-border governmental distrust [21], and offline operability [22]. 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

[2] Specified as "enrolment" in the eIDAS regulation [15]

[3] 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.*

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 [23, 24]. Once the personally identifiable data is 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 [25]. 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[4] [26]. Figure 4 provides more depth to the components within the Zero Trust Architecture.

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 [27] further called the IDknip. This Decentralized Societal Infrastructure is a decentralized platform that is designed to provide identity, trust, money, and data services. The IDknip receives the identity by scanning a person's identity card or passport. The devices in the system are operating on Android OS (BRON). The network used is the internet by IPv8 protocol, which allows for post-quantum secure data sharing and communication among a network of peers [28]. 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.

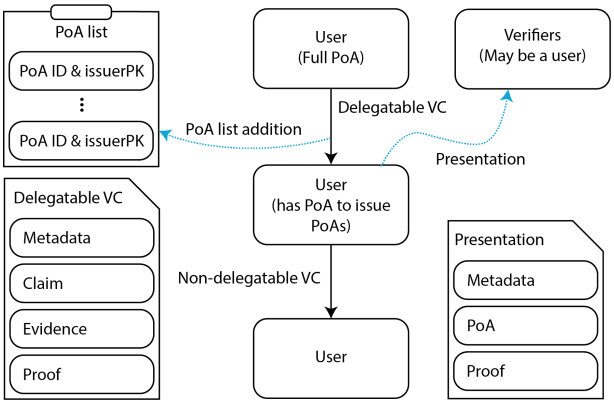


Fig. 4. Components of the Zero Trust Architecture

A. European Blockchain Services Infrastructure

As shown in Figure 3, the Trusted Issuers are ought to put credentials of owners or officers of a legal entity in the EBSI. Implementing the EBSI in a wallet is a burden, there currently exist some wallets that are operational with the EBSI blockchain. However, most of these wallets depend on the open-source work of Walt-ID. In this work we did not implement the integration with EBSI in our wallet, but we made a prototype of how trusted issuers should import their accreditations onto the EBSI. Accordingly, the PoA credentials are directly obtained from the Netherlands Chamber of Commerce Company Registry pre-production server. To enable trusted issuers to enlist their accreditations, a verifiable credential schema should be created in the Trusted Schemas Registry. This schema contains all the information to issue a PoA to the officer of the affiliated company. In Listing

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

1 is presented how the schema should look like. For trusted verifiers to put these verifiable credentials in the EBSI, they should be in the Trusted Issuers Registry. Once the trusted verifier is in this registry, the verifier can put in all the company officers. Accordingly, the user will be able to retrieve the PoA from EBSI by identifying theirself.

Listing 1. EBSI Power of Attorney Verifiable Credential

```
{
  <credential-metadata>,
  "credentialSubject": {
    "id": "did:ebsi:bef...k21",
    "powerOfAttorney": {
      "id": "did:ebsi:c27...9f1",
      "nameIssuer": "Chamber of Commerce NL",
      "idIssuer": "59581883",
      "type": "root",
      "nameLegalEntity": "Nieuwlaar Design",
      "idLegalEntityHolder": "70123101",
      "publicKeyHolder": "4c6..c60",
      "givenNamesHolder": "Erwin",
      "surnameHolder": "Nieuwlaar",
      "dateOfBirthHolder": "23-05-1994"
    },
    <powerOfAttorney-evidence>
  },
  <credential-proof>
}
```

As seen from the listing, the verifiable credential consists of three parts, namely, the credential metadata, the PoA data, and the proof of the credential. The metadata and proofs are left out for overview and because the verifiable credentials simply follow the w3c format.

B. Trusted Issuer - Netherlands Chamber of Commerce

The implementation allows you to easily and securely verify your identity using your legal documents *i.e.* European passport or identity card. Consecutively, the user is able to obtain their PoA 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[5] [29]. 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 [30]. Once successful, the user can issue PoAs to other users. Figure 5 visualizes how a root PoA can be obtained and verified by a verifier.

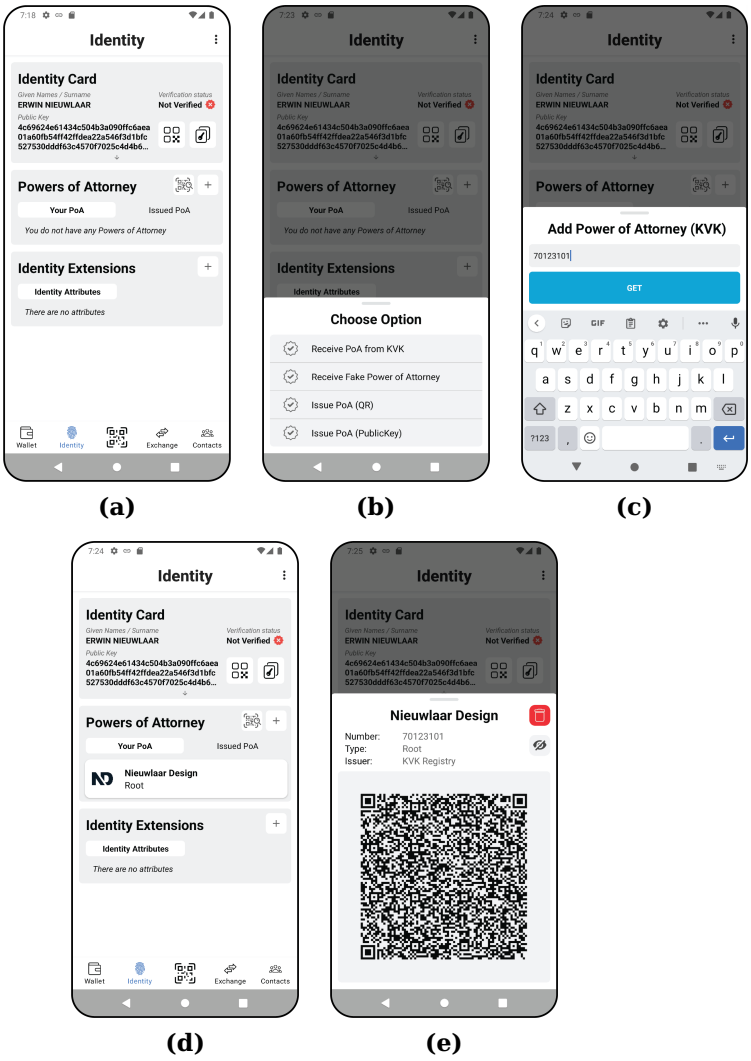


Fig. 5. Flow of obtaining Power of Attorney from the Netherlands Chamber of Commerce. **(a)** Identity fragment of the IDknip application. **(b)** Add PoA menu. **(c)** Adding PoA dialog from the Netherlands Chamber of Commerce. **(d)** Overview of the identity fragment with a root PoA obtained from the Netherlands Chamber of Commerce. **(e)** The detailed dialog of the PoA with a verifiable QR, the option to delete the PoA, and general information of the PoA.

In Figure 5a the identity fragment is shown of the IDknip, from here the user can click the "+" sign to obtain or issue PoAs. Once clicked, the dialog 5b will show. To receive a PoA from the Netherlands Chamber of Commerce the option "Receive PoA from KVK" is chosen. Accordingly, the dialog of Figure 5c will show, where the user can fill in the Chamber of Commerce number of which the user is a registered officer in the Company Registry of the Netherlands Chamber

[5]The price for each call will be free of charge in 2025.

of Commerce of that legal entity. Once filled and clicked upon "GET", a request with the given name, surname, birthday, and the filled legal entity number is sent to the pre-production server of the Chamber of Commerce data service. Accordingly, the Chamber of Commerce verifies if the provided legal entity indeed has a registered officer matching the given name, surname, and birthday provided by the identity of the user. When a match is found, the user will receive the PoA as can be seen in 5d. The user can click the PoA to view the detailed presentation of the PoA as shown in 5e. The detailed presentation contains general information about the PoA, the possibility to revoke or delete the PoA, and a verifiable QR code.

C. User

Once a user in a legal entity has obtained the PoA from the Netherlands Chamber of Commerce, the user is able to delegate PoAs and create a structure of authorizations. Figure 6 shows how a PoA is issued peer-to-peer from one user to another. Firstly, the user who has permission to issue PoAs will select "Issue PoA (QR)" or "Issue PoA (PublicKey)" from 5b. Once the public key is obtained successfully, the principal should choose the PoA with which they would like to issue the PoA with. Furthermore, the principal has to select the PoA it wishes to issue. The dialog to accomplish this is presented in Figure 6a. Once the PoA request is sent, the potential attorney-in-fact will receive a notification to either accept or deny the PoA as shown in Figure 6b. When the attorney-in-fact accepts the PoA, the principal will receive the issuance response shown in Figure 6c. Accordingly, the principal can view its issued PoAs from the identity fragment in the issued PoA tab as presented in Figure 6d. Lastly, the attorney-in-fact now has the authorization to purchase at wholesale as shown in Figure 6e.

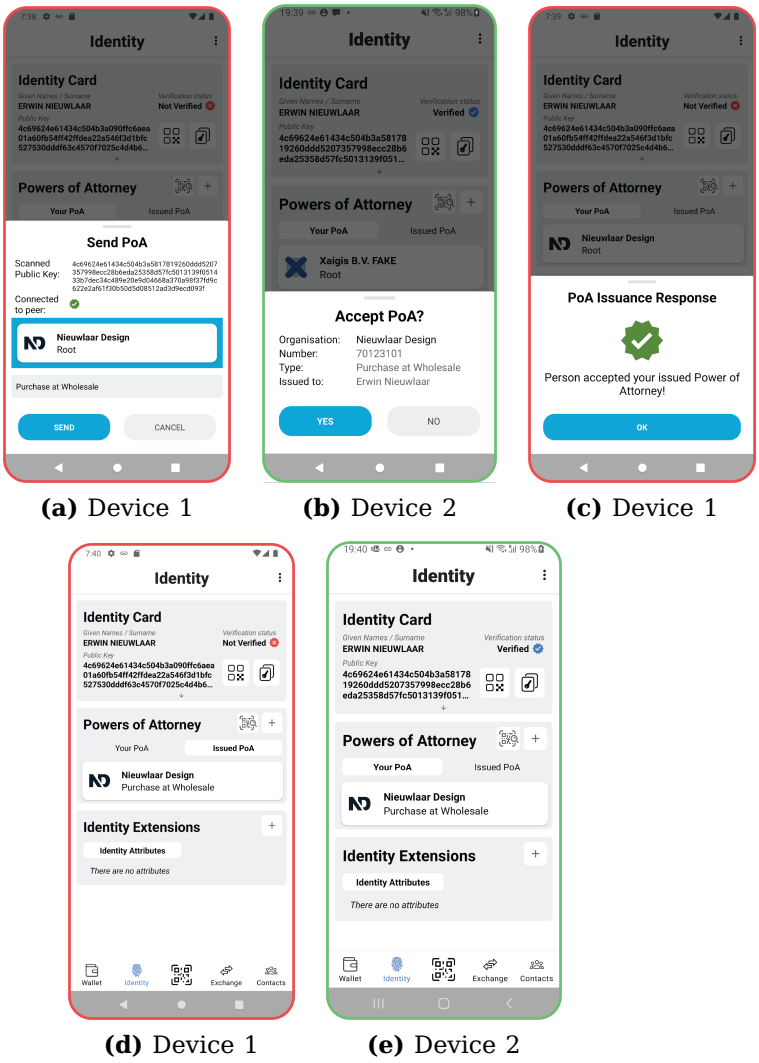
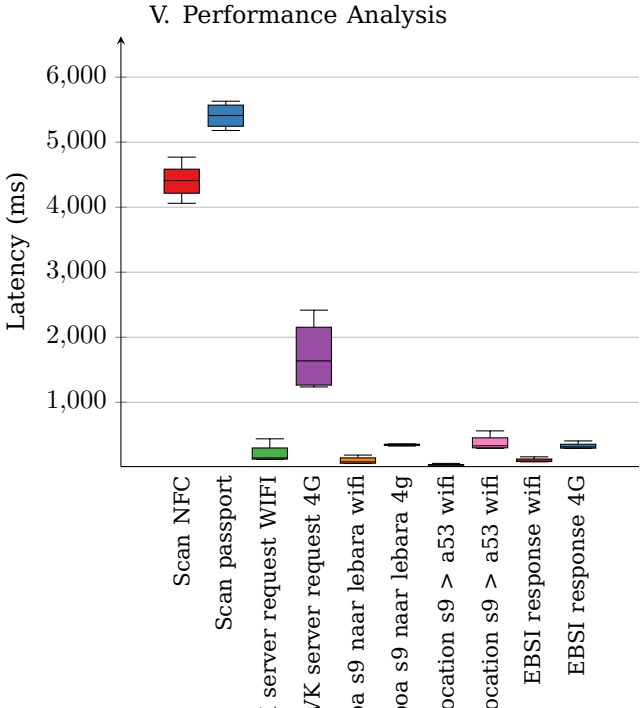


Fig. 6. Peer-to-peer issuance of a Power of Attorney. **(a)** Dialog to choose PoA to issue with and the PoA desired to be issued. **(b)** Dialog to accept receiving PoA. **(c)** Response of sent PoA. **(d)** Issued PoAs of device 1. **(e)** Received PoAs of device 2.

D. Verifier

V. Performance Analysis



VI. Discussion

VII. Conclusion

VIII. Future Work

Future research can focus on several areas to improve the ideas and implementation provided in this thesis. Firstly, additional research can fulify complete implementation of EBSI within the IDknip, which would enable secure and transparent cross-border transactions, digital identity verification, and trusted authorization among the European Member states. Secondly, researchers can work on further refining assumptions related to the identification process of eIDAS with respect to the assurance level high, including the use of mobile technology to enhance the security and privacy of personal data (BRON onderzoek eindhoven/nijmegen, zie TNO). Thirdly, an alternative method for revocation can be developed to improve the efficiency of the revocation process and reduce message and storage complexity. Fourthly, the IDknip could be integrated with TU Delft's TrustChain, a blockchain-based system for verifying the integrity of digital data. Fifthly, exploring cross-community implementation could ensure that the IDknip can be used effectively across various communities in the IPv8 protocol enhancing scalability. Sixthly, finding ways to minimize the amount of information included in the PoA list, without compromising its integrity, can improve the Zero Knowledge methodology and the security of personal data. Seventhly, research can work on developing more information privacy in the light of delegatable Verifiable Credentials (BRONNEN). Finally, maximizing the roundification of the zero-trust architecture, where data is always encrypted, can help enhance the security and privacy of the system. Researchers can look to the CISA Zero Trust Maturity Model for guidance on how to achieve this (CISA bron).

References

[1] 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.

[2] 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

[3] 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.

[4] 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].

[5] 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.

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

[7] "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].

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

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

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

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

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

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

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

[15] 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

[16] 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.

[17] ——, "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.

[18] 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

[19] 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].

[20] 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].

[21] 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].

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

[23] 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].

[24] 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].

[25] 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

[26] 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

[27] 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].

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

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

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