Zero-Trust Architecture for Legal Entities

Erwin Nieuwlaar

26-04-2023

Delft University of Technology

Faculty of Electrical Engineering, Mathematics Computer Science
Distributed Systems Group

Thesis committee: dr. ir. J.A. Pouwelse
dr. ir. C. Lofi
dr. J. Ubacht

To obtain the degree of Master of Science
at the Delft University of Technology
to be defended publicly on 26-04-2023 at 13:30.

Zero-Trust Architecture for Legal Entities

Erwin Nieuwlaar
Distributed Systems EEMCS
Delft University of Technology

***Abstract*—The European Commission is developing a European Digital Identity (EDI), which will enable a trustworthy digital proof of identity for its citizens. We present a proof of identity in combination with cryptographic evidence of the natural person being authorized to act on behalf of a legal entity. Our study achieves this by connecting users of our system with trusted issuers, the European Blockchain Services Infrastructure (EBSI), and verifiers. Accordingly, we provide a zero-trust architecture for legal entity representation, making trust portable by providing irrefutable proof of a natural person acting as a legal representative of an organization. Our zero-trust architecture aims to change how we represent legal entities and delegate authorizations with powers of attorney (PoA) as a legal primitive, making trust portable and secure. With government assistance, we conducted a pilot deployment of our prototype with live connectivity to the legal source of truth, the Kamer van Koophandel (KVK). In our pilot, a commercial business-only retailer acted as the verifier of the PoA. We shorten legally binding delegation that is cross-border, decentralized, verifiable, and revokable from a week-long process to mere seconds.**

***Keywords*—power of attorney, European Blockchain Services Infrastructure (EBSI), decentralized zero-trust architecture, self-sovereign identity, IPv8, legal entities**

I. Introduction

During World War II, allied codebreakers and mathematicians, including Alan Turing, worked on deciphering encrypted messages with the utmost secrecy. Bletchley Park, where the deciphering occurred, was patrolled by armed guards with strict orders to ensure the safety of the classified information and prevent unauthorized access [1]. This legacy of security and trust inspires the zero-trust architecture paradigm, a crucial approach for securing the digital EU economy, from passport-level identity to invoices. Zero-trust architecture is the blueprint for the industrial revolution in the emerging digital-native infrastructure, where traditional security solutions are no longer sufficient to protect against the abundance of data and artificial intelligence [2]. By providing persistent security through access controls that ensure no user, device, or application is trusted implicitly, this paradigm shifts the focus to proactive rather than reactive security measures, making it a vital tool for protecting against cyber threats [3]. Examples include the high occurrence of identity theft. In 2018, the U.S. Department of Justice reported 16.3 million victims of identity theft [4], while in the Netherlands around 110 thousand cases were reported in 2021 [5]. The consequences of these breaches have made "unauthorized access" a highly topical subject. Simultaneously, the European Commission is advocating a data economy in which users control their data [6, 7], whereby the intention is to oppose big tech's control on online identity and the associated induced privacy issues [8, 9].

Therefore, the European Union will provide its citizens with a mainly self-sovereign digital identity by 2025 [10]–[13]. Self-sovereign identity refers to a decentralized digital identity paradigm in which people have complete control and ownership over their personal data and how it is shared [14]. In combination with this identity, the intention is to adopt secure cyber practices, such as the zero-trust architecture methodology within legal entities [15]. The EDI will be implemented at the "high" level of assurance of the revised electronic IDentities And Trust Services (eIDAS) regulation [16, 17]. Thus, a natural person can be confidently identified [18, 19]. We will assume that the identification process is accomplished through a trusted identifier with the high level of assurance described in the eIDAS regulation [20]. Currently, most EU identification processes do not meet this level and the EDI Architecture and Reference Framework requires the EDI to be at eIDAS assurance level "high" [21]. When the EDI is implemented, a natural person can be easily verified, expediting coherent zero-trust architectures. The assurance of the identity of a natural person is important to establish their authority to act on behalf of a legal entity. In the Netherlands, the connection between a natural person and a legal entity is currently established by "eHerkenning", a standardized login system recently made mandatory for many entrepreneurs [22, 23]. However, the Dutch government is also assessing alternatives [24], due to the need for a more

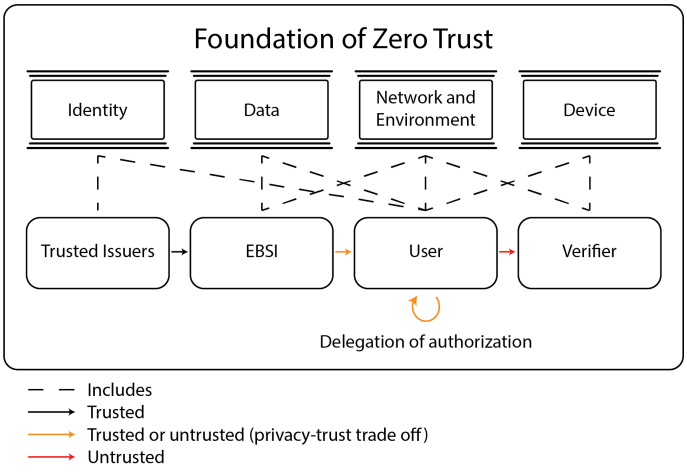

Fig. 1. Zero-trust architecture for delegation

robust, efficient, and less costly means to connect a natural person and a legal entity. Identifying a natural person, and their subsequent connection to a legal entity, are two components forming the foundation of our zero-trust architecture. Our zero-trust architecture is based on the pillars of the United States' Cybersecurity and Infrastructure Security Agency (CISA) zero-trust model and is applied accordingly to represent legal entities in a distributed manner and ensure that data and services are not accessed by unauthorized individuals or entities [25]. The five CISA-pillars are identity, device, network and environment, application workload, and data. However, the application workload, the fifth pillar of the CISA zero-trust model, is inapplicable to our model, as our solution is completely distributed. Figure 1 presents the zero-trust architecture and the other four pillars. It enables users to act on behalf of a legal entity without requiring the verifier to trust the user. This paper, shows that our zero-trust architecture is well-founded, verifiable, irrefutable, profoundly portable, and widely applicable.

The outline of this paper is as follows. Section II presents the current state of research in the area, highlighting the challenges that remain to be addressed. Section III addresses the research methodology, research boundaries, and academic relevance. Subsequently, Section IV explains the terminology and proposes a zero-trust architecture. Section V then showcases the technical details of the implementation and presents a design for the zero-trust architecture. Section VI evaluates the scalability of the system, measurements of latencies, and strategies to optimize its performance and usability. Consequently, Section VII provides a conclusion for our findings. Lastly, Section VIII provides possible improvements and future work.

II. Problem Description

In establishing and maintaining online trust the difficulty concerns verifying the identity of natural users and legal entities within the digital realm. In the physical world, people can rely on visual cues and personal interactions to establish trust, whereas, in the digital world, these methods are limited to pictures or video. Therefore, other means of establishing trust are required - not only for verification purposes, but also to prove a user's authority over a legal entity. Regarding the latter, various methods are available to assess whether a natural person acts on behalf of a legal entity. However, these methods are outside the zero-trust architecture methodology [26]. Figure 2 represents the current ways through which a natural person can be verified by a verifier, to allow them to represent a legal entity. The verifier must verify the (alleged) representative's identity and consult one of the sources that could indicate that the identified person is allowed to act on behalf of the organization. The problem with the current methods of verification for proving authority is that they are costly, non-transparent, inconsistent, outdated, and rigid [27]–[29]. Furthermore, these methods are scarcely implemented outside the Netherlands. Moreover, the registration process for binding a natural person to a legal entity is only available in the Netherlands, and is a cumbersome process taking weeks [30]. Additionally, the centralized nature of these registries imposes security vulnerabilities. All these drawbacks have led to a lack of portability of the trust provided by the present methods. In our solution, we argue that we can make trust portable for legal entities by assuming the existence of the anticipated European Digital Identity and addressing each mentioned drawback by adhering to a decentralized zero-trust architecture.

III. Research Methodology

This study employs a qualitative research design to explore and analyze the zero-trust architecture paradigm and its applicability to ensuring persistent security for distributed legal entity representation. We employ a case study approach to examine a zero-trust architecture implementation of the EDI and its connection to legal entities in the Netherlands. To enable all EU member states to benefit from our research, we provide a system architecture that can be implemented by all EU member states. Furthermore, an open-source implementation is provided according

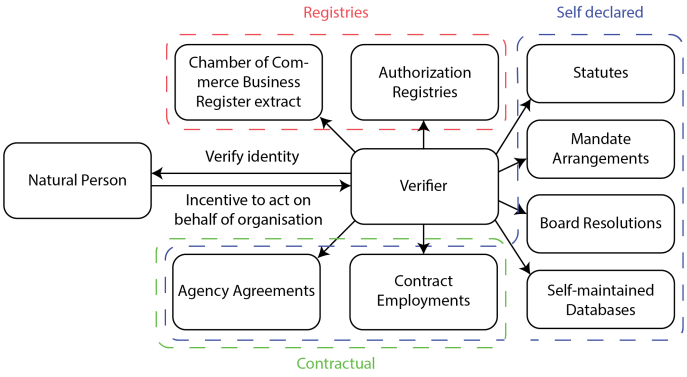

Fig. 2. Current situation of legal entity representation

to the given system architecture to research whether the architecture would withstand integration [31]. Thus, we aim to determine whether it is possible to create a distributed zero-trust architecture for irrefutable legal entity representation. The scope of our research is based on topic, location, time, implementation framework, and financial resources. Firstly, the research topic is digitally representing a legal entity while assuming a natural person has been identified on eIDAS' high assurance level. As the research was performed at the Delft University of Technology in cooperation with the KVK, the system architecture is limited geographically to EU member states because these form the boundaries of the EBSI initiative and EDI. Regarding the implementation, the use case is limited to the Netherlands but considers cross-border functionality within the EU member states' borders. Concerning time, the research was performed within a year such that the author could obtain the degree of Master of Science at the Delft University of Technology. Regarding the implementation, the research is limited to the IPv8 protocol and Kotlin Superapp application developed by the Delft University of Technology. Lastly, the research is financially limited as no budget is provided.

Nonetheless, the significance of our research is in contributing guidance for zero-trust architecture implementation and creating secure and portable legal entity representation. Furthermore, we exhibit possibilities for applications to the EBSI and the planned EDI infrastructure.

IV. System Architecture

This section examines the system architecture of our decentralized peer-to-peer zero-trust architecture. The system architecture is intended to be an open standard for EU member states and demonstrates the potential implications of the planned EDI and applications thereof.

Figure 1 provides a visualization of the open standard system architecture based on the pillars of the CISA zero-trust model. Our system comprises four main components: trusted issuers, the EBSI, users, and verifiers. The trusted issuers are responsible for placing verifiable credentials pertaining to legal entities onto the EBSI. Thereafter, users (natural persons) who want to act on behalf of a legal entity, can retrieve their credentials from the EBSI. Retrieving the credential directly from the EBSI is named a root credential, which gives full authorization over the legal entity. Users may also issue credentials to other users, indicated by the orange self-loop in Figure 1. All users can present their authority to a verifier. The whole chain from a trusted issuer to a verifier is called the zero-trust chain, which is the irrefutable truth. Furthermore, all users may serve as presenters to prove their authorization or act as verifiers to verify another user's credentials. Concerning adoption, it is the presenter's decision to accept the verifier. Conversely, it is the verifier's decision to specify the accepted presentations from presenters. Each component in the system architecture of Figure 1 and accompanying terminology is described in the following subsections.

A. Terminology

The representation by a natural person of a legal entity is described as a type of power of attorney (PoA). A 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 act on the principal's behalf, as specified in the PoA document. PoAs can be used for various 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 inherently authorized on behalf of a legal entity is described as having root PoA over that legal entity. In the Netherlands, this is the functionary enlisted in the KVK business registry, where an enlisted functionary is a user with full authority over the legal entity.

Similar interpretations of PoAs exist, such as delegation, mandate, authorization, and guardianship [32, 33]. For several reasons, the term PoA is used in this work. Firstly, delegation is used ambiguously and may not have legal effect [34, 35]. Secondly, mandating has an alternative definition in public law;[1] moreover,

[1]Article 10:10 Awb

the responsibility in our system should be with the attorney-in-fact, contrariwise to mandates. Thirdly, the term authorization is too vague and does not necessarily concern legal binding. Lastly, guardianship involves transferring all power away from a person who cannot make decisions for themselves [36], which is inapplicable in our system as issuers will remain authorized to act.

Regarding accountability, the attorney-in-fact is expected to use due diligence and sound judgment in performing their duties. They may be held accountable for their actions if they fail to fulfill their responsibilities or abuse their power [37].

B. Trusted Issuers

In our zero-trust architecture, a trusted issuer is responsible for linking a natural person's identity and a legal person, such as a corporation or governmental agency. Correspondingly, trusted issuers play a critical role by providing the trust anchor. In most EU member states, the connection between a functionary and a legal entity is recorded at a chamber of commerce, commercial court, or governmental agency [38]. These chambers, courts, and agencies are potential trusted issuers. Typically, trusted issuers only have a limited number of functionaries cataloged in their registry. This is not an issue for our architecture as we provide a complete architecture for PoAs. The only condition that must be held is that every legal entity has at least one functionary registered at a trusted issuer, this is always the case, as the legal entity would not otherwise exist.

C. European Blockchain Services Infrastructure

The EBSI 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 [39, 40]. The EBSI network is based on the Hyperledger Fabric platform and uses a permissioned consortium model [41] 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 should register functionaries of legal entities in the EBSI. These registrations will become available on the EBSI in the World Wide Web Consortium (W3C) verifiable credentials format [42], achievable through the trusted issuer registry API of the EBSI [43]. The verifiable credential is customized and available in EBSI's trusted schemas registry [44]. If a registration of a functionary must be revoked, this is made feasible by the revocation and endorsement registry [45].

D. Users

A user of our system is required to complete an onboarding process[2] in pursuance of binding their personal record to the device used by them. Correspondingly, the process involves identification 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 EU Architecture and Reference Framework [47] and outlined in the eIDAS regulation [20, 48]. The feasibility of the high LoA has sparked a lively argument regarding the user's hardware concerns [49], privacy issues [50, 51], cross-border governmental distrust [52], and offline operability [53]. In the provided architecture we assume that personally identifiable data on the high LoA is available. Nevertheless, this assumption is not strict, as the zero-trust architecture we provided can still be operational with an existing form of electronic identification, such as Ireland's MyGovID, Italy's SPID, France's FranceConnect, and the Netherlands' DigiD. However, this will make the system more centralized and dependent on these services, altering the decentralized character of this work. Acquiring personally identifiable data on the high LoA 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 [54, 55]. Once the personally identifiable data is linked to the user's device, 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 root PoA of the legal entity of which they are a functionary. Combined, these empower the user to act on behalf of the legal entity and give them 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. In this hierarchy, the user has complete control over their PoAs and issued PoAs. Furthermore, the user is not required to trust another user, the user must only trust the trusted issuer. The system will contain branches and verifiable chains, which can be revoked or altered. Revocation is achieved by adding the ID of the PoA to the revoked PoA list. The list of revocations is disseminated through the network of users and verifiers. Subsequently, the user can provide a presentation of their PoA that a verifier can trust, enabling the

[2]Specified as "enrolment" in the eIDAS regulation [46]

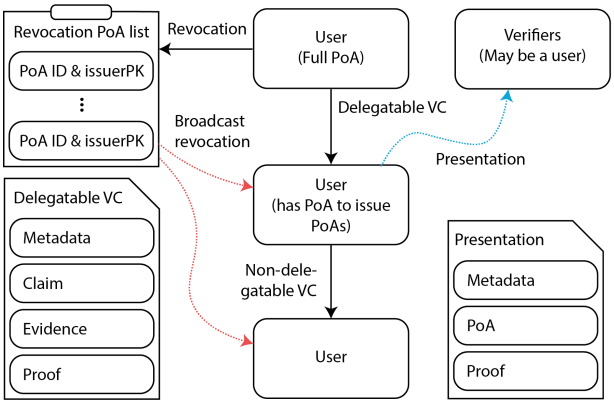

Fig. 3. Zero Trust Architecture for delegation, zoomed in on user

user to irrefutably represent a legal entity where they consider this appropriate.

E. Verifiers

A verifier can verify the presentation presented by a user, and every user within the system can act as a verifier. However, a verifier can also be an entity outside the system that accepts presentations from our system. This is possible due to the format of a PoA, which is a delegatable verifiable credential according to the W3C standard [56]. On revocation of a delegatable verifiable credential, the credential ID, hash and issuer's public key are added to a list that is disseminated through the network. Due to the delegatable verifiable credential format and revocation method, our zero-trust architecture system conjointly adheres to the zero knowledge proof paradigm[3] [57]. Figure 3 provides a detailed overview of the components within our zero-trust architecture.

V. Design

We present the outcomes of implementing the zero-trust architecture for legal entities in an operational design. The design is built on top of TU Delft's decentralized Web3 societal infrastructure [58], further called the IDknip. This societal infrastructure is a decentralized platform constructed to provide identity, trust, money, and data services. The IDknip has the functionality to onboard a user based on their identity which has been issued by a trusted issuer. Our design is built in Kotlin; therefore, it operates on Android OS. The network used is the internet over the IPv8 protocol, which enables secure data sharing and communication among a network of peers [59]. To evaluate the performance and efficiency 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. Trusted Issuer - KVK

The implementation allows someone to quickly and securely verify their identity using their legal identity. Subsequently, the user can obtain their PoA from the KVK. The requirement is that they are registered as a functionary at that legal entity. This is achieved through connecting with the HR data service from the KVK to receive a signed XML from which the functionaries of a legal entity can be deduced. A fee for start-up costs of €1040 and €2.40 for each call is required to access this data[4] [60, 61]. In our implementation, the user interacts with a pre-production server of the HR data service; switching to production involves paying, adding the keys, and adjusting one boolean [62]. Once successful, the user can issue PoAs to other users. Figure 4 visualizes how a root PoA can be obtained from the KVK and then verified by a verifier.

Figure 4a shows the identity fragment of the IDknip; from here, the user can click the "+" sign to obtain or issue PoAs. Once clicked, dialog 4b will appear. The option "Receive PoA from KVK" is chosen to receive a root PoA from the KVK. Accordingly, the dialog of Figure 4c will appear, where the user can insert the KVK-number of which the user is a registered functionary in the company registry of the KVK of that legal entity. Having completed and clicked upon "GET", a request with the given name, surname, birthday, and the inserted legal entity number is sent to the pre-production server of the KVK data service. Accordingly, the KVK verifies whether the provided legal entity indeed has a registered functionary matching the given name, surname, and birthday provided by the user identity. When a match is found, the user will receive the PoA as shown in Figure 4d. The user can click on the PoA to view the detailed presentation of the PoA as shown in Figure 4e. The detailed presentation contains general information about the PoA, the possibility of revoking or deleting the PoA, and a verifiable QR code.

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

[4]The price for each call will be free of charge from 2025.

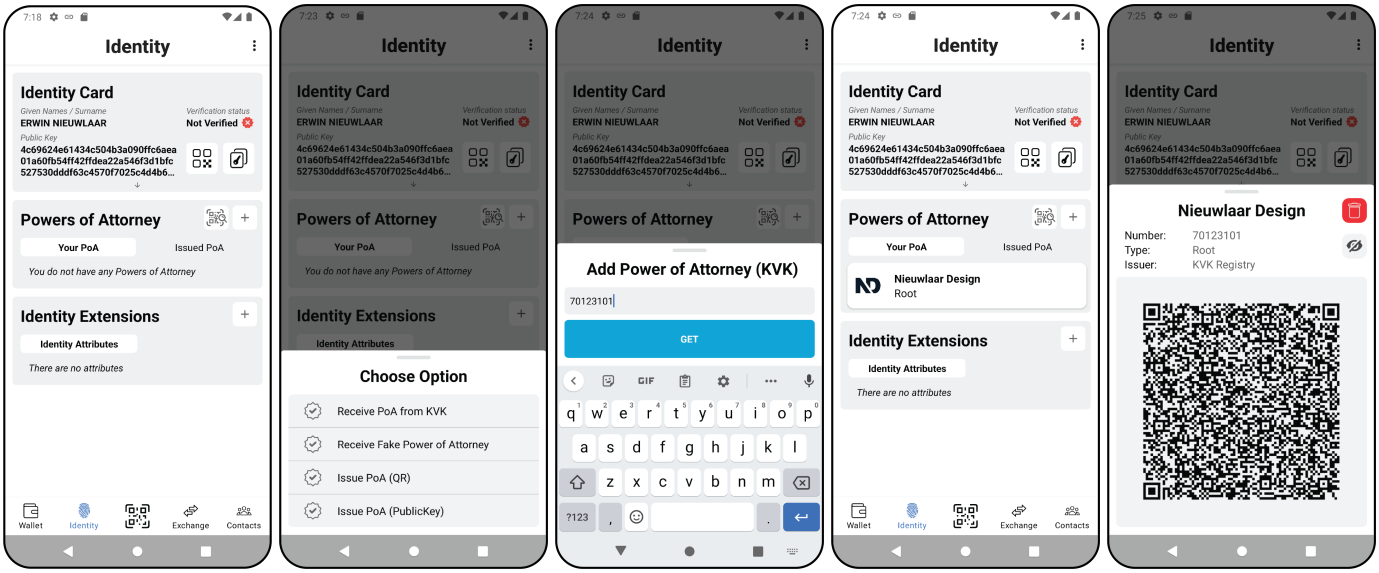

Fig. 4. Flow of obtaining power of attorney from the KVK. **(a)** Identity fragment of the IDknip application. **(b)** Add PoA menu. **(c)** Adding PoA dialog from the KVK. **(d)** Overview of the identity fragment with a root PoA obtained from the KVK. **(e)** The detailed dialog of the PoA with a verifiable QR, the option to delete the PoA, and general information on the PoA.

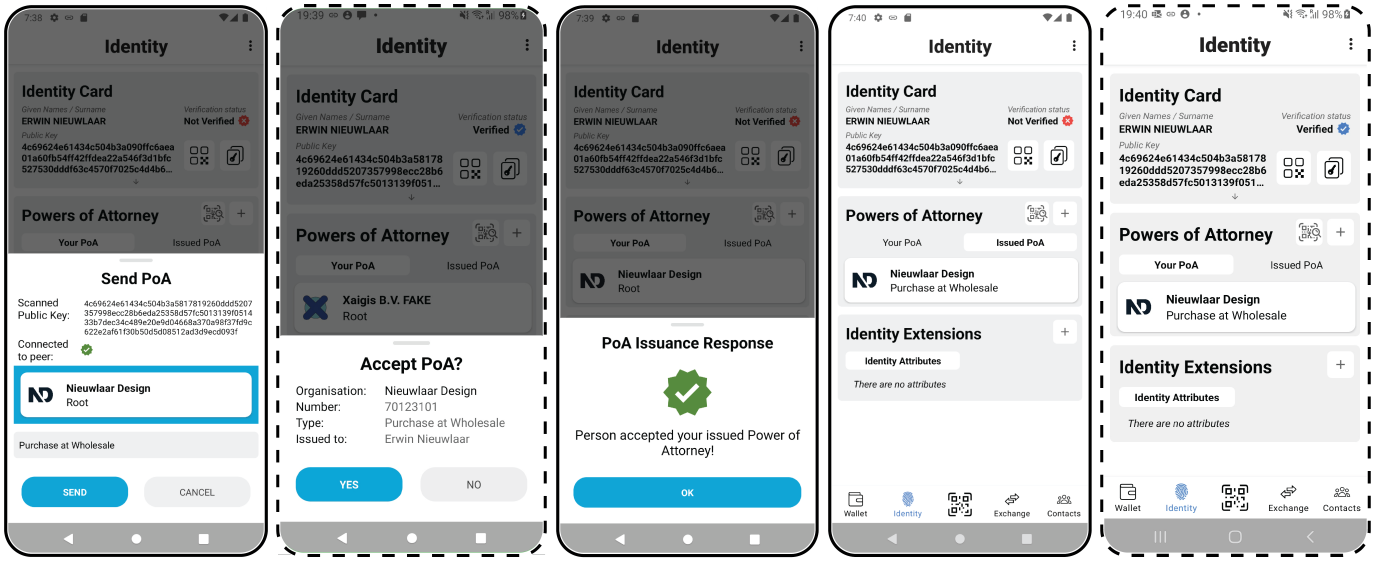

Fig. 5. Peer-to-peer issuance of a power of attorney. **(a)** Dialog to choose PoA to issue with and the PoA desired to be issued. **(b)** Dialog to accept receiving PoA. **(c)** Response of sent PoA. **(d)** Issued PoAs of Device 1. **(e)** Received PoAs of Device 2.

B. European Blockchain Services Infrastructure

As shown in Figure 1, the trusted issuers are expected to place the credentials of owners or functionaries of a legal entity in the EBSI. Implementing the EBSI in a wallet is a burden as the login is frequently incomprehensible. Additionally, resolving an issue with the assistance of the service desk took several weeks. However, currently, a few wallets exist that are operational with the EBSI blockchain, although most of these wallets depend on the open-source work of Walt-ID. In this work, we did not implement the integration with the EBSI in our design; however, we made a prototype of how trusted issuers should import their accreditations into the EBSI. Accordingly, the PoA credentials are directly obtained from the KVK's company registry pre-production server. Trusted issuers can be enabled to enlist their accreditations by creating

a verifiable credential schema in the trusted schemas registry. This schema contains all the information to issue a PoA to the functionary of the affiliated company. Scheme 1 presents the appearance of the schema. For trusted verifiers to place 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 be placed in all the company functionaries. Accordingly, the user can to retrieve the PoA from EBSI by identifying themselves, making our architecture functional for all EU member states.

Scheme 1. EBSI power of attorney verifiable credential

```
{
  <credential-metadata>,
  "credentialSubject": {
    "id": "did:ebsi:bef...k21",
    "powerOfAttorney": {
      "id": "did:ebsi:c27...9f1",
      "nameIssuer": "KVK",
      "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 observed in the scheme, the verifiable credential comprises three parts; the credential metadata, the PoA data, and the proof of the credential. The metadata and proofs are according to the W3C standards and are therefore minimized for a clearer overview.

C. User

Once a user in a legal entity has obtained the PoA from the KVK, the user can delegate PoAs and create a structure of authorizations. Figure 5 shows how a PoA is issued peer-to-peer from one user to another. Firstly, the user with permission to issue PoAs will select "Issue PoA (QR)" or "Issue PoA (PublicKey)" from Figure 4b. Once the public key is obtained successfully, the principal should choose the PoA with which they would like to issue the PoA. Furthermore, the principal must select the PoA it wishes to issue. The dialog to accomplish this is presented in Figure 5a. Once the PoA request is sent, the potential attorney-in-fact will receive a notification to accept or deny the PoA as shown in Figure 5b. When the attorney-in-fact accepts the PoA, the principal will receive the issuance response shown in Figure 5c. Accordingly, the principal can view its issued PoAs from the identity fragment in the issued PoA tab as presented in Figure 5d. Lastly, the attorney-in-fact is now authorized to purchase at a business-only wholesale, as shown in Figure 5e. Within the application, any PoA can be created including the possibility to delegate PoAs.

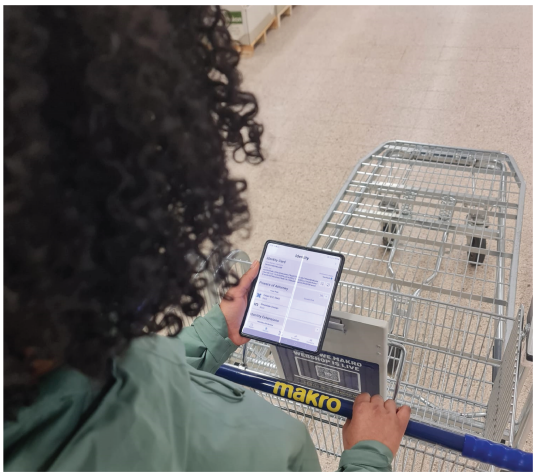

Fig. 6. Demonstration at Makro

D. Verifier - Makro

During a live demonstration at a Makro, the Makro functioned as the verifier. Makro is a wholesale store in the Netherlands for business only; that is, only representatives of a legal entity are allowed to purchase at Makro. The users enrolled as a functionary at the KVK obtained their PoA credentials. Subsequently, they could present a Makro with their authorization to enter it. Alternatively, the user who obtained the PoA credentials from the KVK could delegate another user a PoA. The user who has received the PoA can show a PoA presentation to the Makro. The Makro can verify the presentation. Accordingly, the user can enter and purchase at the wholesale.
The live demonstration at the Makro showed that our design was successfully implemented. The user could show their presentation to the Makro, which could verify the user's PoA. The demonstration highlights the feasibility and practicality of implementing our zero-trust architecture for legal entities in an operational environment. Figure 6 shows a picture of a live demonstration at the Makro.

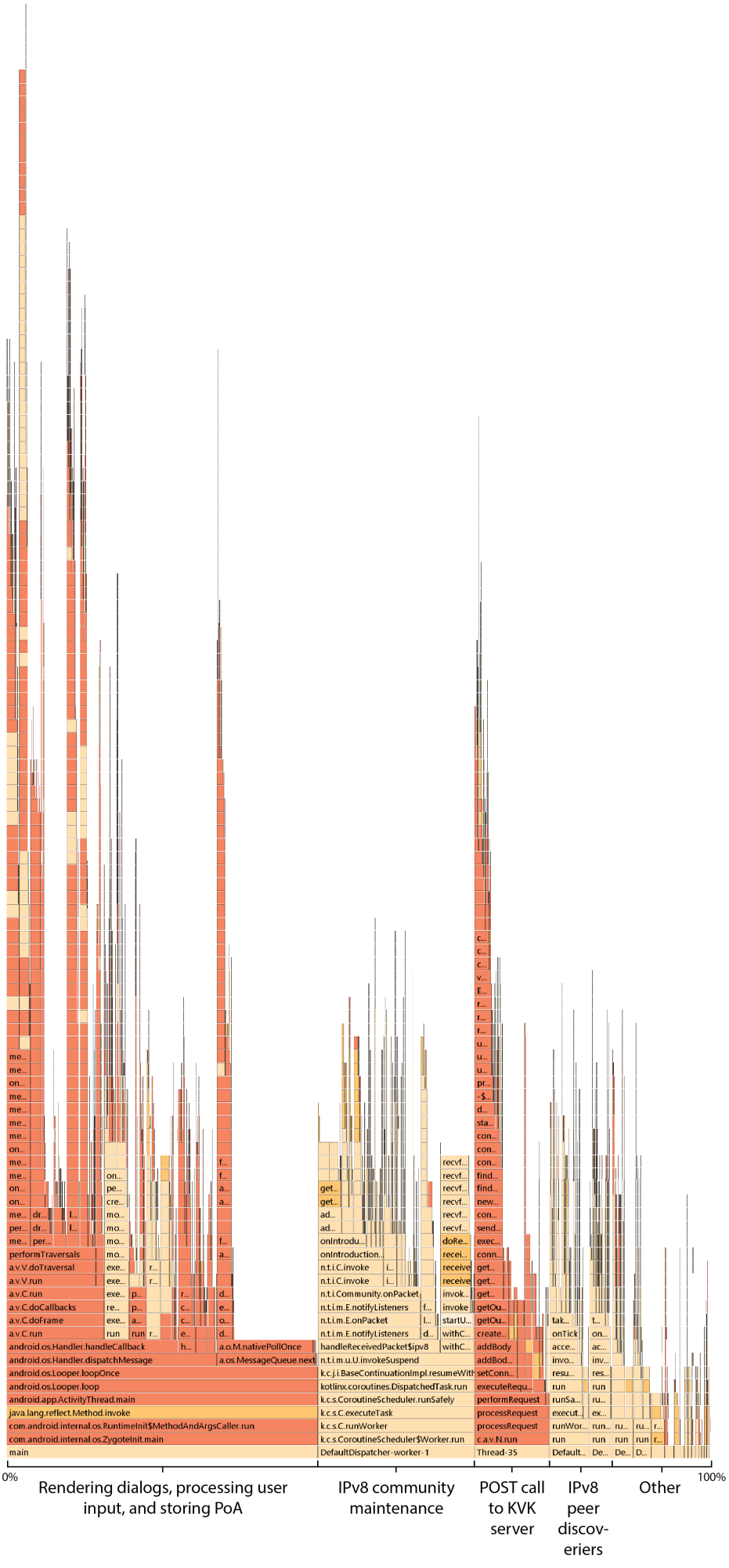

Fig. 7. Flame chart of retrieving PoA from the KVK

VI. Performance Analysis

We will determine whether our zero trust design is fit-for-purpose by analyzing the technical feasibility and user experience. The technical feasibility is analyzed by measuring CPU usage through various user stories and the user experience is measured based on the time needed for the onboarding process and latencies of all user stories concerning PoAs. Considering the CPU usage, the processes of the IDknip have been recorded and visualized in flame charts [63, 64]. The process of obtaining a PoA from the KVK server was recorded using a Samsung Fold 3, which has a Snapdragon 888 CPU and is shown in Figure 7. This user story was chosen for display as it appeared to be the most CPU-consuming process of all PoA user stories within the IDknip. For clarity purposes, the steps of the user story recorded in Figure 7 are visualized in Figure 4. During the recording, the IPv8 protocol claimed a part of the CPU computational power by maintaining connectivity with all Superapp's communities and new peer discoveries. However, we can conclude that the load of IDknip on the mobile's CPU is relatively low, as the maximum percentage of CPU use only reached 35% during the complete recording. Accordingly, we can conclude that the load of the IDknip is small as through all its functionalities the CPU use is 35% at maximum. Based on Figure 7, the process of obtaining a PoA from the KVK server involves multiple steps, including sending a POST request, processing the response, rendering dialogs, processing user input, and storing the PoA. The flame chart provides a detailed view of all the threads involved in this process, highlighting the specific components of the system that contribute to the overall latency.

Furthermore, the latencies associated with onboarding a user's identity are displayed in Figure 8. The data shown in Figure 8 represents the identity onboarding of seven novice users except for the data including the trained tag within their label. The data with the trained tag represents the latencies of 10 repeated measurements where the person knows all the onboarding steps beforehand. Therefore, the trained person positioned the camera and NFC reading device more accurately, achieving a faster onboarding process and principally measuring the speed of the camera and NFC data transfer. As the figure shows, the total time for novice users to onboard their identity is high. The primary reason is the difficulty in understanding how the passport should be scanned with NFC. This is caused by users not receiving a confirmation of their camera scan, or understanding the image and text explaining the instructions for

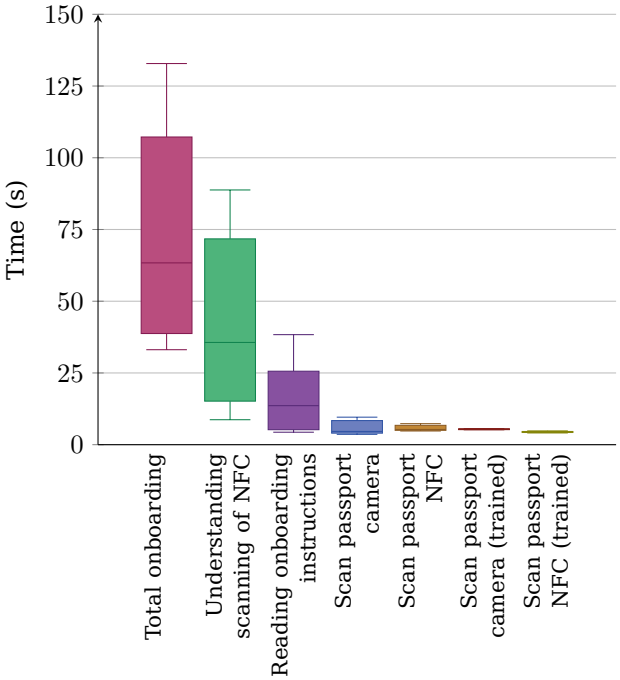

Fig. 8. Latencies onboarding identity

the NFC scan. An improved UX design for this step could solve this issue, enabling users to onboard their identity within a minute.

Figure 9 displays the network latencies associated with various user stories; KVK requests, issuing PoA P2P requests, revoking PoA P2P requests, and EBSI requests, for both WiFi and 4G connections. As the figure shows, the network latencies are generally low for both WiFi and 4G connections, except for requests made to the KVK server. The high latency associated with KVK requests is primarily due to the larger amount of data sent from the KVK server to the user. This data includes detailed information about the business or organization, and the amount of data can potentially slow the request process, resulting in higher latencies. Conversely, the latencies associated with issuing PoA P2P requests, revoking PoA P2P requests, and EBSI requests are relatively low, indicating that the system performs efficiently for these operations. We also observe that the latencies are generally low for both WiFi and 4G connections, indicating that the system can handle requests on top of moderate network connectivity with similar efficiency.

VII. Conclusion

We presented a decentralized peer-to-peer zero-trust architecture for EU member states and showed

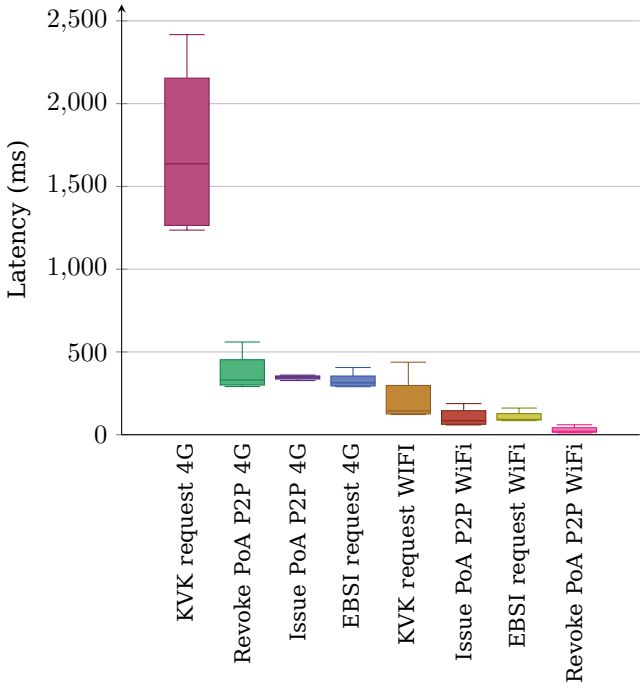

Fig. 9. Network latencies

it to be feasible to implement in a real-world use case. The architecture is proposed as an open standard, and we provide a reference open-source implementation to demonstrate its potential implications. The system architecture components are related to the pillars of the CISA zero-trust model. These components comprise the trusted issuers, the EBSI, users, and verifiers. The trusted issuers place verifiable credentials on the EBSI, and users retrieve their credentials from the EBSI. Once a user obtains a credential from the EBSI, the user can delegate power by issuing PoAs, empowering natural persons to hold their credentials and decoupling from the existing methods of legal entity representation as described in the problem description. These users may present their authority to a verifier to prove authorization to irrefutably represent a legal entity. The whole system adheres to the GDPR, revised eIDAS regulation, SSI principles, and W3C delegatable credentials standard. Integrating the EBSI in the IDknip was too time-consuming; hence additional research can fulfill the complete implementation of the EBSI. This integration would enable secure and transparent cross-border transactions, digital identity verification, and trusted authorization among the European member states. Inspired by the legacy of security and trust established by allied codebreakers and mathematicians during World War II, our proposed decentralized peer-to-peer zero-trust architecture offers a promising solution for securing the digital EU economy, from passport-level identity to cross-border transactions. By providing persistent security through access controls and verifiable credentials, our architecture represents a scalable and vital tool for protecting against cyber threats in the emerging digital-native revolution.

VIII. Future Work

Future research can focus on several areas to improve the ideas and implementation provided in this thesis. Firstly, researchers can work on further refining assumptions related to the identification process of eIDAS with respect to the high assurance level, including the use of mobile technology to enhance the security and privacy of personal data [49]. Secondly, an alternative method for revocation can be developed to improve the efficiency of the revocation process and reduce message and storage complexity. Thirdly, the IDknip could be integrated with TU Delft's TrustChain, a blockchain-based system for verifying the integrity of digital data. Fourthly, exploring cross-community implementation could ensure that the IDknip can be used effectively across various communities in the IPv8 protocol enhancing scalability. Fifthly, 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. Sixthly, research can work on developing more information privacy based on delegatable verifiable credentials [56, 65]. Finally, maximizing the deployment of the zero-trust architecture paradigm, where data is always encrypted, can help enhance the security and privacy of the system. Researchers can use the CISA zero-trust maturity model for guidance on maturing our zero-trust architecture [25].

References

[1] M. Campbell, “Beyond zero trust: Trust is a vulnerability,” Computer, vol. 53, no. 10, pp. 110–113, 2020.

[2] A. Froehlich, “Perimeter security vs. zero trust: It’s time to make the move,” October 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/tip/Perimeter-security-vs-zero-trust-Its-time-to-make-the-move

[3] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” aug 1 2020, [Online; accessed 2023-02-22]. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-207/final

[4] U.S. Department of Justice, “Victims of Identity Theft, 2018,” apr 1 2021, [Online; accessed 2023-02-21]. [Online]. Available: https://bjs.ojp.gov/library/publications/victims-identity-theft-2018

[5] “2,5 miljoen Nederlanders in 2021 slachtoffer van online criminaliteit,” feb 28 2022, [Online; accessed 2023-02-21]. [Online]. Available: https://www.cbs.nl/nl-nl/nieuws/2022/09/2-5-miljoen-nederlanders-in-2021-slachtoffer-van-online-criminaliteit

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

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

[8] 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/

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

[10] 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

[11] P. Mart, “Is the EU Digital Identity Wallet an Implementation of Self-Sovereign Identity?” jul 13 2022, [Online; accessed 2023-01-26]. [Online]. Available: https://thepaypers.com/expert-opinion/is-the-eu-digital-identity-wallet-an-implementation-of-self-sovereign-identity--1257446

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

[13] 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

[14] C. Allen, “The path to self-sovereign identity,” Apr 2016. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[15] B. GROOTHUIS, “Report on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 | A9-0313/2021 | European Parliament.” [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0122

[16] “Revision of the eIDAS Regulation: Findings on its implementation and application | Think Tank | European Parliament,” https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)699491, jul 3 2022.

[17] “Report from the commission to the european parliament and the council - on the evaluation of regulation (eu) no 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eidas),” June 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0290

[18] Feb 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

[19] “Commission recommendation (eu) 2021/946 of 3 june 2021 on a common union toolbox for a coordinated approach towards a european digital identity framework,” June 2021. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H0946&qid=1478030835186

[20] The European Commission, “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.

[21] “European Digital Identity Architecture and Reference Framework – Outline,” feb 22 2022. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

[22] Jun 2022. [Online]. Available: https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:HR:2022:1787

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

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

[25] “Zero Trust Maturity Model,” 6 2021, [Online; accessed 2023-02-22]. [Online]. Available: https://www.cisa.gov/zero-trust-maturity-model

[26] J. Kindervag et al., “Build security into your network’s dna: The zero trust network architecture,” Forrester Research Inc, vol. 27, 2010.

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

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

[29] J. Patel, “Bridging data silos using big data integration,” International Journal of Database Management Systems, vol. 11, no. 3, pp. 01–06, 2019.

[30] “Meldingsplicht voor buitenlandse bedrijven en zelfstandigen.” [Online]. Available: https://ondernemersplein.kvk.nl/meldingsplicht-voor-buitenlandse-bedrijven-en-zelfstandigen/

[31] E. Nieuwlaar, “Github - Nieuwlaar/trustchain-superapp at IDelft_EBSI_trust,” jan 23 2023. [Online]. Available: https://github.com/Nieuwlaar/trustchain-superapp

[32] 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.

[33] 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

[34] 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.

[35] [Online; accessed 2023-01-04]. [Online]. Available: https://www.proz.com/kudoz/spanish-to-english/law-contracts/702330-apoderamiento-%22power-of-attorney%22-vs-%22delegation-of-authority%22.html

[36] 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.

[37] M. Goetting, “Power of attorney,” Revised Mar, 2013.
[38] “European business registers,” [Online; accessed 2023-01-03]. [Online]. Available: https://www.kvk.nl/english/about-the-netherlands-chamber-of-commerce/foreign-registers-overview/european-business-registers/
[39] “ukraineebsi,” jun 17 2022, [Online; accessed 2023-01-03]. [Online]. Available: https://thedigital.gov.ua/news/ukraina-priednalasya-do-evropeyskogo-blokcheyn-partnerstva-v-statusi-spostergacha-1
[40] “Europeancountriesjoinblockchainpartnership,” apr 10 2018, [Online; accessed 2023-01-03]. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/european-countries-join-blockchain-partnership
[41] M. Turkanović and B. Podgorelec, “Signing blockchain transactions using qualified certificates,” IEEE Internet Computing, vol. PP, pp. 1–1, 09 2020.
[42] “Verifiable Credentials Data Model v1.1,” mar 3 2022, [Online; accessed 2023-01-03]. [Online]. Available: https://www.w3.org/TR/vc-data-model/
[43] “Trusted Issuers Registry API v3 | EBSI developers hub,” [Online; accessed 2023-01-03]. [Online]. Available: https://api-pilot.ebsi.eu/docs/apis/trusted-issuers-registry/latest
[44] “Trusted Schemas Registry API v2 | EBSI developers hub,” [Online; accessed 2023-01-03]. [Online]. Available: https://api-pilot.ebsi.eu/docs/apis/trusted-schemas-registry/latest
[45] “Education Verifiable Accreditation Records - EBSI Specifications -,” [Online; accessed 2023-01-03]. [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Education+Verifiable+Accreditation+Records
[46] 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.
[47] “The European Digital Identity Wallet Architecture and Reference Framework,” feb 10 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework
[48] 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.
[49] 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
[50] M. Walsh, “The challenges facing the EU’s new digital identitysystem - Raconteur,” nov 7 2022, [Online; accessed 2023-01-05]. [Online]. Available: https://www.raconteur.net/technology/problems-identified-for-new-eu-digital-identity-wallet/
[51] J.-H. Hoepman, “Civil liberties aspects of the European Digital Identity Framework.” jan 31 2022, [Online; accessed 2023-01-05]. [Online]. Available: https://blog.xot.nl/2022/01/31/civil-liberties-aspects-of-the-european-digital-identity-framework/index.html
[52] 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,” 7 2022, [Online; accessed 2023-01-05]. [Online]. Available: https://geopolitique.eu/en/2022/07/13/the-scale-of-trust-local-regional-national-and-european-politics-in-perspective/
[53] D. Mekinec, “Offline face recognition: why use it? - Visage Technologies,” aug 12 2022, [Online; accessed 2023-01-05]. [Online]. Available: https://visagetechnologies.com/offline-face-recognition/
[54] A. Traichuk, “6 Best Open-Source Projects for Real-Time Face Recognition | HackerNoon,” apr 28 2021, [Online; accessed 2023-01-05]. [Online]. Available: https://hackernoon.com/6-best-open-source-projects-for-real-time-face-recognition-vr1w34x5
[55] O. B. Maestro, “Biometrics in Identity,” oct 27 2022, [Online; accessed 2023-01-05]. [Online]. Available: https://dis-blog.thalesgroup.com/identity-biometric-solutions/2022/10/27/biometrics-in-identity/
[56] 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
[57] 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
[58] J. Bambacht, “Web3: A decentralized societal infrastructure for identity, trust, money, and data,” feb 28 2022, [Online; accessed 2023-01-08]. [Online]. Available: https://repository.tudelft.nl/islandora/object/uuid%3A3ad68dbd-3444-4e01-94a2-d28044b0ba3f
[59] Tribler, “Ipv8 documentation,” 2022. [Online]. Available: https://py-ipv8.readthedocs.io/_/downloads/en/latest/pdf/
[60] “Hoe bepalen wij onze tarieven?” [Online; accessed 2023-01-08]. [Online]. Available: https://www.kvk.nl/over-kvk/over-het-handelsregister/tarieven/
[61] “Kamerbrief over voortgang Datavisie Handelsregister.” [Online]. Available: https://www.rijksoverheid.nl/documenten/kamerstukken/2023/01/09/voortgang-datavisie-handelsregister
[62] M. Mayer, “Handleiding kvk bevoegdheden,” [Online; accessed 2023-01-08]. [Online]. Available: https://bevoegdheden.mayersoftwaredevelopment.nl/
[63] C.-P. Bezemer, J. Pouwelse, and B. Gregg, “Understanding software performance regressions using differential flame graphs,” 2015 IEEE 22nd International Conference on Software Analysis, Evolution, and Reengineering, SANER 2015 - Proceedings, pp. 535–539, 04 2015.
[64] B. Gregg, “The flame graph,” Commun. ACM, vol. 59, no. 6, p. 48–57, may 2016. [Online]. Available: https://doi.org/10.1145/2909476
[65] J. Blömer and J. Bobolz, “Delegatable attribute-based anonymous credentials from dynamically malleable signatures,” in Applied Cryptography and Network Security - 16th International Conference, ACNS 2018, Leuven, Belgium, July 2-4, 2018, Proceedings, ser. Lecture Notes in Computer Science, B. Preneel and F. Vercauteren, Eds., vol. 10892. Springer, 2018, pp. 221–239. [Online]. Available: https://doi.org/10.1007/978-3-319-93387-0_12