Aligning eIDAS and Trust Over IP: A Mapping Approach

Cristian Lepore, Romain Laborde, Jessica Eynard

Aligning eIDAS and Trust Over IP: A Mapping Approach

Cristian Lepore*
Institut de Recherche en Informatique de Toulouse
Toulouse, France
Université Paul Sabatier Toulouse III
Toulouse, France
cristian.lepore@irit.fr

Romain Laborde
Institut de Recherche en Informatique de Toulouse
Toulouse, France
Université Paul Sabatier Toulouse III
Toulouse, France
romain.laborde@irit.fr

Jessica Eynard
Université Toulouse Capitole
Toulouse, France
jessica.eynard@ut-capitole.fr

ABSTRACT

On 29 February 2024, the European Parliament approved the amendment of the eIDAS Regulation. The revision introduces new elements and a new EU Digital Identity Wallet, expected to be ready by the end of 2026. Even after the wallet is released, the numerous digital identity schemes operating within the Member States will continue to function for some time. The introduction of the new wallet and the coexistence of numerous digital identity schemes will pose challenges for service providers, who will need to adapt to support various means of identity, including the EU wallet, for their services. In response to this challenge, this study examines how to plan interoperability between eIDAS and existing frameworks. First, we organize the eIDAS components in a knowledge graph that encodes information through entities and their relations. While doing this, we highlight various design patterns and use a graph entity alignment method to map components of eIDAS and the Trust Over IP.

KEYWORDS

Digital Identity, eIDAS, European Digital Wallet, Interoperability, Mapping, Trust Over IP, Trust Services

ACM Reference Format:
Cristian Lepore, Romain Laborde, and Jessica Eynard. 2024. Aligning eIDAS and Trust Over IP: A Mapping Approach. In *The 19th International Conference on Availability, Reliability and Security (ARES 2024), July 30–August 02, 2024, Vienna, Austria.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3664476.3670919

1 INTRODUCTION

The Internet needs trust mechanisms to know with whom we interact. Earlier Internet designers did not implement trust services because they knew and trusted each other [35]. The first to warn about the consequences of the lack of trust was Kim Cameron in The Seven Laws of Identity (2005) [7], then quoted by the MIT scientist David D. Clark in a series of articles from the Washington Post (2015) [47]. Online fraud and identity theft rise everywhere, with consequences for users [27] and organizations [22]. For example, compromised firms lost 2.1% of market value within the two days surrounding a data breach [8]. Effects can last up to 2 years [5].[1] Thus, Europe considers building trust in cyberspace a priority [48].

The first tentative to create a trustworthy digital space was in 1999 when Europe published directive 1999/93/EC to harmonize the use of electronic signatures [14]. However, the directive was transposed into national laws differently. In 2014, the eIDAS Regulation federated existing flavors and expanded the scope of the previous directive to include identity verification and trust services [17]. The Regulation introduced a supervisory regime to guarantee secure interactions, although the number of cross-border transactions was low [13]. In 2021, the Regulation was revised to meet the evolving digital landscape [30]. The revision introduced new elements and an EU Digital Identity Wallet (EDIW). These new entities should allow every person in Europe to exchange identity information from trusted private and public sources. Today, industry partners are actively collaborating to streamline the wallet, with a mandate to be ready by Q4 2026. The European Union has also introduced a supporting specification, the Architecture Reference Framework (ARF), that will assist the industry in designing the wallet [16].

The ARF provides a set of functional and non-functional requirements and templates [44]. Those requirements were initially quite abstract; for example, the ARF needed to provide insights regarding technical aspects to consider when implementing the stored cryptographic functions of the EDIW, as stated in [44]. It also lacked an in-depth analysis of relationships between entities. Today, the ARF – which is currently at v1.3 and v1.4 is meant to be published in the coming weeks – is a more comprehensive specification that defines the roles and responsibilities of entities such as (Q)TSPs, PID Providers, QEAA Providers, and QES Providers – along with the necessary trust relationships. These are in Section 4 (European Digital Identity Wallet Ecosystem) and Section 6 (Trust Model) of the ARF [16]. Besides conforming to best practices, some challenges remain unresolved for the future implementation of the eIDAS framework:

a) Standards and technological immaturity. Many existing technologies for developing the basic building blocks of the EDIW are still in their early stages. Several working groups, such as the Decentralized Identity Foundation (DIF),[2] OpenID

*Cristian Lepore contributed to the article's conception, design, mapping exercise, and writing. Dr. Romain Laborde supervised the work, provided review and assistance in securing funding. Dr. Jessica Eynard provided review and securing funding.

ARES 2024, July 30–August 02, 2024, Vienna, Austria

ACM ISBN 979-8-4007-1718-5/24/07
https://doi.org/10.1145/3664476.3670919

[1] This data refers to three automaker companies that suffered a trust incident in 2015. Their market capitalization has been compared to the value of the STOXX Europe 600 Automobiles index record.
[2] https://identity.foundation/ accessed on 12 April 2024

Foundation (OIDF),[3] World Wide Web Consortium (W3C),[4] Open Wallet Foundation,[5] and ISO 18013-5 [33], contribute with protocols and components. A pre-emptive assumption of what technology to include in the ARF can be challenging for most of these technologies.

b) In 2022, there were 24 notified eID schemes with 40 eID means operating within the Member States (MSs). It is expected that these will continue to operate long after the release of the EU wallet. Thus, Service Providers (SPs) need to be able to support several eIDs, including the EDIW, for their services [44].

c) In addition to this, even a preliminary study of the interoperability between eIDAS and private sources of identity information from existing trust frameworks, such as banks and the aviation industry, can be challenging. In corner cases, this may require inspecting the wallet's source code or the vendor's archetypal assumptions.

Given these challenges, we aim to streamline the interoperability between eIDAS and the public/private sources by mapping the eIDAS components to the Trust Over IP model. The Trust Over IP (ToIP) is a reference model for implementing interoperable trust systems, which has recently gained traction among the decentralized identity community. By mapping eIDAS to the ToIP, we can potentially enhance the efficiency of future interactions between eIDs and existing trust frameworks that rely on private companies as a source of information. This could also streamline the implementation of new interoperable protocols and technologies.

Contributions. This paper contributes with:

(1) a mapping of eIDAS entities along the Trust Over IP stack. By positioning eIDAS entities along the Trust Over IP stack, we guide the industry in the design of interoperable wallets and ecosystem entities. We clarify where to position services for data provisioning, the interface to open, and the protocol to choose when planning interoperability with other frameworks. However, this requires to know with whom to interact.

(2) Therefore, while doing this, we organize eIDAS as a knowledge graph. A knowledge graph frames the relationships between entities. This graph provides information about whom to address for legal and technical hurdles.

Contributions (1) and (2) are consistent with the actual eIDAS revision and help to address challenges (a – c). The remainder of this paper is as follows. We model information from the Regulation and its complementing ARF in the form of a knowledge graph (Section 2). For clarity, we favor high-level descriptions over low-level details: e.g., we do not list all instances of (Q)TSPs; rather, we generalize them as one entity. We then highlight the evolution of trust models (Section 3); in doing so, we overview the Trust Over IP model, which is a dual-layered stack that guides the design of interoperable trust systems [11]. We use the entity alignment method to map the eIDAS and Trust Over IP (Section 4) and discuss findings (Section 5). We examine the limitations of our mapping process in Section 6. Finally, we summarize key contributions and provide avenues for future research.

[3]https://openid.net/ accessed on 3 May 2024
[4]https://www.w3.org/ accessed on 1 May 2024
[5]https://github.com/openwallet-foundation accessed on 24 April 2024

2 THE EIDAS REGULATION

The eIDAS is the European Regulation that aims to harmonize the use of electronic identification and trust services across Europe. It defines identification schemes that require users to authenticate to a service with a level of confidence that can be low, substantial, or high [24]. Once authenticated, users have access to a range of services that allow them to sign documents (eSignature), ensure the origin of data (eSeal), and provide evidence (timestamp, delivery service, website authentication) [43].

Trust establishment. The framework establishes a trust pyramid [3]. At the top of the pyramid are the EU Trusted Lists, which are XML-based repositories appointed by Member States to retrieve relevant information about identity providers. On the second level, Conformity Assessment Bodies (CABs) and accreditation authorities set a supervisory regime for specific service providers referred to as Trust Service Providers (TSPs). Among TSPs, Qualified Trust Service Providers (QTSPs) adhere to specific trustworthiness requirements to issue services with high assurance [39]. Examples of QTSPs include ValidatedID and InfoCert [10]. They can issue identity documents and attestations with legal value. For instance, opening an online bank account requires customers to (digitally) sign a statement accepting the bank's conditions. The bank cannot release this statement; it must be issued by a qualified service provider (e.g., ValidatedID or InfoCert) on its behalf. Once signed by the parties (bank and customer), the document confirms the opening of the bank account. Finally, the bottom level of the pyramid includes standards and best practices from the European Telecommunications Standards Institute (ETSI), the European Committee for Standardization (CEN), and the International Standard Organization (ISO).

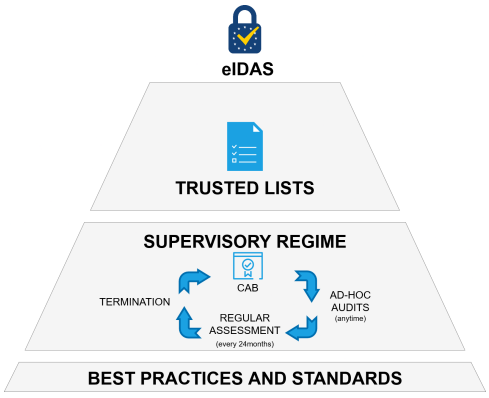

Figure 1: eIDAS pyramid of trust [1].

Service provisioning. The service provisioning starts with (Q)TSPs to issue personal data (PIDs) for holders who store them in their wallet storage component. The wallet also has additional logical components to interface human behaviors, such as the Driving

application, and prepare a composition of personal data as credentials for Relying Parties (RP). The holder then presents credentials to the Relying Parties. When the holders and Relying Parties are physically close and without Internet connectivity, communication can be initiated through NFC (or QR-code) in compliance with ISO/IEC 18013-5 [2].[6] For online communication, alternative protocols that extend the OpenID specifications can be used: the OpenID for Verifiable Credential Issuance [31] and its counterpart for credential presentation [46]. The former is used to ship credentials from (Q)TSPs for holders, while its counterpart, the OpenID for Verifiable Presentation, allows holders to present attestations to Relying Parties. These protocols will be tested within pilot projects to cover primary use cases, roughly divided into user authentication, e-signatures, and website authentication. The pilot projects aim to concretize the effort to instill technical assurance and human accountability.

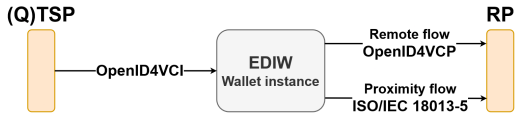

Figure 2: eIDAS service provisioning [15].

Next steps. After the plenary vote on 29 February 2024, we expect the amendment to enter into force between April and May. A six-month period of implementing acts for the technical specifications of the wallet will follow. Then, Member States will have 24 months to provide their respective wallet solutions. Figure 3 shows the timeline of the legislative process and technical implementation of the EU wallet. However, this approach to legal mandates, trust establishment, and technical interoperability may deviate from other frameworks. Over the years, there have been several attempts to create interoperable models for digital trust.

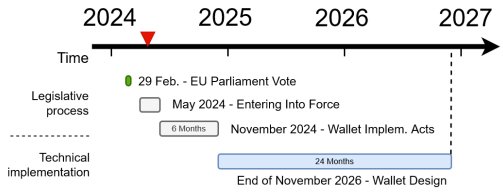

Figure 3: Timeline of the legislative process and technical implementation of the EU wallet.

3 TRUST MODELS EVOLUTION

We synthesize some major efforts to create interoperable models for digital trust. We then discuss the main differences between the models.

Sovrin. Sovrin was among the pioneers in creating trust models. Its stack consists of a ledger, agents, and clients [38]. The ledger is a public, permissioned network that employs agents and runs transactions. Agents are the counterparts of digital personas who execute, read, and write commands on the chain; clients are system endpoints, such as smartphones or laptops, that facilitate users' interaction with the network. With time, discussions on promising standards, new Decentralized Identifiers, and protocols hardened the work on the stack; thereby, the Sovrin Foundation produced a list of reference documentation as a legal foundation of the Sovrin Network. Since then, Sovrin has provided only governance of technology. Today, Sovrin deploys human accountability. Its work also strengthens governance in the Trust Over IP stack [19].

Trust Over IP. The Trust Over IP (ToIP) is a late-generation model [11] resulting from the collaboration of organizations and individual contributors from various research fields. The model is a dual-layered stack that integrates technical verifiability and human accountability at every layer. The stack features a four-layer hourglass [26] (Figure 4), which is commonly used to describe the design of the TCP-IP Internet stack, where a large number of protocols at the top and bottom narrow to only one protocol in the middle: the IP protocol. A similar shape is now being used to lay

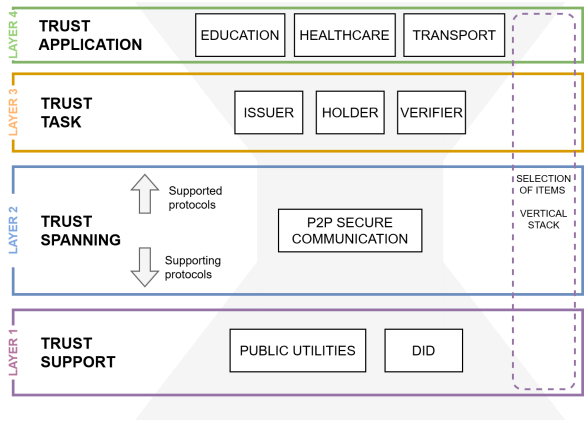

Figure 4: The hourglass model of the Trust Over IP [11, 26].

interoperability across trust systems by the Trust Over IP. In the ToIP model, the bottom is supporting items for trust tasks. This layer provides public utilities and anchor points for trust system items on a persistent layer. It includes identifiers and data registries that should last for a long time. They narrow to a second layer: agent-to-agent communication, which provides a standard way to establish secure communication between two endpoints. The second layer is also the hourglass neck. The hourglass neck must be as thin as possible. While the other layers may implement items to accomplish the same trust task, layer two abstracts from the specific implementation underneath while supporting the composition of items from the trust task (layer three). The third layer is where e-identity data is exchanged between parties. It involves the type of data with credential formats and entities: issuer, holder, and verifier. Protocols depend on ecosystem applications, such as healthcare systems and educational purposes. Therefore, technology items may vary slightly between vertical stacks for different industry

[6] The ISO/IEC 18013-5 provides references and specifications to consume personal information from a mobile driving license.

solutions. The task of layer four is to combine the technology items from the previous layers in a convenient and easy-to-use way. Human mandates and policies intertwine with technology in each of these layers.

Decentralized Identity Foundation – DIF. The DIF hosts discussions on decentralized identity with many industry contributors. Its Interoperability Working Group proposes a stack inspired by the classic OSI model [6]. The stack is similar to the Trust Over IP, with a few exceptions: 1) the target is on cross-cutting technology in the sphere of decentralized identity; 2) the stack refers only to technical considerations; 3) it has a traversal "Layer X" that deals with cross considerations, such as storage, crypto primitives, and accountability. However, the layer still needs a proper definition, as the ToIP did for all its layers.

We synthesize the scope of the three models in Table 1. The Sovrin governance layer provides legal documents for the Sovrin network, while the DIF deals with technical aspects of decentralized identity. Besides, the Trust Over IP needs to harden its stack. For example, layer two requires a deeper insight; its establishment of trust spans beyond the identity field and potentially covers several trust systems. Additionally, it deals with technology and human accountability. Given these considerations, we aim to map the eIDAS entities and the Trust Over IP model.

Table 1: Summary of Sovrin, ToIP, and DIF.

Model	Scope	Tech	Governance
Sovrin	Identity / Sovrin Network		✓
ToIP	Several trust systems	✓	✓
DIF	Decentralized Identity	✓	

4 MAPPING METHODOLOGY

Mapping is the process of finding equivalence between entities in different contexts [53]. It involves matching two or more elements from a source domain and a target domain [9]. Those domains can be encoded as two distinct knowledge graphs (KGs) to provide a visual representation of human knowledge. A knowledge graph $KG = (E, R, A)$ consists of entities E , relationships R, and attributes A. Graphs possess an excellent property that allows annotations to match identical entities in two distinct graphs.

Therefore, in the reminder, we describe our methodology to map eIDAS and ToIP using manually annotated knowledge graphs. While doing this, we depart from previous mapping exercises [23, 36], as they did not formalize a methodology, leaving the reader with a leap of faith. Our procedure, instead, tweaks a process described for knowledge graph alignment [12] that consists of the following steps:

1. Organization of knowledge. First, we express eIDAS and Trust Over IP concepts as two distinct knowledge graphs (KG). Figure 5 shows the knowledge graph of eIDAS. The knowledge graph is incrementally built starting from the overview of the wallet logical components and ecosystem entities presented in the ARF v1.3 [15].

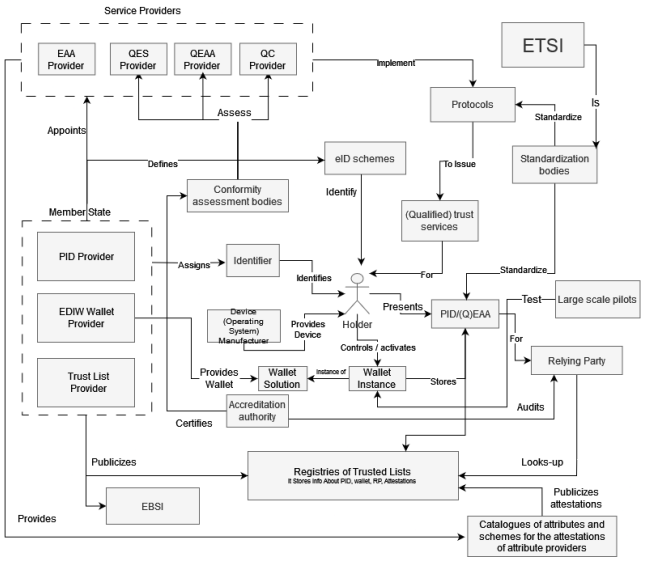

Figure 5: The knowledge graph representing eIDAS framework. As service providers, from left to right: (Q)EAA is (Qualified) Electronic Attestation of Attributes provider. QES stands for Qualified Electronic Signatures and Seals provider. QEAA stands for Qualified Electronic Attestation of Attributes provider. QC is Qualified certificate for electronic signature/seal provider.

Since it defines the roles and responsibilities of entities along with the necessary trust relationships, we just used academic papers and the European Union Agency for Cybersecurity (ENISIA) to complement the information [1, 34, 43]. Similarly, the ToIP knowledge graph combines documents from official deliverables and papers [11, 20]. The result is shown in Figure 6. This step is crucial to plan the mapping exercise. For brevity, in the following, we refer to the eIDAS knowledge graph as KG_e and the ToIP as KG_t.

2. Selection of entity in eIDAS. We select one entity from KG_e, the eIDAS Knowledge Graph. The selection can be random or comply with specific heuristics. Once the entity has been selected, it is removed from the graph KG_e.

3. Selection of the next candidate in ToIP. The mapping happens in the space of possible candidates for KG_t. The next candidate is selected by systematically identifying all potential pairs.

4. Matching. Given the two knowledge graphs $KG_e = (E_i, R_i, A_i)$ and $KG_t = (E_j, R_j, A_j)$, where E is the set of entities, R is the set of relationships, and A are the attributes; we define a mapping $m = (e_i, e_j)$ with $e_i \in E_i$ and $e_j \in E_j$ as a pair e_i and e_j of identical entities [51]. We consider two entities identical when they serve the same purpose and can perform the same function or activity. The purpose of the entity is specified under the ARF v1.3 [15]. The result of this step is to identify all possible mapping pairs M for a given entity e_i. In other words, this step results in exploring all possible candidates in the target space for a given eIDAS entity.

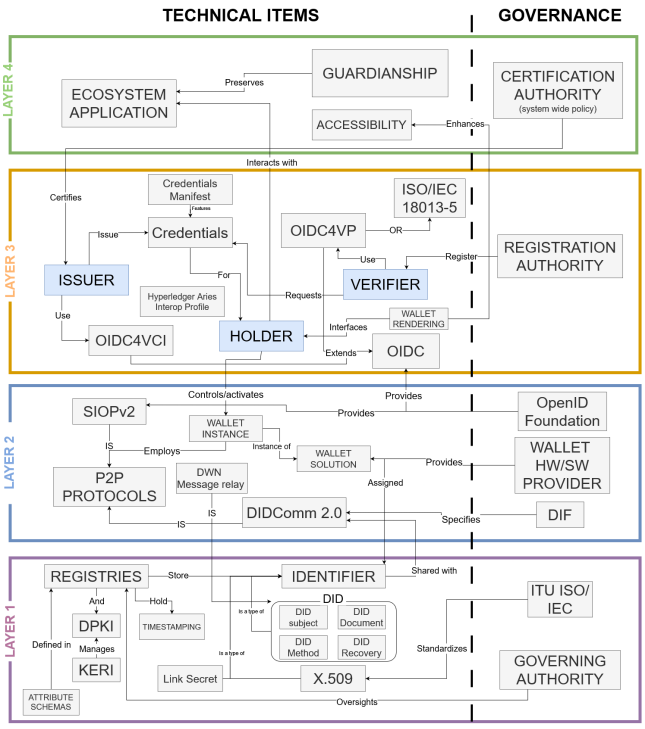

Figure 6: The knowledge graph representing the Trust Over IP items along the stack.

5. Placement. If a mapping exists, so M is not an empty set, we position the entity within the layer of the ToIP stack to which the target entity e_j pertains. Whereas M is an empty set, the entity e_i will not be part of the final graph. Finally, if M contains more than one possible mapping for e_i, a conflict is solved by referring to the official documentation of e_i to find the best match. As a result of the mapping exercise, a new graph is created, containing entities from the original eIDAS graph KG_e that are common to the ToIP graph KG_t. As a direct result of the matching process, the' new' entities mirror the position of E_j in KG_t within the ToIP's layering architecture. For this reason, the entities of the ToIP stack will not appear in the final graph. Only the eIDAS entities that directly match the ToIP entities will take the respective place of the entity from the ToIP.

6. Iteration. Steps 2 – 5 are iterated to build the output graph progressively. Iterations halt when E_i is empty, and all possible entities have been explored. Hence, no new alignment is proposed. We then use the intermediate results of step 5 as output.

The following section synthesizes the outcome.

5 RESULTS AND OBSERVATIONS

We present the outcomes of our eIDAS and Trust Over IP mapping exercise. We complete the description with a visual representation of eIDAS components along the Trust Over IP stack. The next part kickstarts the technical discussion, whereas the subsequent part concerns governance. We conclude with findings and observations as a result of the mapping process.

5.1 Technical Stack

The following is a high-level description of entities that serves as an introduction to Figure 7. The left-hand side of the figure reports entities for anchoring technical trust and services for system end-points.

Layer 1: Trust support. System end-points are anchored on a persistent layer through identifiers and public registries. The European Union foresees the implementation of several national and pan-European public registries to provide information about attributes and their revocation. Identifiers play a pivotal role in cross-border transactions. By identifying transactions, they simplify the process, improving efficiency and convenience. Provisioning identifiers demands an infrastructure that can be centrally managed, e.g., the Public Key Infrastructure (PKI), or a decentralized database, e.g., EBSI [45]. The EBSI, the European Blockchain Service Infrastructure, stands as a robust solution, ensuring the secure storage of identifiers and personal information in a tamperproof manner, maintaining the integrity of data over time. The EBSI then becomes an authoritative source of information on the respective wallet, certificates, and relying parties. By querying these registries, verifying the accuracy of the information shared by the wallet is possible. A unique identifier links the holder, issuer, and verifier to the registry. One of the main differences between Europe and the United States, for example, is that central registries managed by governments are considered by citizens (in Europe) as a source of authority. At the same time, in the US, people tend to consider a central database untrustworthy.

Layer 2: Trust spanning. This layer hosts hardware, software components, and protocols for the peer-to-peer communication between system end-points. The European Commission foresees a mobile wallet app installed on the user's device. The app will contain several logical components to manage attributes and key material and present a collection of attributes to relying parties. Peer-to-peer communication between wallets and relying parties follows the OpenID SIOPv2 specification, a variant of the OpenID Connect client that does not rely on a preconfigured Provider but uses a Self-issued OIDC Provider [32]. The P2P communication allowed by SIOPv2 specification allows us to concentrate on the use case description of proximity supervised and unsupervised flows, as depicted in the ARF. In a proximity flow scenario, when the user is physically close to a Relying Party, the exchange and disclosure of mDL attributes occur through proximity technologies like NFC or Bluetooth. These two proximity flows vary significantly: in the supervised flow, the EUDI Wallet showcases mDL attributes to a human Relying Party or under their guidance (who may also utilize a device), while in the unsupervised flow, the EUDI Wallet reveals mDL attributes to a machine without human supervision. Additionally, several options are available for implementing proximity (in-person) flow, with Europe featuring the ISO/IEC 18013-5, commonly used for mobile driver's licenses [4].

Layer 3: Trust task. This layer employs protocols and data formats where data exchange happens over the Internet (remote flow). In the EUDI Wallet, we have two distinct scenarios. In the remote cross-device flow, the User accesses information from the service on a different device than the one hosting the EDIW Wallet, which solely serves to secure the session. This could be, for instance, scanning a QR code with the EUDI Wallet on a login page to access a bank account via a web browser. On the other hand, in the remote same-device flow, the EUDI Wallet User utilizes the EUDI Wallet device to secure the session and access information from the service. The remote communication happens through a family of protocols that complement the OpenID Connect family of protocols with APIs to support the issuance and presentation of credentials: the OpenID Connect for Credential Issuance and OpenID Connect for Credential Presentation. The OpenID for Verifiable Credential Issuance provides a standardized framework for securely issuing digital credentials using decentralized identity technologies. This not only ensures their tamper-evident nature and interoperability across different platforms but also enables a trusted and interoperable ecosystem for managing and exchanging verifiable credentials in digital transactions. Similarly, the OpenID for Verifiable Credential Presentation focuses on the secure presentation and verification of these digital credentials, allowing individuals to selectively disclose their credentials to relying parties in a privacy-preserving manner. This leverages cryptographic proofs to demonstrate the credentials' authenticity and validity without revealing unnecessary personal information, a significant benefit in today's data privacy landscape. This OpenID Connect protocol family supports different JSON-based data formats, from SD-JWT and JSON-LD/LD-Proof [28].

Layer 4: Trust application ecosystem. Technology items from the previous layers are selected on a vertical stack for specific applications. For this purpose, the European Union has actively initiated pilot projects to implement the vertical stack for several primary use cases. The eIDAS large-scale piloting projects represent a crucial step towards fostering seamless digital interactions across Europe. The projects are centered around e-travel credentials (EWC), e-government website authentication (POTENTIAL), instant payment (NOBID), and education services (DC4EU) [50]. Through these pilot projects, various stakeholders collaborate to test and validate innovative solutions. By facilitating the mutual recognition of electronic identities and enabling secure electronic transactions, these projects contribute significantly to Europe's digital transformation, empowering citizens, businesses, and public administrations alike.

These projects organize technical items in a vertical stack. For those items to work together in a concerted manner, they need policies and rules under a governance framework. These rules are enforced by public institutions acting on behalf of national or supranational authorities.

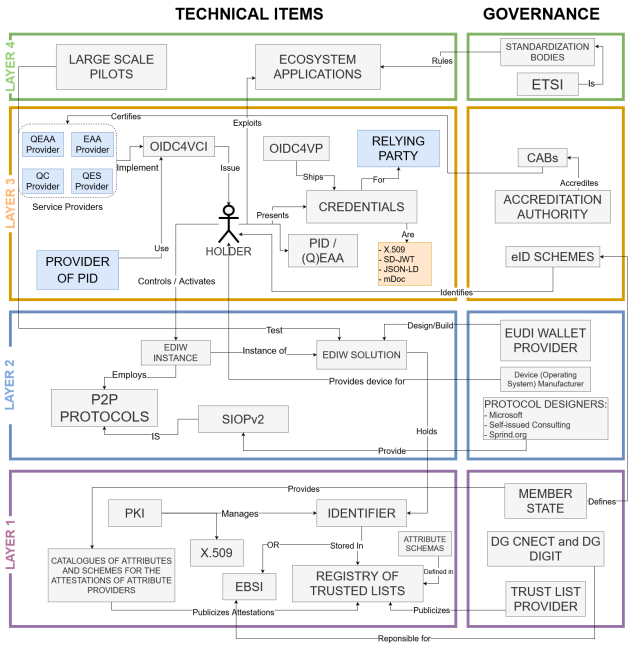

Figure 7: The result of the mapping exercise of eIDAS and Trust Over IP.

5.2 Governance stack

The following is a high-level description of entities and must serve as an introduction to the right-hand of Figure 7, which shows entities that promote human accountability.

Layer 1: Trust support. Public utilities require ad hoc providers, such as Member States and national authorities, to provide catalogs of attributes and attestations. The pan-European blockchain network (EBSI) comprises node operators selected by the Member States and certified by the European Blockchain Partnership (EBP). Policies for the EBSI are carried out under the European Directorate-General DG CNECT, with the DG DIGIT department managing the technical implementation of the network.

Layer 2: Trust spanning. The layer primarily encompasses system end-point manufacturers and protocol designers. The prospect of a single wallet for all European citizens versus multiple digital wallets remains uncertain, and its emergence will depend on pilot projects. More than 200 organizations collaborate on the wallet's design with different degrees of commitment. Regarding the peer-to-peer protocol, developing the OpenID SIOPv2 is a collaborative effort involving Microsoft, Self-Issued Consulting, and Sprind.org [52].

Layer 3: Trust task. A few authorities supervise the provisioning of electronic identification and services. Member States account for national e-identity schemes; those schemes define rules for the delivery of services. These services may include electronic signatures, which must meet specific European Telecommunications Standards Institute (ETSI) standards. Standards in compliance with

the ETSI are Advanced Electronic Signatures based on CMS-signed data, such as CAdES, XML with XAdES, PDF-based with PAdES, and JSON-based JAdES [25].

Layer 4: Trust application ecosystem. Several governing authorities facilitate the trust scaling. First and foremost, the trialogue formally drafted the revision of the Regulation. The trialogue is an informal negotiation process in which the EU Commission, the Council, and the Parliament meet. The Regulation mandates Member States to publish and maintain the lists of qualified trust service providers. Any modification must reflect the online tool (List of Trusted Lists) [10] provided by the European Commission. Finally, standards are approved and promoted by the European Telecommunications Standards Institute (ETSI).

5.3 Observations

The mapping exercise has yielded valuable insights into eIDAS. All items from eIDAS have been positioned along the stack, and no companion is left behind. Notably, each layer contains at least one element, indicating the absence of empty layers within the stack. This observation suggests that Europe possesses a robust framework encompassing human accountability and technical verifiability.

On the one hand, Europe has increased support for technical protocols and data formats. This is evident from the increased support for technical items like the SIOPv2 protocol. SIOPv2 is a federated protocol that allows for self-assertion of credentials. Including SIOPv2, Europe aims to bridge the gap between traditional centralized identity management systems and emerging decentralized models. SIOPv2, or Self-Issued OpenID Provider (version 2), plays a critical role in bridging different identity management approaches by allowing users to assert their own identities across various online platforms. However, to enhance its effectiveness in this role, there is a need for more evidence and clarity regarding its implementation and benefits. This could involve comprehensive case studies, empirical data, and clear documentation outlining how SIOPv2 facilitates interoperability between different identity systems. Additionally, providing clearer guidelines and best practices for integrating SIOPv2 into existing identity management frameworks would further strengthen its role in harmonizing diverse identity approaches. By addressing these aspects, stakeholders can better understand and leverage the capabilities of SIOPv2 to achieve seamless and secure identity management across different digital ecosystems.

On the other hand, the number of technical items included is only a portion of the items in the ToIP stack. For example, eIDAS does not support Decentralized Identifiers (DIDs). DIDs work with whatever registry is on the first layer. Therefore, the number of supported standards limits eIDAS's ability to compose items on a vertical technical stack.

The governance side has plenty of authoritative bodies in each layer. This is probably because the European Union may leverage direct or indirect control over government authorities. It may also result from eIDAS being a mere Regulation for harmonizing service provisioning and identity in Europe.

Concluding the observations, practitioners may now streamline the work of pilot projects and compose a custom selection of items in each layer to build their vertical stack. This approach facilitates the identification of optimal interfaces between eIDAS components and wallet solutions within the industry. Furthermore, stakeholders can replicate this exercise within existing ecosystems to identify potential overlaps between vendor solutions and eIDAS. Europe can bring trust to identity solutions and interoperability, as the GDPR did for privacy protection regulations.

6 LIMITATIONS

Although process mapping has several advantages, there are some downsides to consider. One significant drawback of process mapping is the considerable time investment required for manual alignment, which can significantly slow down the overall process. Although manual alignment creates knowledge graphs tailored to our specific case and does not use external tools, the time to process the mapping increases with the graph's size. As the size of the graph increases in a manual alignment, the performance decreases, and more time is needed to map all items between the two graphs, highlighting a potential challenge. In particular, exploiting our methodology, if the cardinality of the eIDAS knowledge graph is $|KG_e| = m$ and the Trust Over IP knowledge graph is $|KG_t| = n$, the algorithm's upper time complexity will be $O(n \times m)$; this while considering a constant time for the instruction execution. The time complexity increases when KG_e is a large graph. Therefore, we strive to have eIDAS descriptions at a high level rather than low-level details.

Manual alignment may also result in conflicts between entities, such as an eIDAS entity that matches two items in the ToIP stack. These conflicts can be resolved by referring to the ARF's supporting documentation. However, conflicts are still biased towards personal understanding rather than algorithmic functions. Alternative techniques based on ontology alignment perform better [51], but they can be tedious to settle.

7 CONCLUSIONS

This work is a segment of the research line that aims to develop an assessment model to evaluate digital identity solutions [41, 42]. Such models are essential in response to the numerous attempts to create identity systems and to reason on the existing technical standards and specifications [37]. Interoperability is a crucial criterion for an evaluation model and eIDAS.

More specifically, this work provides an in-depth analysis of eIDAS, as outlined in Section 2. It also maps eIDAS entities with the Trust Over IP framework (Section 5). This mapping offers valuable insights to professionals on where to position their services to ensure interoperability between eIDAS and other frameworks [29, 40].

Related work. Besides creating a trusted digital space and harmonizing national identity schemes, the eIDAS introduces new elements and a new identity wallet, which promises interoperability between systems. The European Union has introduced the ARF, a set of specifications to streamline the wallet's design. On one hand, the supervisory regime guarantees standard rules for service providers. On the other hand, the ARF guides the delivery of

interoperable solutions. Besides the effort, Europe's paradigm of trust establishment through legal mandates may diverge from other frameworks. These differences demand a comprehensive mapping of entities and protocols that differ from previous works.

Past exercises include a graphical overview of identity technology structured along the Trust Over IP technology stack [49] and the DIF stack [23]. They help to position technical items to explore future interoperability challenges. A graphical representation of the eIDAS trust services and corresponding provisioning along a pyramid of trust [18] led to a common understanding of digital identity initiatives on both sides of the Atlantic: EU and the US [36]. Our work departs from previous exercises, where the target is either to list all possible standards within a stack [23, 49] or to build and coordinate future interactions on two frameworks [18, 36].

Future work. Future research may explore ontology alignment techniques to overcome conflicts during the mapping process [51]. An ontology is essentially a meta-model that assists in constructing a knowledge graph [21]. Specifically, a knowledge graph is generated by applying an ontology to a given domain. Besides resolving conflicts, an ontology can be used with automatic or semi-automatic tools to expedite entity mapping. This not only enhances performance but also fast-tracks conflict resolution. Similar work has been done with entity-alignment [51] and network-based approaches [53].

ACKNOWLEDGMENTS

The authors thank Dr. Daniele Canavese from CNRS for suggestions on the mapping methodology and for critically reviewing the paper.

Funding. This work was partially supported by the European research project H2020 LeADS (GA 956562).

REFERENCES

[1] Ignacio Alamillo, Stefane Mouille, Andrea Röck, Nikolaos Soumelidis, Michal Tabor, and Slawomir Gorniak. anno. *Digital Identity Standards.* https://www.enisa.europa.eu/publications/digital-identity-standards/@@download/fullReport ENISA - European Union Agency for Cybersecurity.

[2] Zahra Ebadi Ansaroudi, Roberto Carbone, Giada Sciarretta, and Silvio Ranise. 2023. Control is Nothing Without Trust a First Look into Digital Identity Wallet Trends. In *IFIP Annual Conference on Data and Applications Security and Privacy*. Springer, 113–132.

[3] Olivier Barette, Sylvie Lacroix, Erik Van Zuuren, and Hans Graux. 2017. *Security framework for Trust Service Providers - Technical guidelines on trust services.* https://www.enisa.europa.eu/publications/tsp-security Accessed on March 3, 2024.

[4] V Blynkov and V Yaremenko. 2020. Mobile driving license system deployment model with security enhancement. (2020).

[5] Deloitte CA. 2020. *The Chemistry of Trust Part 1: The Future of Trust.* https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-chemistry-of-trust-pov-aoda-en.pdf Accessed on February 28, 2024.

[6] Juan Caballero, Henk van Cann, and Snorre Lothar von Gohren Edwin. [n. d.]. *Identity Foundation FAQ.* https://identity.foundation/faq/ Accessed on 5 March 2024.

[7] Kim Cameron. 2005. The laws of identity. *Microsoft Corp* 12 (2005), 8–11.

[8] Huseyin Cavusoglu, Birendra Mishra, and Srinivasan Raghunathan. 2004. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce* 9, 1 (2004), 70–104. Accessed on February 28, 2024.

[9] Allan Collins and Mark Burstein. 1989. A framework for a theory of mapping. *Similarity and analogical reasoning* (1989), 546–565.

[10] European Commission. 2024. *eIDAS Dashboard. EU/EEA Trusted List Browser.* https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home Accessed on 8 March 2024.

[11] Matthew Davie, Dan Gisolfi, Daniel Hardman, John Jordan, Darrell O'Donnell, and Drummond Reed. 2019. The trust over ip stack. *IEEE Communications Standards Magazine* 3, 4 (2019), 46–51.

[12] Jos De Bruijn, Marc Ehrig, Cristina Feier, Francisco Martín-Recuerda, François Scharffe, and Moritz Weiten. 2006. Ontology mediation, merging and aligning. *Semantic web technologies* (2006), 95–113.

[13] Ignacio Alamillo Domingo. 2020. SSI eIDAS Legal Report. *How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market. European Commission* (2020).

[14] Jos Dumortier. 2002. The European Directive 1999/93/EC on a Community Framework for Electronic Signatures. *Edirectives: guide to European Union law on ecommerce: commentary on the directives on distance selling, electronic signatures, electronic commerce, copyright in the information society, and data protection, edited by AR Lodder & HWK Kaspersen The Hague* (2002).

[15] EU Digital Identity Wallet. 2023. *Architecture and Reference Framework.* https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md Accessed on 1 March 2023.

[16] EU Digital Identity Wallet. 2024. Architecture and Reference Framework. https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md. Version 1.3.0. Accessed on 8 May 2024.

[17] European Parliament and European Council. 2014. Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union* 57, L 257 (2014), 73–114. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0910 Accessed on February 28, 2024.

[18] ENISA European Union Agency for Cybersecurity. 2021. *Security Framework for Trust Service Providers.* https://www.enisa.europa.eu/publications/security-framework-for-trust-providers Accessed on 7 March 2024.

[19] Sovrin Foundation. 2021. *Sovrin and Trust Over IP Signed Mutual Agreement.* https://sovrin.org/sovrin-and-trust-over-ip-signed-mutual-agreement/ Accessed on 7 March 2024.

[20] Trust Over IP Foundation. [n. d.]. *Changing the landscape—through deliverables.* https://trustoverip.org/our-work/deliverables/ Accessed on 2 March 2024.

[21] Nicola Guarino, Daniel Oberle, and Steffen Staab. 2009. What is an ontology? *Handbook on ontologies* (2009), 1–17.

[22] Chander Mohan Gupta and Devesh Kumar. 2020. Identity theft: a small step towards big financial crimes. *Journal of Financial Crime* 27, 3 (2020), 897–910.

[23] Technische Universität of Berlin Hakan Yildiz. 2020. *Layers of SSI interoperability, DIF Interop WG.* https://github.com/decentralized-identity/interoperability/raw/master/assets/interoperability-mapping-exercise-10-12-20.pdf Accessed on 7 March 2024.

[24] Muhammad Abdullah Hamid, Isha Fatima Ifrah Dar, and Nouman Cheema. [n. d.]. Digital Identity and Legal Rights: the EU's eIDAS Regulation as a Model for Global Digital Trust. *Democracy, Rule of Law, and Protection of Human Rights in the European Union* ([n. d.]), 88.

[25] Juan-Carlos Cruellas Ibarz. 2020. Bringing JSON signatures to ETSI AdES framework: Meet JAdES signatures. *Computer Standards & Interfaces* 71 (2020), 103434.

[26] Trust Over IP. 2023. *The TOIP Trust-Spanning Protocol.* https://www.trustoverip.org/blog/2023/01/05/the-toip-trust-spanning-protocol/ Accessed on March 6, 2024.

[27] Tarmo Kalvet, Marek Tiits, and Pille Ubakivi-Hadachi. 2019. Risks and societal implications of identity theft. In *Electronic Governance and Open Society: Challenges in Eurasia: 5th International Conference, EGOSE 2018, St. Petersburg, Russia, November 14-16, 2018, Revised Selected Papers 5*. Springer, 67–81.

[28] Vid Kersic, Urban Vidovic, Andraz Vrecko, Martin Domajnko, and Muhamed Turkanovic. 2023. Orchestrating Digital Wallets for On-and Off-Chain Decentralized Identity Management. *IEEE Access* (2023).

[29] Jan Lauinger, Jens Ernstberger, Andreas Finkenzeller, and Sebastian Steinhorst. 2023. Janus: Fast privacy-preserving data provenance for tls 1.3. *Cryptology ePrint Archive* (2023).

[30] Silvia Lips, Natalia Vinogradova, Robert Krimmer, and Dirk Draheim. 2022. Re-Shaping the EU Digital Identity Framework. In *DG. O 2022: The 23rd Annual International Conference on Digital Government Research*. 13–21.

[31] T. Lodderstedt, K. Yasuda, and T. Looker. 2024. *OpenID for Verifiable Credential Issuance - draft 13.* https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html Published on 8 February 2024. Accessed on 4 March 2024.

[32] Zoltán András Lux, Dirk Thatmann, Sebastian Zickau, and Felix Beierle. 2020. Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 71–78.

[33] Ketan Mehta, Arun Vemury, Jon Prisby, and Jeff Finke. 2023. Accelerate Adoption of Digital Identities on Mobile Devices: Identity Management. (2023).

[34] Stefan Mocanu, Ana Maria Chiriac, Cosmin Popa, Radu Dobrescu, and Daniela Saru. 2019. Identification and trust techniques compatible with eIDAS regulation. In *Security and Privacy in New Computing Environments: Second EAI International Conference, SPNCE 2019, Tianjin, China, April 13–14, 2019, Proceedings 2*. Springer, 656–665.

[35] Darrell O'Donnell and Jacques Latour. 2023. *A Trust Layer for the Internet is Emerging Toward a More Interoperable and Trusted Internet for Canadians.* https://doi.org/10.13140/RG.2.2.19921.71529
[36] National Institute of Standards and NIST Technology. 2024. *EU-US TTC WG-1 Digital Identity Mapping Exercise Report.* https://www.nist.gov/identity-access-management/eu-us-ttc-wg-1-digital-identity-mapping-exercise-report Accessed on 7 March 2024.
[37] Alex Preukschat and Drummond Reed. 2021. *Self-sovereign identity.* Manning Publications.
[38] Drummond Reed, Jason Law, and Daniel Hardman. 2016. The technical foundations of Sovrin. *The Technical Foundations of Sovrin* (2016).
[39] Esther Ruiz Ben and Margit Scholl. 2023. Usability in Online Public Services. In *Usable Privacy and Security in Online Public Services.* Springer, 13–31.
[40] Abylay Satybaldy, Md Sadek Ferdous, and Mariusz Nowostawski. 2024. A Taxonomy of Challenges for Self-Sovereign Identity Systems. *IEEE Access* (2024).
[41] Abylay Satybaldy, Mariusz Nowostawski, and Jørgen Ellingsen. 2020. Self-sovereign identity systems: Evaluation framework. *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers 14* (2020), 447–461.
[42] Steffen Schwalm. 2023. The possible impact s of the eIDAS 2.0 digital identity approach in Germany and Europe. (2023).
[43] Steffen Schwalm, Daria Albrecht, and Ignacio Alamillo. 2022. eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI. *Open Identity Summit 2022* (2022).
[44] Amir Sharif, Matteo Ranzi, Roberto Carbone, Giada Sciarretta, Francesco Antonio Marino, and Silvio Ranise. 2022. The eidas regulation: a survey of technological trends for European electronic identity schemes. *Applied Sciences* 12, 24 (2022), 12679.
[45] Evrim Tan, Ellen Lerouge, Jan Du Caju, and Daniël Du Seuil. 2023. Verification of education credentials on european blockchain services infrastructure (EBSI): Action research in a cross-border use case between Belgium and Italy. *Big Data and Cognitive Computing* 7, 2 (2023), 79.
[46] O. Terbu, T. Lodderstedt, K. Yasuda, and T. Looker. 2023. *OpenID for Verifiable Presentations - draft 20.* https://openid.net/specs/openid-4-verifiable-presentations-1_0.html Published on 29 November 2023. Accessed on 4 March 2024..
[47] Craig Timberg. 2015. *Net of Insecurity: A Flaw in the Design.* The Washington Post. https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/ Accessed on 1 March 2024.
[48] ULLA-MARI TUOMINEN. 2021. Establishing a framework for a European digital identity. (2021).
[49] Maaike van Leuken (TNO Group). 2023. *SSI Standardisation Overview.* https://tno-ssi-lab.github.io/standardisation-overview/docs.html Accessed on 7 March 2024.
[50] Megne Vangen11, Arn Wassmann12, and Sandro Wefel. 2023. EU Cross-border and OOTS for HEI/Edu Workflows and Infrastructures with Interoperability, Standards, and Security. *Proceedings of European University* 95 (2023), 266–284.
[51] Yuejia Xiang, Ziheng Zhang, Jiaoyan Chen, Xi Chen, Zhenxi Lin, and Yefeng Zheng. 2021. OntoEA: Ontology-guided entity alignment via joint knowledge graph embedding. *arXiv preprint arXiv:2105.07688* (2021).
[52] K. Yasuda, M. Jones, and T. Lodderstedt. 28 November 2023. *Self-Issued OpenID Provider v2.* https://openid.net/specs/openid-connect-self-issued-v2-1_0.html Accessed on 3 March 2024.
[53] Kaisheng Zeng, Chengjiang Li, Lei Hou, Juanzi Li, and Ling Feng. 2021. A comprehensive survey of entity alignment for knowledge graphs. *AI Open* 2 (2021), 1–13.

Received 11 May 2024; accepted 2 June 2024