Trusted and Secure Self-Sovereign Identity framework

Vaios Bolgouras*
Anna Angelogianni*
vbolgouras@unipi.gr
annaaggelogianni@ssl-unipi.gr
Department of Digital Systems,
University of Piraeus
Piraeus, Greece

Ilias Politis
Department of Digital Systems,
University of Piraeus
Piraeus, Greece

Christos Xenakis
Department of Digital Systems,
University of Piraeus
Piraeus, Greece

ABSTRACT

Digitization, in terms of online services, work environment and other day-to-day procedures, has lead to the wide adoption and use of the respective digital identities. Users utilize their digital personas and their corresponding attributes on a daily basis, in order to gain access to resources and services. This is achieved through the use of numerous identity management schemes, which often suffer from multiple vulnerabilities and are susceptible to threats. This results in the compromise of user privacy and data security. In the recent years, new technologies related to identity management, like the Self-Sovereign Identity (SSI) and eIDAS concepts, are employed to mitigate these issues. This paper presents an architecture that combines state-of-the-art technologies regarding identity management, authentication and secure storage. More specifically, the proposed framework utilizes IOTA-based SSI, the eIDAS framework, FIDO protocol and Trusted Execution Environment (TEE), resulting in a trusted and secure identity management framework. Our solution is thoroughly presented via scenarios, showcasing its robustness and how well it copes in relation to our threat model.

CCS CONCEPTS

• **Networks** → Network reliability.

KEYWORDS

Identity Management, eIDAS, SSI, FIDO, IOTA

ACM Reference Format:
Vaios Bolgouras, Anna Angelogianni, Ilias Politis, and Christos Xenakis. 2022. Trusted and Secure Self-Sovereign Identity framework. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3538969.3544436

*Both authors contributed equally to this research.

ARES 2022, August 23–26, 2022, Vienna, Austria

ACM ISBN 978-1-4503-9670-7/22/08…$15.00
https://doi.org/10.1145/3538969.3544436

1 INTRODUCTION

Digital transformation, especially in government services, is rapidly evolving. This rapid shift towards digitization has been greatly facilitated by the COVID-19 pandemic. A large amount of individuals nowadays are becoming more experienced with digital technologies and as a result, they turn more willingly to digital services in order to perform daily tasks, such as acquiring signed documents, certifications, etc. Current infrastructures may be usable but cannot cover the demanding needs of cyber security and protection of highly sensitive personal data. In the past year alone, there was a significant rise of cyber crime. According to the Forbes, in 2021 the most targeted sectors worldwide were the Education/Research sector and Government/Military sector, which handle crucial data, while credential theft was the third most common type of attack [Forbes 2022]. The main reason behind these occurrences is the centralised structures utilized to perform processes related to Identity Management. Researchers have already proposed techniques to mitigate this threat, the most promising among them being the concept of Self Sovereign Identity (SSI) [Preukschat and Reed 2021].

It is crucial to utilize novel technologies, like SSI, in order to facilitate citizen's lives but also provide a strong level of security assurance and privacy protection. Several Identity Management and Authentication frameworks have been proposed throughout the years. Nevertheless, these solutions are not flawless, but are susceptible to one or more of the following: i) they require to place too much trust on a third party or ii) they require users to remember different passwords for multiple services. Through SSI, there is no more need for the utilization of a third party, but the problem of using passwords still remains while at the same time the issue of trust among entities arises. The solution to these last challenges is given by the eIDAS framework [Cuijpers and Schroers 2014], which forms a network where trust is established among all participating entities. There have already been some efforts towards this end, combining SSI and eIDAS concepts ([Kavassalis 2020], [Abraham et al. 2018], [Nóbrega Gonçalves et al. 2020]), but compared to those this paper proposes a complete architecture, providing an extra layer of security via the addition of the Fast IDentity Online (FIDO) protocol and the utilization of a Trusted Execution Environment (TEE) to safely store credentials. Moreover, the distributed ledger infrastructure in our solution is based on Tangle technology - the IOTA framework, providing interoperability with the European Blockchain Services Infrastructure (EBSI) [1].

The aim of this paper is to provide a hybrid authentication scheme combining the advantages of SSI, eIDAS, FIDO and TEE, to

[1]https://www.iota.org/solutions/ebsi

empower users with a secure, user friendly and seamless authentication and authorisation solution based on eDIDs - Decentralized IDentifiers (DIDs) stemming from a corresponding eID that a user acquires through the eIDAS framework - and Verifiable Claims (VCs). More specifically, through the SSI approach users are given the ability to manage their own identity, having full control over its attributes and with whom they share them, without relying on centralised authorities. This is achieved through the DIDs accompanied by VCs, which represent certain attributes of the subject's identity. VCs can be issued at any time by the corresponding organisation, as required by the user. The Achilles' heel of SSI is that it is not easily scalable for cross-border use, as it is highly likely that the issuers of the DIDs and VCs in one country are not considered trusted entities in another. eIDAS on the other hand is a scalable solution that operates across EU countries. It provides a trusted way for service providers to authenticate citizens through their eID, who in turn can identify themselves to third parties and digitally sign documents via an official channel that complies with the corresponding regulations. SSI and eIDAS concepts complement each other and offer the best of both worlds, trust provided by a centralised solution and ensuring privacy by giving full control of the personal data to the data subject through decentralized means. Merging the citizens' DID with their corresponding eID is achieved by sharing a common Pk/Sk key pair, thus allowing them to use an internationally recognised digital identity along with the ability to issue VCs, for example a vaccination certificate, that can be accepted and verified in multiple countries. The FIDO protocol and the TEE offer an additional layer of security, ensuring that even if identity theft has taken place, personal data will not be compromised and unauthorized access to resources will not be allowed.

The paper is structured as follows: In Section 2, we discuss the proposed framework, providing a problem statement along with a threat model and the architecture description. Section 3 describes certain scenarios and demonstrates how the proposed architecture will function. Finally, Section 4 concludes this paper.

2 PROPOSED FRAMEWORK

In this section our framework's novel architecture is presented. The innovative combination of state-of-the-art technologies - more specifically SSI, eIDAS and FIDO - is analysed, along with its components and functionalities.

2.1 Problem Statement

Our approach aims to resolve a plethora of issues. Firstly, centralised solutions are proven to be ineffective since they constitute a *single point-of-failure*. Solutions that are based on the notion of blockchain, are able to provide high *availability, scalability, transparency* as well as *traceability*. Nevertheless, organisations cannot entirely trust the identities provided by the blockchain, which may not involve *certified authorities* or universally employed identities. On the other hand, a cross-boarder, thus approved scheme, such as the eIDas cannot guarantee user's *privacy protection*, since the information is shared across the parties involved.

Both credentials and certifications should be managed in a provable secure, thus usable authentication scheme which utilises internationally approved *standards* (i.e., FIDO) and conforms to certain *regulations and legislative frameworks* (i.e., GDPR). Lastly, is is crucial for the proposed framework to *support all types of devices*, thus provide *extensibility*.

2.2 Threat Model

We have considered various threats against our model, which we aim to overcome with our proposed architecture. These threats may be grouped to the following categories: i) Threats against Confidentiality, ii) Threats against Integrity, iii) Threats against Availability, iv) Threats against Non-Repudiation.

The **User Device** is the most eminent link in terms of security in our architecture. It is interconnected with all the other components and in case it gets compromised, actions related to identity theft could take place. This would negatively impact on both the confidentiality and integrity of the system. This threat is mitigated by utilizing the TEE environment for storing sensitive data, combined with the use of FIDO for user authentication to entities that could potentially share personal data.

The numerous **Organizations** that issue VCs, along with the **eIDAS** infrastructure, may be targeted through impersonation attacks aiming to extract personal data concerning users with compromised credentials. The realization of such a threat would deliver a significant blow to the confidentiality of the system. To avoid such adversities, authentication via the FIDO protocol is required.

Potential compromise of the **Distributed Ledger** could mean the disruption of the information flow towards and from the verifiers and issuers respectively. Moreover, resting data could be manipulated and edited without authorization. Both availability and non-repudiation would be severely affected by such an occurrence. Our proposed architecture is fortified against this kind of threats, as the Distributed Ledger resides in multiple entities across the IOTA network, mitigating threats that could cause a single point of failure.

2.3 Architecture

An overview of our proposed architecture can be found in Figure 1. Below there is a description and analysis regarding the purpose and functionalities of each entity and its components.

(1) *eIDas*: The eIDAS framework includes functionalities related to the management of the eIDs, the corresponding public and private key pairs, along with FIDO server capabilities in order to be able to authenticate users via the respective method.
The **eIDAS-Node** can either request or provide cross-border authentication, allowing mutual recognition of electronic identities across multiple countries. It essentially acts as a gateway through which users from abroad, who attempt to access foreign services, can authenticate. For example, a user from country B can access services from providers that reside on country A by communicating the required data via the corresponding eIDAS-Nodes.
The **FIDO Server** is utilized for cross-border communication as well, providing an extra layer of security in cases where a user request to send information abroad takes place. More specifically, user authentication via FIDO is required prior the exchange of data between two eIDAS-Nodes.

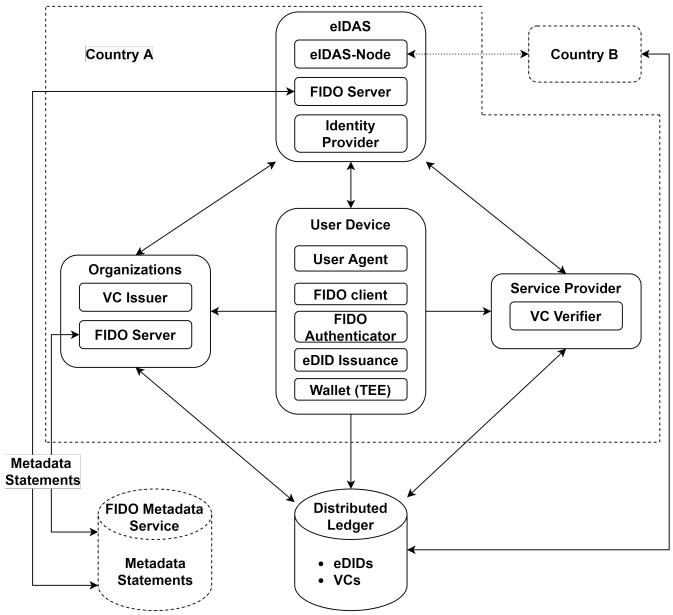

Figure 1: Proposed Architecture

The **Identity Provider** (IdP), as the name suggests, is responsible for the issuance of a key pair and the corresponding eID for individual citizens. IdPs may also be asked to share information regarding the validity of an identity presented to organizations, for the purpose of VC issuance.

(2) *User Device:* The device of the user is the center-point of our architecture, which is essential in order to achieve self sovereignty for the end user. The user device is involved in all actions regarding authentication, authorization, issuance and handling of credentials.
The **User Agent** is the tool (for example an Internet browser, standalone applications, etc.) via which the user access other entities and services. More specifically, service providers can be accessed to satisfy the user's needs, the eIDAS infrastructure in order to acquire an identity and the corresponding key pair, along with multiple organizations regarding the issuance of VCs.
The **FIDO client** is responsible to discover the available authenticators residing on the client side thus, handle the FIDO requests and responses and send them either to the authenticator or to the relying party residing on the respective FIDO server(s). It is essential for the user to authenticate via the FIDO protocol.
The **FIDO authenticator** is responsible to generate the user credentials, meaning the keypair (i.e., a public and a private key) used to sign the challenge sent by the FIDO Server. It can be either an external device (i.e., USB token) or an embedded module to the user device (i.e., TEE or TPM).
Moreover, of utmost importance is the module responsible for the **issuance of the eDID**, the unique user Decentralized IDentifier, which is based on the corresponding user eID stemming from the eIDAS infrastructure. The creation of the eDID is based on the utilization of the same Pk/Sk key pair used for the eID. This way, the users will be able to perform numerous actions with their decentralized identifier, like signing documents, and enjoy the trustworthiness that the eIDAS infrastructure offers. This eDID will be utilized for user identification, as well as an anchor to the respective VCs that will be issued for this eDID from multiple organizations. The eDID, along with the VCs that refer to it are logged on the IOTA distributed ledger.
The **wallet** that resides on the user device is essential for the secure storage of the identity credentials (eID, eDID) and the corresponding VCs. To ensure the integrity and proper safeguarding of the data stored in the wallet, a TEE module is employed. This TEE can act as a **FIDO authenticator** as well, for cases where users do not possess an external device [FIDO Alliance 2021a]. The user does not have to perform queries on the distributed ledger in order to retrieve essential information, which would be costly in terms of time and resources. Instead, the information is readily available for use on the device.

(3) *Organizations*: The organizations are entities, like universities and other certifications authorities, which are in possession of information and data regarding individuals that are/have been associated with them.
The main purpose of these entities is to **issue VCs**, which are required to be presented by the users to service providers, in order to prove that they possess a certain identity attribute. Users who make an inquiry for a VC issuance have to also be authenticated via the FIDO protocol - an extra measure to mitigate the threat of stolen keys and identity theft.

(4) *Service Providers (SPs)*: Users try to access SPs according to their needs. As the name hints, SPs offer certain services, which most of the time are available for someone only when specific requirements regarding the corresponding identity attributes are met. To that end, the users utilize VCs. Upon the receival of a VC, the SP **verifies** its authenticity, applicability and validity. Once the aforementioned verification procedure has taken place, the users gain access to the resources they need.

(5) *IOTA Distributed Ledger*: Facilitates the use of the SSI infrastructure. Provides a secure and distributed architecture for storing eDIDs and VCs, along with giving the ability to any party with interest to verify the validity of this data.

(6) *FIDO Metadata Service* The Metadata Statements, included in the Metadata Service provide the "Trust Anchor", required to validate the authenticator [FIDO Alliance 2021b]. These Metadata Statements may further include information regarding the characteristics of the authenticator.

3 SCENARIOS

In this section certain scenarios are presented in order to facilitate the understanding of the processes and procedures that take place in the presented architecture, through real-life instances. The actions that take place are described using steps.

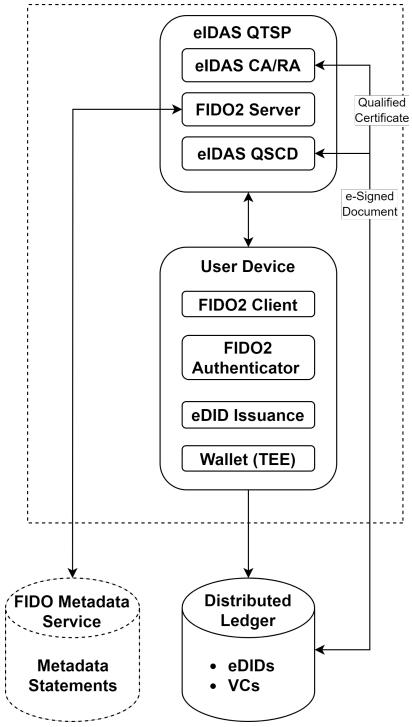

Figure 2: Case B-oriented components interaction

3.1 Case A

Firstly, we analyze the case where the user uses FIDO for authentication purposes, along with some fundamental scenarios that concern obtaining credentials and commence utilizing the proposed framework.

3.1.1 New user - eDID formulation. The user device is responsible for the creation of an eIDAS-derived DID, denoted as eDID, which can be potentially utilized for identification purposes and anchoring VCs to itself. It is considered that the user has already registered the FIDO authenticator to the Identity Provider.

Step 1: The user authenticates to the Identity Provider and acquires an eID identifier from the eIDAS framework, along with the corresponding Pk/Sk key pair. These keys are essential in the processes related to digitally signing and verifying documents, authorizing third parties, etc.

Step 2: A DID stemming from the key pair that the user acquired in the last step is created. The Pk is signed by the Sk, via a predetermined encryption algorithm (RSA, DSA, etc.).

Step 3: The eDID has been created, so it is safely stored on the Wallet that resides on the TEE environment, while at the same time it is logged on the distributed ledger.

3.1.2 Issuance of a new VC. A user who has already produced an eDID and wants to access an online service offered by an SP, is asked to prove that meets certain requirements in relation to her identity attributes. Therefore, the issuance of a corresponding VC is necessary.

Again, we consider that the user has registered the FIDO authenticator to the Organisation prior to the issuance.

Step 2: The user makes a query for the issuance of a VC to the appropriate organization, using her eDID.

Step 2: The organization, in order to authenticate the user and mitigate the threat of a stolen identity, proceeds to authenticate the user via FIDO. In the event that further information on the identification and validity of the user's eDID is required, the relevant eID is examined using the eIDAS infrastructure.

Step 3: Upon the successful FIDO authentication, the organization issues the VC.

Step 4: The user receives the requested VC and stores it to her wallet, while at the same time the VC issuer communicates the newly issued VC to the distributed ledger.

3.1.3 Access a domestic SP. A user, who is already in possession of her eDID and has obtained the required VCs request access to an online service offered by an SP that resides in the same country.

Step 1: The user requests access to the online services, and the SP responds with the requirements that should be met by a user's identity attributes.

Step 2: The user retrieves from the wallet the corresponding VCs that prove possession of the required identity attributes.

Step 3: The SP receives the requested VC(s) and proceeds to the verification process. More specifically, it performs a check via the distributed ledger entries, regarding the validity of the VC and the eDID that it is connected to. In case that further information is needed regarding the identification and validity of the user's eDID, the corresponding eID is being reviewed, utilizing the eIDAS infrastructure.

Step 4: Once the verification process has successfully concluded, the user is granted access to the SP's online services.

3.1.4 Authentication using FIDO. In order to provide an added level of security regarding the credential management, the proposed architecture supports the FIDO Authentication scheme both in the communication between the User and the Identity provider as well as the communication between the User and the Organisation.

We consider that the user has registered the FIDO authenticator to the Identity Provider prior to the authentication.

Step 1: The FIDO Server, residing either in the Identity Provider or in the Organisation side, sends a randomly generated challenge to the FIDO Client, residing in the User Device.

Step 2: The FIDO Client locates and forwards the challenge to the FIDO Authenticator.

Step 3: The FIDO Authenticator upon receiving the challenge, signs it using the authentication private key and returns back to the FIDO Client the signed challenge.

Step 4: The FIDO Client receives the information from the Authenticator and sends it to the FIDO Server.

Step 5: Lastly, the FIDO Server receives and verifies the challenge using the user's authentication public key, previously acquired during the registration. The FIDO Server can further communicate with the Metadata Service in order to verify the security characteristics of the FIDO Authenticator.

3.1.5 Cross-border utilization of SPs. A user requires to access an SP that resides in a different country. In this case, that SP needs to

verify that the eDID utilized by the user is derived from a valid eID. The issue to overcome is that there is no direct connection to the SP and the eIDAS-Node of the user's country. In order to resolve this:

Step 1: The user makes an inquiry to its corresponding eIDAS-Node, requesting that it shares the required information with the eIDAS-Node that resides in the SP's country
Step 2: The eIDAS-Node authenticates the user via FIDO
Step 3: Upon successful authentication, the information is exchanged between the two eIDAS-Nodes and the user will be able to access the cross-border services from the corresponding SP.

3.2 Case B

Apart from the FIDO being used in a Federated eIDas node for cross border identification, FIDO2 has been proposed for the case of Qualified Trust Service Provider (QTSP), as defined in the eIDAS regulation [FIDO Alliance 2020]. Figure 2 provides an overview of the components that will be used in the scenarios described below.

3.2.1 Certificate Generation in QTSP. A user who has already produced an eDID and wants to issue a Qualified Certificate, is asked to prove that meets certain requirements in relation to her identity attributes, in order to issue a certificate. The Certification Authority could be either part of the QTSP or an external entity.

Step 1: The user is identified by the QTSP Registration Authority (RA) and if the identification is successfully completed, the QTSP's Certification Authority (CA) issues a Qualified Certificate. The information provided by the user for the identification, during the certificate application, is stored in the QTSP database.
Step 2: The Qualified Signature Creation Device (QSCD) is requested to generate the Qualified Certificate key-pair by the QTSP CA.
Step 3: The CA signs the Qualified Certificate using the generated public key.

3.2.2 FIDO2 Credential Registration to the QTSP. In order to provide an added level of security regarding the authentication of the user to the QTSP, the proposed architecture supports the FIDO2 scheme in the communication between the User and the QTSP.

Step 1: The FIDO2 Server residing in the QTSP sends a randomly generated challenge to the FIDO Client residing in the User Device.
Step 2: The FIDO Client locates and forwards the challenge to the FIDO Authenticator.
Step 3: The FIDO Authenticator upon receiving the challenge, generates a new keypair (i.e., public and private user authentication key) dedicated to the specific QTSP and signs the challenge along with the user authentication public key using the attestation private key. Afterwards it returns back to the FIDO Client the signed information.
Step 4: The FIDO Client receives the information from the Authenticator and sends it to the FIDO Server.
Step 5: Lastly, the FIDO Server receives and verifies the challenge using the attestation public key, which can be retrieved from the Metadata Service. The FIDO2 credentials at the server side are cryptographically bound/associated with the Qualified Certificate and key-pair in the QSCD.

FIDO2 usage is dual in this scheme. First it provides strong authentication of the user to the QTSP. Secondly, it is used for unlocking the user's key in the QSCD.

3.2.3 Qualified Electronic Signature. A user that has already registered a FIDO2 Authenticator to the FIDO2 Server of the QTSP invokes the QTSP to sign a document.

Step 1: The FIDO2 Authenticator, residing in the user device is authenticated to the FIDO Server, residing in the QTSP, following the steps defined in subsection 3.4 in order to access the services offered by the QTSP.
Step 2: The user uploads the Document To Be Signed (Doc-TBS) to the QTSP Server Signing Application (SSA).
Step 3: The QTSP Server retrieves the Qualified Certificate (from the QTSP database) and the associated private key in the QSCD and then invokes the FIDO2 Server to generate a new challenge. This challenge includes a unique identifier of the document to-be-signed (i.e., a hash).
Step 4: The FIDO2 Server sends this challenge to the FIDO2 Client, which forwards it to the FIDO2 Authenticator.
Step 5: The FIDO2 Authenticator signs the challenge using the user authentication private key and afterwards it sends the signed challenge to the FIDO2 Client, which forwards it to the FIDO2 Server
Step 6: The signed challenge it is sent from the FIDO2 Server to the QTSP in order for the latter to validate it. If the challenge is indeed valid, then the QTSP permits the QSCD to unlock the user's private key residing within the QSCD, in order to sign the document.

4 CONCLUSION

In this paper we propose a framework based on the novel combination of SSI, eIDAS, FIDO and TEE technologies. This framework empowers the users, giving them complete control over their identity, along with seamless functionality across online services that may reside in a different country. Security and trusts are essential and constitute the main pillars around which we built the corresponding architecture. This work can find application in a plethora of real-life use cases and paves the way for further research and implementation of the presented components.

ACKNOWLEDGMENTS

- INCOGNITO (H2020-MSCA-RISE-2018, GA 824015)
- ERATOSTHENES (SU-DS02-2020, GA 101020416)

REFERENCES

Andreas Abraham, Kevin Theuermann, and Emanuel Kirchengast. 2018. Qualified eID Derivation Into a Distributed Ledger Based IdM System. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE).* 1406–1412. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00195

CMKC Cuijpers and Jessica Schroers. 2014. eIDAS as guideline for the development of a pan European eID framework in FutureID. (2014).

FIDO Alliance. 2020. FIDO Alliance White Paper: Using FIDO with eIDAS Services. https://media.fidoalliance.org/wp-content/uploads/2020/06/FIDO_Using-FIDO-with-eIDAS-Services-White-Paper.pdf Last accessed 9 May 2022.

FIDO Alliance. 2021a. FIDO Authenticator Allowed Restricted Operating Environments List. https://fidoalliance.org/specs/fido-security-requirements-v1.0-fd-20170524/fido-authenticator-allowed-restricted-operating-environments-list_20170524.html Last accessed 9 May 2022.

FIDO Alliance. 2021b. FIDO Metadata Service. https://fidoalliance.org/specs/mds/fido-metadata-service-v3.0-ps-20210518.html Last accessed 9 May 2022.

Forbes. 2022. Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats. https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/

Petros Kavassalis. 2020. Designing an academic electronic identity management system for student mobility using eIDAS eID and Self-Sovereign Identity technologies. *EUNIS* (2020).

Sérgio Manuel Nóbrega Gonçalves, Alessandro Tomasi, Andrea Bisegna, Giulio Pellizzari, and Silvio Ranise. 2020. Verifiable Contracting. In *European Symposium on Research in Computer Security*. Springer, 133–144.

Alex Preukschat and Drummond Reed. 2021. *Self-sovereign identity*. Manning Publications.