VDE SPEC

Decentralized identity management (DIM) based on Self-Sovereign identity (SSI) – concept, technologies and application in a microgrid

VDE SPEC 90026 V1.0 (en)

VDE

Foreword

Publication date of this VDE SPEC: 21.08.2026.

No draft has been published for the present VDE SPEC prior to publication.

This VDE SPEC resulted from the work of a project group between the authors as stated below.

This VDE SPEC was developed according to the VDE SPEC procedure. VDE SPEC 90026 V.1 (en) has been developed in a project group and it cannot be granted that all possibly interested parties could have been involved. However, a proposal for interaction for public interaction was made by means of according to the VDE procedure and all parties – possibly not involved at this point – were asked to participate in the process.

This VDE SPEC is not part of the VDE set of regulations or the German set of standards. In particular, this VDE SPEC is not a technical rule within the meaning of Section 49 EnWG.

The authors of this VDE SPEC are:

- Prof. Dr.- Ing. Debora Coll-Mayor, Reutlingen University
- Prof. Dr.-Ing. Antonio Notholt, Reutlingen University
- Dr. Thomas Brenner, OLI Systems GmbH
- Dr. Brigit Haller, OLI Systems GmbH
- Athina Savvidis, VDE DKE

Despite great efforts to ensure the correctness, reliability and precision of technical and non-technical descriptions, the VDE SPEC project group can neither explicitly nor implicitly guarantee the correctness of the document. This document is used in the knowledge that the VDE SPEC project group cannot be made liable for damage or loss of any kind. The application of the present VDE SPEC does not release the user from responsibility for their own actions and is therefore at their own risk.

In the course of the manufacture and / or introduction of products into the European internal market, the manufacturer shall carry out a risk analysis in order to first determine which risks the product may entail. After performing the risk analysis, he evaluates these risks and, if necessary, takes suitable measures to effectively eliminate or minimize the risks (risk assessment). The present VDE SPEC does not release the user from this responsibility.

Links to third-party websites do not constitute an approval of their content on the part of VDE. VDE is not responsible for the availability or the content of these websites. The establishment of a link to these websites is at the user's own risk.

Attention is drawn to the possibility that some elements of this document may affect patent rights. VDE, DKE, and DIN are not responsible for identifying any or all of the related patent rights.

Executive Summary

This VDE SPC outlines key findings, including the requirements profile for Distributed Identity Management (DIM), the overarching DIM concept and practical implementation strategies for the energy sector. It also covers laboratory testing procedures and documentation, including test reports and insights gained from these evaluations.

The VDE SPC is structured as follows: It begins with a general introduction to the issue of device identities in the energy industry. Then it presents the status of DIM for the energy sector (see Section 5) and provides an overview of SSI frameworks and DIM technologies, as well as comparing their suitability for energy applications (see Section 6). The DIM concept developed is defined for a specific energy application: 'A microgrid'. Section 7 presents this SSI-based DIM for implementing distributed identity management for a microgrid. The developed concept was implemented, tested and verified by simulating it in a hardware-in-the-loop laboratory system and demonstrating it in an isolated microgrid. The results of the test phase and laboratory tests can be found in Section 8. Section 9 contains a discussion of the results, focusing on security, data protection and compliance with legal requirements in the presented test case. This documentation concludes in Section 10, which provides suggestions on how the work can be developed further in future.

Contents

List of figures

List of tables

Introduction

In the digital age, the management of personal and device identities has become a critical concern. Traditional centralized identity management systems, where a single authority stores and controls user data, are increasingly challenged with security vulnerabilities, privacy concerns, lack of user autonomy and interoperability issues. Contrary to centralized identity systems, Distributed Identity Management (DIM) offers a transformative approach by decentralizing control processes and giving individuals sovereignty over their own identity or device data. Furthermore, DIM offers solutions to the main challenges faced by centralized systems: (a) While centralized databases are the main targets of cyberattacks and their breaches can lead to massive leaks of confidential information, DIM systems mitigate this risk by eliminating single points of failure, making it significantly harder for attackers to compromise large amounts of data at once [1]; (b) While in centralized models, users often have limited insight into how their data is used or shared, DIM empowers users to control their personal information, deciding what data to share and with whom, thereby enhancing privacy [2]; (c) While in centralized managed systems enabling user consent and data protection[1] requires implementing redundant and complicated processes to ensure that all the users are aware and consent the use of their data, DIM aligns with those requirements by design, ensuring that users have control over their personal data and; (d) As centralized systems are faced with interoperability issues while users engaging with multiple services, DIM systems facilitate identities to be recognized and verified across different platforms without redundant registrations. For all these reasons, DIM offers a solution to the main challenges faced by centralized identity management systems providing a reliable and secure solution. Additionally, many DIM solutions are based on Distributed Ledger Technologies (DLT) such as blockchain, which adds transparent and tamper-proof records of identity transactions, fostering trust between users and service providers [4].

In implementing a DIM framework, different concepts can be used, in this work the solution proposed is based on Self Sovereign Identities (SSI). The advantage of SSI compared with other DIM concepts is that in SSI, individuals or organizations have sole ownership of their digital and analog identities, and therefore, control how their data is shared and used. As in other DIM concepts, using SSI eliminates reliance on central authorities [5] and provides the infrastructure necessary for implementing distributed identity systems [6]. SSI requires a new type of identifier called Decentralized Identifier (DID). This DID developed by the World Wide Web Consortium (W3C), enables verifiable and decentralized digital identity and is designed to function without a centralized registration authority [7]. Another component of SSI is the verifiable credentials, which are standardized by the W3C. These verifiable credentials are cryptographically secure digital documents that assert claims about an entity, enabling secure, privacy-preserving sharing of attestations (like driver's licenses or diplomas) in a digital format that can be cryptographically verified [8].

Summarizing, DIM represents a significant shift towards more secure and user-centric identity solutions. As digital interactions continue to expand, adopting distributed identity frameworks would lead to more secure and efficient identity verification processes. Furthermore, when those DIM frameworks are coupled with SSI, they present clear advantages in improved user control and ownership, enhanced privacy and security, interoperability and increased trustworthiness. Even if the advancements in SSI have led to different DIM potential solutions in various sectors [9], there is still limited application of DIM in the energy sector. Previous works focus mainly on implementing or developing secured networks for identity management, rather than integrating them in energy use cases. This work takes a step forward and aims to develop, implement and test a SSI based DIM system for energy sharing in a microgrid, one of the most popular use cases when using DLTs in the energy sector [10].

1 Scope

This specification aims to provide a comprehensive overview of the current state of Decentralized Identity Management (DIM) technologies with a focus on their applicability in the energy sector. It includes a detailed presentation of Self-Sovereign Identity (SSI) frameworks and associated DIM technologies. A comparative analysis is conducted to evaluate the suitability of leading SSI frameworks for energy-related use cases, with the objective of identifying the most appropriate framework for implementation. Based on this analysis, a model for SSI-based DIM is developed for application in a microgrid environment. The proposed model is validated through simulation within a hardware-in-the-loop (HIL) laboratory system and demonstrated in an islanded microgrid scenario. Furthermore, this specification includes a discussion of the security, privacy, and regulatory compliance aspects relevant to the developed use case.

---

1 Data protection requirements such as the defined by the General Data Protection Regulation (GDPR) [3]

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

3.1
advanced metering infrastructures
AMI

an integrated system of smart meters, communication networks, and data management systems that enables two-way communication between utilities and customers and supports the collection, storage, analysis, and presentation of energy usage data. AMI refers to systems that measure, collect, analyse and control energy distribution and usage, with the help of advanced energy distribution automation devices such as distribution network monitoring and controlling devices, network switching devices, load/source-shedding devices, electricity meters, gas meters and/or water meters, through various communication media on request or on a pre-defined schedule. This infrastructure includes hardware, software, communications, energy distribution-associated systems, customer-associated systems and meter data management (MDM) software.

The bidirectional communication network between the smart grid and metering devices and business systems allows collection and distribution of information to customers, suppliers, distribution network companies, utility companies and service providers. This enables these businesses to either participate in, or provide, demand response solutions, products and services.

[SOURCE: International Electrotechnical Commission (IEC). (n.d.). Advanced metering infrastructure. Retrieved June 9, 2026, from https://syc-se.iec.ch/iec-63097-smart-energy-roadmap/advanced-metering-infrastructure/]

3.2
Distributed Identify Management
DIM

an approach to managing digital identities in which identifiers and credentials are created, controlled, and verified without reliance on centralized authorities, using decentralized identifiers (DIDs) and verifiable credentials

[SOURCE: W3C Decentralized Identifiers (DIDs) v1.1]

3.3
decentralized identifier
DID

identifier that is issued or managed in a decentralized system and designed to be unique within a context

Note 1 to entry: Decentralized identifiers are used in systems that do not rely on central registration authorities.

[SOURCE: ISO 22739:2024]

3.4
distributed ledger

ledger that is shared across a set of distributed ledger technology (DLT) nodes and synchronized between the DLT nodes using a consensus mechanism

[SOURCE: ISO 22739:2024]

3.5
Self Sovereign Identities
SSI

enables individuals and organizations to own, control, and share their digital identities without the involvement of intermediaries

3.6
Hardware-in-the-loop
HIL
testing method in which real hardware is integrated into a real-time simulation of a system, enabling the hardware to be tested under realistic, simulated conditions

[SOURCE: IEEE Std 2004-2025]

3.7
Web-of-trust
WoT
a decentralized trust model in which users authenticate each other's public keys through mutual certification (digital signatures), rather than relying on a central certification authority

[SOURCE: Walfield, N. H. (2022). OpenPGP Web of Trust (Internet-Draft). IETF.]

3.8
Microgrid Operator
MO
party responsible for the safe and reliable operation of a microgrid

[SOURCE: IEV ref 617-02-19]

3.9
remote procedure call
RPC
communication paradigm that enables a program to execute a procedure on a remote system as if it were a local function call, abstracting the underlying network communication

[SOURCE: Tay, B. H., & Ananda, A. L. (1990). A survey of remote procedure calls. *ACM SIGOPS Operating Systems Review*, *24*(3), 68-79.]

3.10
Distribution System Operator
DSO
party operating a distribution system

[SOURCE: IEV ref 617-02-10]

3.11
Zero Knowledge Proof
ZKP
cryptographic protocol that enables a prover to convince a verifier that a statement is true without revealing any information beyond the validity of that statement

[SOURCE: NISTIR 8301]

3.12
Internet of Things
IoT
infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical world and virtual world

[SOURCE: ISO/IEC 20924:2024]

3.13
Application Programming Interface
API
a system access point or library function that is accessible from application programs to provide well-defined functionality

[SOURCE: NISTIR.5153]

4 Abbreviations

Abbreviations	Meaning
AMI	advanced metering infrastructures
API	Application Programming Interface
DID	Decentralized Identifier
DIM	Distributed Identity Management
DLT	Distributed Ledger Technologies
DSO	Distribution System Operator
GDPR	General Data Protection Regulation
HIL	hardware-in-the-loop
HW	hardware device
IoT	Internet of Things
KYC	know your customer
MO	Microgrid Operator
OEM	Original Equipment Manufacturers
RPC	remote procedure call
SDK	Software Development Kit
SSI	Self Sovereign Identities
W3C	World Wide Web Consortium
WoT	Web-of-Trust
ZKP	Zero Knowledge Proof

5 Distributed Identity Management in the Energy Sector

5.1 Introduction

The energy sector is undergoing a rapid digital transformation, driven by the integration of new distributed energy sources, smart grids technologies, new sector coupling concepts or advanced metering infrastructures (AMI). These technological advancements have paved the way for the decentralization of the energy system and created the need for secure and efficient identity management systems. This identity management has become critical to enable the identification and access to information of the different participants within energy ecosystems. At the same time, traditional centralized identity management approaches for electrical devices are increasingly seen as inadequate for the evolving needs of decentralized energy systems [11], while DIM systems leveraging on technologies such as blockchain and decentralized identifiers (DIDs) are gaining attention over the years [12]. In this Section, the current state of the art of DIM in the energy sector will be reviewed, highlighting its significance, challenges, and emerging trends.

5.2 Short Bibliographic Analysis

Overall, DIM refers to a system in which identity verification and authentication processes are decentralized, allowing individuals or entities to control their identity information without relying on a central authority [9], [13]. In contrast to traditional centralized models, where a single entity or institution manages user identities, DIM leverages on technologies such as cryptographic techniques, peer-to-peer networks or blockchain technology to enable a trustless and secure system applications [14], [15]. Different works are dealing with the use of blockchain for ensuring trust and increasing security while managing identities. For example, Ref. [13] develops an identity management model based on certificateless encryption algorithm of blockchain to enable users have full control over their identity data. The results of the model verification showed that it has fast information response ability compared to a centralized identity management system and an average delay of 0.4 seconds. Taking a step forward, Ref. [16] proposes a network model called “Trustful” based on public key infrastructure and signature

verification to build trust among users in a decentralized network for identity management. This works on a “Web-of-Trust” (WoT) network”[2] model that allows the network participants to verify attributes about other users through a trusted network.

SSI, the core component of the DIM framework, enables individuals and organizations to own, control, and share their digital identities without the involvement of intermediaries [17], [18], [19]. For example, in P2P energy trading, where participants exchange energy directly, SSI allows for the secure authentication of prosumers (sellers) and consumers (buyers) [15], [20]. The development of SSI-based DIMs is still in an early stage, however several solutions have been already proposed. For instance, Ref. [21] designed the workflows and implementation of SSI based solution that enables zero-trust authentication for resources sharing and acquisition. Similarly, Ref. [15] proposes a blockchain-based SSI and authentication mechanisms to prevent identity theft and masquerading in a distributed smart grid. In this case, a Merkle tree architecture was used for identification and authentication of IoT devices.

Interesting applications of those ideas can be found for example in the use of SSI for renewable energy certification [22]. In all these works SSI has shown a main benefit by mitigating risks associated with identity fraud and unauthorized access to energy networks, while also improving transaction transparency and trust between participants, this fact has been analysed in [23]. The use of Distributed Ledger Technology (DLT), such as blockchain, when implementing SSIs provides a robust platform and allows for the immutable recording of identity data, ensuring that each transaction is securely logged and can be audited when necessary [12], [17]. Researchers have explored the use of blockchain-based identity systems for different applications such as smart contracts, grid management or energy markets, a survey can be found in [17]. An interesting analysis is provided in [14], where the relationship and architecture of DLT-based DIM is introduced and then three SSI technologies (uPort, ShoCard, and Sovrin) are evaluated. This evaluation was based on how those SSI can be applied for identity management using a framework that characterizes the nature of successful identity management schemes.

Despite numerous research works on the development and implementation of SSI based DIM, there is still need for real applications to ensure a seamless integration of this technology in energy use cases.

5.3 Need for standardized protocols and frameworks

One of the major current areas under development in SSI based DIM are related to addressing the challenge of the limited availability of standardized protocols and frameworks [24], [25]. Energy systems are highly heterogeneous, with varying technologies and standards across different regions and markets. For DIM to be effective, it must ensure seamless interoperability between different energy systems and stakeholders. Ongoing efforts by organizations such as the Decentralized Identity Foundation (DIF) and the World Wide Web Consortium (W3C) aim to address these issues by developing standards for decentralized identifiers (DIDs) and verifiable credentials (VCs) [7], [8]. While DIM offers several advantages over traditional models, it also introduces new security and privacy concerns. The decentralized nature of DIM requires robust cryptographic mechanisms to protect against identity theft, data breaches, and unauthorized access. Additionally, the management of cryptographic keys presents a significant challenge, as users must safeguard their private keys to prevent identity loss [23]. Data privacy is also a critical concern in DIM systems [20], [26] and another major current research areas in SSI based DIM.

Although decentralized systems allow for greater user control over personal data, there is a risk of correlation attacks, where adversaries link multiple transactions to infer sensitive information about individuals [17]. Techniques such as zero-knowledge proofs (ZKPs) and homomorphic encryption are being developed to enhance privacy in DIM, allowing users to prove their identities without revealing unnecessary information [14]. The proliferation of IoT devices in the energy sector, such as smart meters and sensors, presents new opportunities for DIM, those have been analysed in [27]. Edge computing, where data processing occurs closer to the source, can be combined with DIM to provide real-time authentication and authorization of devices [28], [29]. This integration enables more efficient energy management and reduces latency in energy transactions.

5.4 Conclusion

This section has presented the state of the art of SSI-based DIM for the energy sector as well as the main research areas at the moment. In conclusion, as energy systems become more decentralized,

---

2 In cryptography, a WoT is a concept for establishing the authenticity of the bond between a public key and its owner. It offers a decentralized alternative to the centralized trust model of a public key infrastructure (PKI), which relies solely on a certificate authority (or a hierarchy thereof).

the adoption of DIM is considered crucial to enable trust and transparency in energy transactions, however still questions in interoperability and data privacy have to be answered and research is needed in applications of this technology in energy use cases.

6 Selecting a Framework for Energy Use Cases

6.1 Introduction

SSI-based DIM solutions must meet certain requirements to be implemented in energy use cases, for example with regard to usability or interoperability. In this section, these requirements will be identified and an overview of selected SSI technologies that can be used in a DIM ecosystem will be presented. Those SSI technologies will be analyzed based on their inherent features, such as high data security, DIDs supports, performance and reliability as well as its applicability in the energy sector and other sectors with similar challenges. At the end of this section, these SSIs will be compared based on their response to the identified requirements and the most suitable one will be selected.

6.2 Requirements Analysis of DIM for Energy Use Cases

The provided requirements analysis considers functional, non-functional, security and compliance related requirement categories. From these categories, only the 10 most important requirements for energy use cases have been selected and presented as follows:

1. **Interoperability**: The selected solution must comply with relevant standards, such as W3C, and allow for verifiable credentials. It must also be able to integrate with existing systems and be interoperable with multiple blockchain networks.
2. **Usability and accessibility**: The user interface of end-user applications must be easy to use, with comprehensive development, integration and customization of SSI tools. This is necessary to enable easy interaction of end users with the platform and support easy integration of other tools in the future.
3. **Developers community ecosystem**: The presence of an active community is of utmost importance as it provides developers with valuable support, resources and innovative ideas needed to develop cutting-edge systems and applications. In addition, established partnerships can also help improve credibility and integration potential.
4. **Decentralization**: The system should be fully decentralized to allow for a unique, tamperproof identity that is not controlled by a central authority. If possible, the process should be automated so that end users who wish to participate in the energy use cases can easily register, receive a DID, and get confirmation for energy exchange.
5. **Scalability**: It is necessary to have a platform that is scalable and allows access to data so that a large volume of devices can be identified in a few seconds (preferably nanoseconds).
6. **Performance and reliability**: The platform must always be available and minimize downtime disruptions, and ensure reliable performance under adverse conditions. So that secure communication and identification can be established between all participants within the platform at all times.
7. **Flexibility and extensibility**: To meet the specific needs and requirements of stakeholders, as well as to support diverse future use cases, the technology must allow for customization. This means that it must be dynamic and allow for new use case requirements to be easily integrated.
8. **Cost-effectiveness**: To ensure effective application of the use case scenario in a real-world energy exchange, it is necessary to ensure cost-effective technology and reduced/zero device identification cost.
9. **Security and privacy**: As end-customer data provides insights into user behaviors and how critical infrastructure can be used to adapt to changes in grid usage, the DIM system or platform must comply with, for example, the GDPR [3], implement privacy-preserving features (e.g. ZKP), and have a robust mechanism for verifying identities and authorizing transactions.
10. **Regulatory compliance**: Compliance with energy standards and regulations is important when selecting the technology, to ensure legal acceptance and reduce regulatory risk during field trial implementation.

6.3 Overview of the main available Frameworks

There are different SSI frameworks that can support DIM, however most of them are still in an early stage of development. Due to their maturity and applicability[3] only four SSI types of frameworks have been considered in this work, with different main characteristics, on Table 1 the 4 types of most suitable frameworks with its main characteristics are presented.

Table 1 – SSI Types of Frameworks

SSI Framework Type	Description
SSI-F Type 1	Type of framework focused on decentralized attestations, allowing trusted entities to issue verifiable claims without a central authority, supporting revocable credentials to maintain dynamic trust over time.
SSI-F Type 2	Type of framework enabling secure messaging, agent interoperability, and decentralized identity exchange based on the DIDComm protocol.
SSI-F Type 3	Type of framework designed to enable privacy-preserving identity management with support for minimal disclosure of personal information.
SSI-F Type 4	Type of framework that supports the issuance, management, and verification of digital credentials throughout their lifecycle.

6.3.1 SSI-F Type 1

This Framework type represents a blockchain-based SSI framework designed to issue, manage and verify decentralized digital identities and credentials, an example of those SSI-F Type 1 would be KILT [31], Dock.io [41] or Polygon ID [46]. For example, KILT is built on the Polkadot ecosystem [32] and it provides users with control over their digital identities ensuring privacy preservation through selective disclosure of credentials. Protocols following this type provide tools to implement Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). Those can be used for selective disclosure of data, this means that it allows users to share only the necessary information/data [31]. They are also compatible with various blockchain ecosystems and usually support revocation of verifiable credentials. The main use cases for type of framework are found in supply chain management for verifying the identity of suppliers and products, in digital identity verification for “know your customer (KYC) processes”, in financial services and also for issuing academic credentials [33], [34].

6.3.2 SSI-F Type 2

This second type of framework is used for building, managing and exchanging verifiable credentials on a blockchain network. An example of this second type would be the Hyperledger Aries [35] which focuses on providing the necessary tools to create interoperable identity solutions. Other examples would be Trinsic [47] or Indicio Network [48]. This type of SSI framework is mostly designed to enable different SSI frameworks and blockchain networks and supports DIDComm protocols for secure messaging and can work with different DLTs. It can be used for creating systems that can interact across different SSI frameworks and can be used by organizations issuing and verifying credentials in various industries and to securely manage identities across different organizations and ecosystems. Use cases for this technology can be found in health care, supply chain management, energy management, education and training, and finance [36], [37].

6.3.3 SSI-F Type 3

The SSI- Framework type 3 is a privacy-focused SSI platform that leverages decentralized identity principles to give users control over their personal data, for example Privado [38], Microsoft ION [49] or Animo (w/ Hyperledger Aries + ZK extensions). It aims to enable secure and compliant identity management across various applications. The system focuses on user privacy and data minimization and users can only share the necessary information with others. The systems also ensures that all personal data is securely stored and transmitted and it helps organizations comply with data protection regulations like GDPR [3]. The main use cases of this technology are found in the health care sector, allowing patients control who accesses their medical records. In financial sector, the use case is to help customers to verify their identity with minimal data sharing [39]. In the E-commerce sector, there

3 See applicability analysis of those technologies in following references [30] [12] [9] [14].

are also use cases found in enabling secure and private sharing of identity information with online merchants [40].

6.3.4 SSI-F Type 4

The SSI- Framework type 3 is a decentralized network that enables secure issuance, management and verification of verifiable credentials, for example Dock [41], Hyperledger Indy/Sovrin [50] or Veres One. It is built to provide an interoperable solution for SSI across various industries. The system supports the creation and management of VCs and uses a blockchain for immutable credential storage and verification. It should be compatible with most existing identity standards and offers APIs and SDKs for easy integration. The main use cases are found in the education sector for issuing and verifying academic credentials and for verifying professional qualifications and work history [40]. There are also use cases of this technology in supply chain for ensuring the authenticity of products and materials through verifiable credentials [42].

6.4 Matching Requirements and Selected Framework Types

The subsections above presented the requirements for energy use cases and the selected frameworks based on general assessments. The remaining question is which of these frameworks will offer the best performance in an energy use case. To determine this, the frameworks must align with the identified requirements. A comparative analysis has been performed between the selected technologies and the results are summarized in Table 2.

A detailed analysis of this comparison can be found in Table A.1, in the Annexes.

Table 2 – Comparison of selected SSI Types of frameworks for DIM application in the energy sector

Technology	Strength	Weakness	Suitability for energy use cases
SSI-F Type 1	■ Decentralized identity management ■ Interoperability ■ Privacy and security ■ Active community	■ Complex integration ■ Emerging technology	■ High
SSI-F Type 2	■ Strong privacy focus ■ User-centric	■ Limited decentralization ■ Lack of interoperability	■ Low to moderate
SSI-F Type 3	■ Interoperability ■ Modular and extensible ■ Strong community support	■ Complex setup ■ Less focus on blockchain	■ Moderate to high
SSI-F Type 4	■ Blockchain-based credentials ■ Ease to use ■ Interoperability	■ Relatively new ■ Limited features	■ Moderate to high

6.5 Conclusion

The SSI framework types presented in this section offer unique approaches to managing and verifying digital identities. These technologies have been applied across different industries and use cases ranging from financial services, e-commerce, education, healthcare, supply chain management, etc. The selection of a particular technology for a particular application depends primarily on the requirements and characteristics of the use case. In the next subsection, the selected SSI types of frameworks will be compared based on their performance against the identified energy use case requirements. For energy use case requirements, the comparison results of different framework types indicate that, due to decentralized identity management, privacy, high security, an active community, and interoperability, the SSI-Type 1 framework is the most suitable choice.

7 Development of the System Architecture for a Microgrid Use Case

7.1 Introduction

A microgrid is an entity consisting of multiple coordinated loads and generating units, which functions as a controllable structure for the main grid and constrained within well-defined electrical boundaries. It may connect/disconnect to the utility grid, enabling it to serve in both grid-tied and autonomous

(islanded) modes, see [43] and [44]. A microgrid however presents currently the same challenges as the rest of use cases in the energy sector regarding to security vulnerabilities, privacy concerns, lack of user autonomy and interoperability issues. This section describes the microgrid for the case study, proposes a SSI-based DIM framework as a solution to the current challenges presented above, and finally develops the methodology for creating the decentralized identities.

7.2 Proposed SSI-based DIM Model Framework Description

The decentralized identity management model platform with its core components is presented in Fig. 1. The framework is built up upon five basic components namely the user side components, the Microgrid control system, the side-chain components, the on-chain components, and the stakeholders' components.

The user side components include the user application (App) and hardware device (HW). The user App is used by the consumer/prosumer to create their decentralized identifier and manage the private keys of the user. The hardware device houses the HW wallet and is used to communicate verifiable credentials together with the offer/request to the central trading platform of the Microgrid Operator (MO).

The Microgrid control system is responsible for setting the business logic behind the trading mechanism and communicating it to the central trading platform, through remote procedure call (RPC) to the enclave.

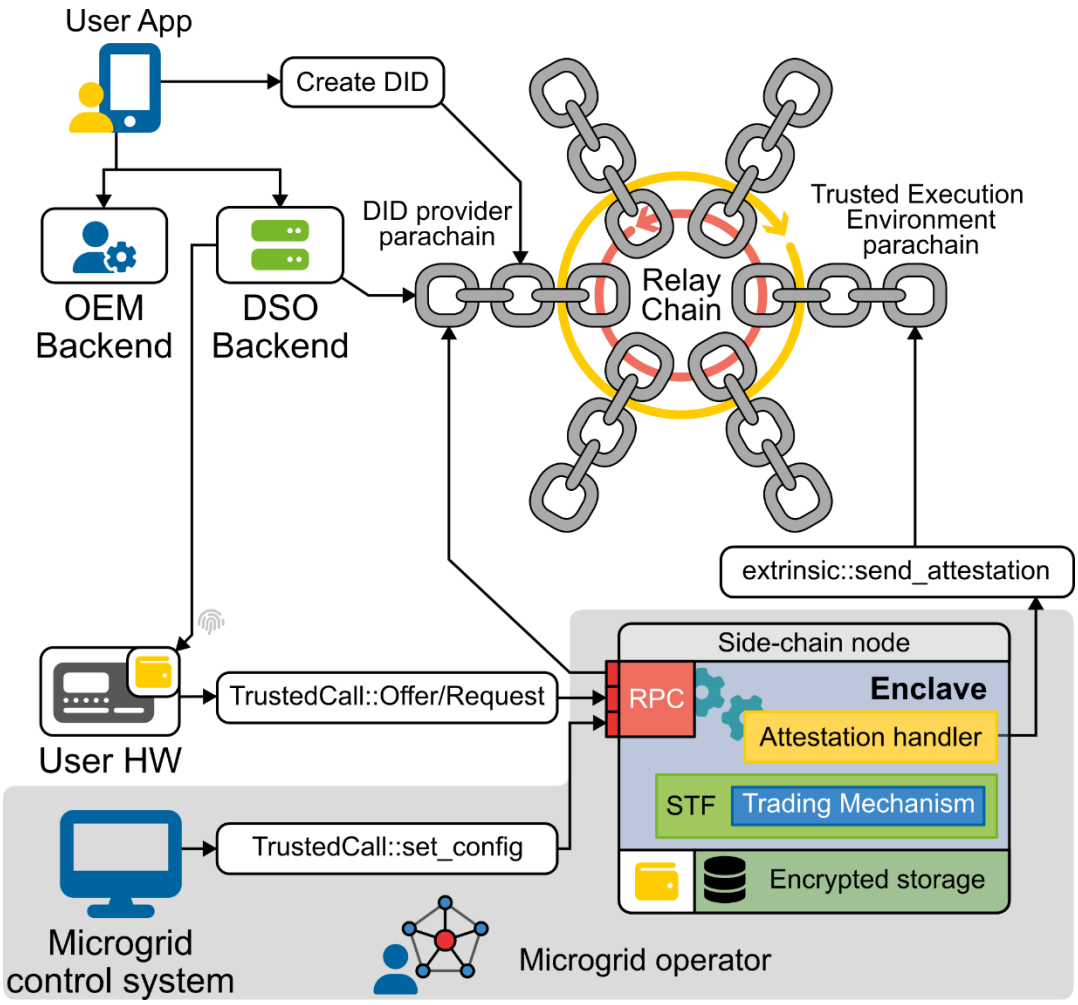

Figure 1 – Proposed DIM General Architecture

The side-chain components include the enclave and encrypted storage. The enclave contains the trading mechanism which resides on the state transition function (STF) and guarantees the confidentiality and integrity of the code to the users through the attestation service. The development and working of the enclave are discussed in [45]. Both Microgrid control system and enclave are operated by the MO.

The on-chain components used in this example are the IntegriTEE and KILT parachains which are second-layer blockchain networks built on Polkadot relay chain. The IntegriTEE parachain is used for storing the attestation of the enclave while the KILT parachain is used for creating and storing the users DIDs.

The last set of basic components include the stakeholders' components. Those are the Distribution System Operator (DSO) and Original Equipment Manufacturers (OEM) back-ends, that represent together with the MO, the central authorities regulating the participation into the microgrid energy trading platform.

7.3 The double-triangle of trust

In decentralized identity management, it is important to identify where trust already exists between actors and how to verify each communication before data is accepted or read, to avoid violating privacy law and ensure secure communication. A double-triangle of trust is used to show that the model satisfies the trust requirements which are used for data verification between the actors in the network. Fig. 2 shows the double-triangle of trust for the proposed model. The dotted lines show where trust already exists, while the full lines show the presentation or issuing of verifiable credentials. It is important to note that the DSO and the User are participating in both triangles of trust. While the User acts as Holder in both triangles, the DSO acts as a Verifier in one and as an Issuer in the other one.

The double-triangle of trust follows the following logic: Triangle I is activated by the OEM which issues the device owner (User) a Verifiable Credential (VC) upon request. This VC (VC1) will be submitted to the DSO to request approval to participate in the energy trading platform. Once the DSO has approved the VC1 of the User, the triangle II will be activated. In this second triangle, the DSO issues a new VC (VC2) for the participation in the trading platform and the User presents this new VC2 to the microgrid control system (MO – enclave) to offer/request energy in the energy trading platform. In this way, trust among participants is established and it is ensured that the devices are securely identified and verified during energy exchange. Also, this helps to ensure that data exchanged in the platform is secured and confidential.

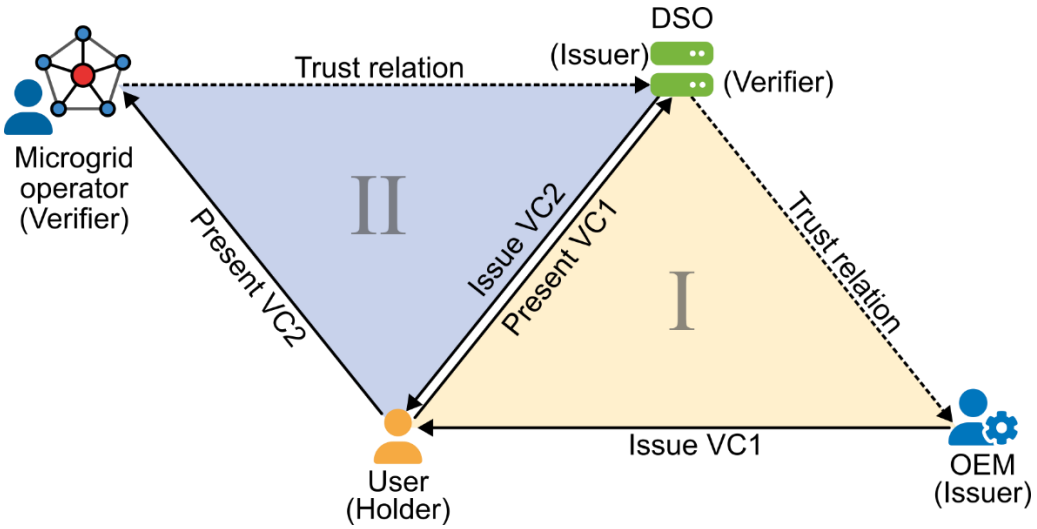

Figure 2 – Double-Trust triangle of the proposed model

7.4 Decentralized Identity Creation

The decentralized identity creation follows the sequence diagram presented in Fig. 3. Each User (consumer, prosumer, or energy producer) generates a Decentralized Identifier (DID) by sending a DID creation request from its User APP to the KILT Protocol (1:Request DID). This process involves creating a public-private key pair, where the private key remains with the participant, and the public key is used to create the DID. The KILT Parachain Generates DID (2:Generate DID) and send it to the User (3:Send User's DID). The User then sends a verification request to OEM with their DID and device identification number (4:Request device VC). The OEM creates the device's VC (5:Create VC1) and responds by sending the User the VC1 (6:Send VC1) upon confirmation that the device identification number belong to a list of devices that have manufactured in the past. This VC1 contains the device characteristics and the VC expiration date. The VC1 is stored in the Users Wallet (7:Store VC1 in User Wallet). The User submits his VC1 to the DSO to request approval to participate in the energy trading

platform (8:Present VC1). The DSO verifies the VC1 submitted by the User (9:Verify VC1). This means the DSO evaluates the characteristics of the verified User's device, such as maximum power, voltage, current, location, etc., to determine whether it can safely participate in the energy trading platform. Upon verifying that the device characteristics meet the requirements for participating in the energy trading platform then, the DSO verifies the DID in the Kilt Parachain (10:Request DID verification / 11:Verify DID / 12:Send verification) and issues the User another signed verifiable credential (13:Create VC2). This VC (VC2) is signed with the DSO private key. VC2 contains the DID of the device and its characteristics and it enables the User to participate in the energy trading and the maximum power allowed by the DSO (14:Post VC2). The User stores this VC2 in its HW Wallet (15:Store VC2 in HW Wallet). The attestation in both VC1 and VC2 are stored on the KILT blockchain, and the credential are posted to the User. Users can manage these credentials, deciding when and with whom to share them. Credentials are shared selectively during interactions within the microgrid, ensuring that only necessary information is disclosed. Two general issues that are important for the implementation are: 1) the process of getting "prepaid" KILT token into an Raspberry Pi (called OLI Box) works under the usability aspect, and 2) that the hardware secure modules are (not) required for this process.

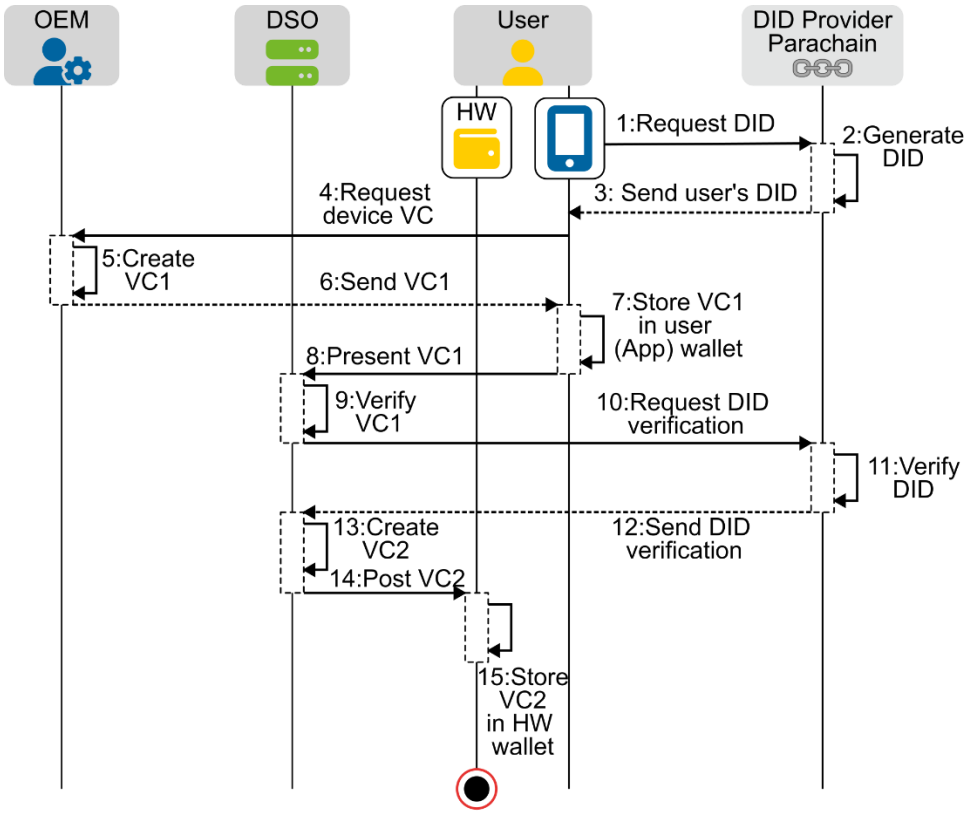

Figure 3 – Sequence diagram of the proposed decentralized identity creation

7.5 Secured Energy Trading and Transaction Management

The energy exchange for the proposed decentralized identity management platform follows the sequence diagram shown in Fig. 4. The participant's agent (User HW) calculates the energy request/offer (1:Calculate energy request/offer) and sends it to its HW's Wallet to authenticate the Request/Offer (2:Send offer/request data / 3:Create verifiable offer/request with VC2). The Userwallet authenticates the information by adding the verifiable credential (VC2) and signing it using the User's private key. The verifiable credential, together with the request/offer is then posted to the enclave of the Microgrid Operator (MO) (4:Post offer/request). The enclave of the MO, then verifies if the credential (VC2) is authentic and not revoked and that it was issued by the DSO (5:Verify DSO signature / 6:Request VC verification). The KILT protocol verifies the participant's credentials without revealing unnecessary personal information, ensuring privacy and security. If the verification is successful (7:Verify VC / 8:Send confirmation), the energy sharing of the User will be accepted (9:Confirm energy trading). The verification is repeated any time the User presents an energy offer/request to the MO. In this way, the trust between participants is established and the secure identification and verification of devices during energy exchange it is ensured. Additionally, this helps ensure that data exchanged on the platform is

secure and confidential. The user receives the confirmation of the enclave (10:Publish energy trading results), verifies the signature of the enclave (11:Verify enclave signature) and implements the new set points (12:Send data / 13:Analyze results and set controls).

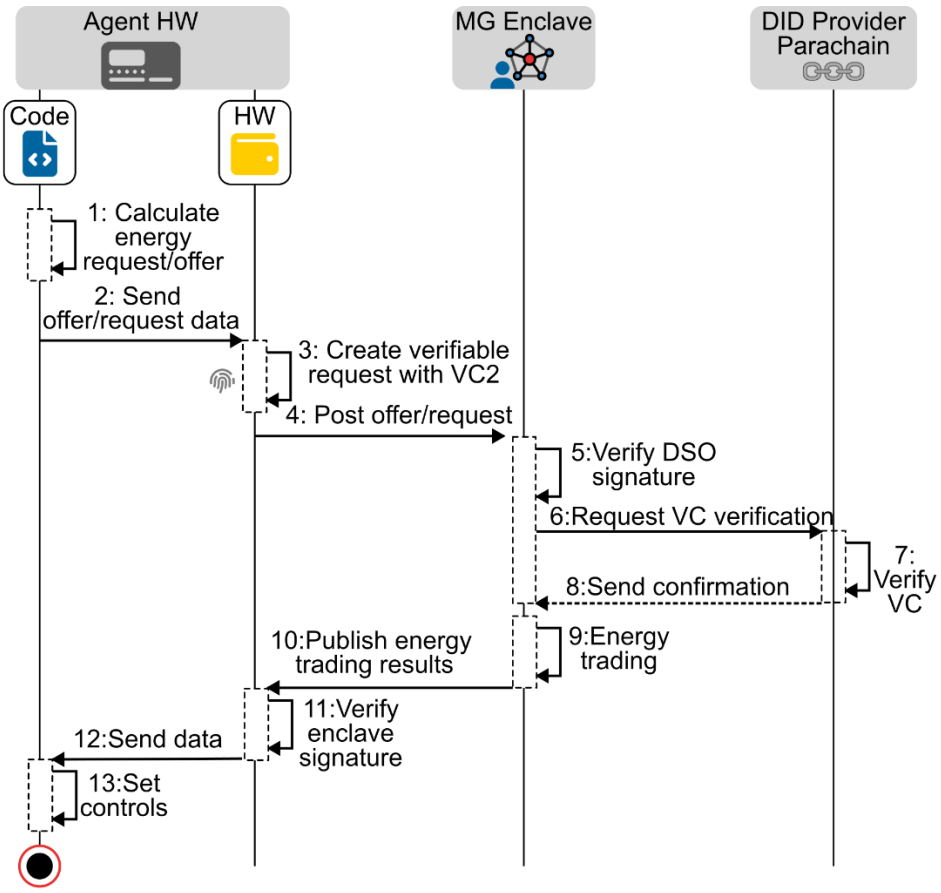

Figure 4 – Sequence diagram of energy exchange for the proposed DIM

7.6 Conclusion

In this subsection, the general DIM framework model has been explained, and all core components have been described. The underlying logic of the SSI-based DIM framework follows the double-triangle of trust model. Identity creation and transaction management have also been developed and illustrated through the sequences of necessary information exchanges and activities.

8 Laboratory Testing and Evaluation

8.1 Introduction

This section presents the laboratory test set-up, the tested on-boarding and energy exchange and the main experimental results of the test. In order to make the results of this section easily to follow, all the details in the Laboratory implementation have been provided in the Annexes.

8.2 Experiment Set-up

The proposed model was evaluated in a hardware-in-the-loop test at the Energy Systems Laboratory of the Reutlingen University. A simple four-user microgrid was emulated and each user device was represented by a Raspberry Pi. The developed DIM model was deployed on a cloud virtual machine to facilitate communication with the application programming interface (API) and to perform configuration experiments close to a field test scenario. The Postman desktop application was used to demonstrate the user interface for participants **to** show how they communicate with the model from the device level and the corresponding response.

8.3 On-boarding and energy exchange

The laboratory test followed 5 main steps, from registration to energy exchange.

- **Step 1**: OEM and DSO registration. For that purpose, two accounts are created[4], one for the OEM and one for the DSO. Both accounts are doted with Faucet Kilt coins[5]. The DIDs are then created for each of the admins accounts and used to create a schema[6] and those are stored on the blockchain. The OEM schema (used to issue VC2) includes the device name, device serial number, device id, maximum voltage, rated power, electronic description, and device validity. The DSO schema (used to issue VC2) includes the device id, device validity, max allowed power, rated power, and device type.
- **Step 2**: User registration. The four users on the microgrid are represented by a single Raspberry Pi device each. Those devices are used to initiate the on-boarding process by inputting the details of their household on the Postman App and sending a request for registration to the platform and the creation of a DID in the Kilt parachain[7]. **Thus,** this means that the users are now fully registered and can exchange energy within the platform.
- **Step 3**: Device certification. Through the Postman App, the four users submit a request to the OEM address to certify their device, obtain VC15, to participate in the energy trading of the microgrid.
- **Step 4**: Claim creation. **Also,** through the Postman App, the four users submit a claim to the DSO to become a participant in the microgrid trading. This claim includes the VC1 already issued by OEM and the response is the VC26 for each of the user.
- **Step 5**: Service Access/Energy exchange. With their credentials in place, the users are able to access the microgrid energy trading and submit request/offers7 at any time. This energy trading and identity verification process happens in every market slot. During energy exchange, the user agent residing on the Raspberry Pi calculates the quantity of energy that will be available for exchange in the platform. This amount is entered as an input together with VC2 and posts to the Enclave from the Participants Raspberry Pi.

8.4 Conclusions and Experimental Results

The experiment was successfully developed in its 5 steps and showed how microgrid participants (users) can create and use their DID to receive their verifiable credentials and participate in the microgrid trading mechanism. From the requirements identified, the following were tested with successful results: interoperability, developers community ecosystem, decentralization, performance and reliability, security and privacy and regulatory compliance. Because of its importance, the results in data privacy and regulatory compliance are discussed separately in the next section.

9 Discussion about Data Security, Privacy and Regulatory Compliance

9.1 Introduction

In the developed model, participants use their DID to control which entities have access to their energy usage data, contributing to enhanced data privacy. For example, a prosumer may choose to trade energy production data with the central hub for grid stability monitoring but may withhold it from other participants. Also, since DID are pseudoanonymous, the particular owner of a certain verifiable credentials may not be known by the market operator managing the central hub. However, the market operator can be assured that the participant is allowed to participate in the energy trading by verifying their VC. The decentralized nature of the Framework used allows for compliance with local energy regulations by providing auditable records of energy transactions.

Regulatory bodies can access anonymized data to verify compliance without infringing on individual privacy. They can also verify the eligibility of the individuals to trade electricity without infringing on the individuals data privacy. In terms of security threats, the protocol and associated DID management systems provides opportunity for regular update to protect against emerging security threats. This

---

4 The instruction used to create those accounts is createAdminKeyPair EndPoint and the resulting account types are admin accounts and usually represented by an address.

5 The link to the facet used in this experiment is https://faucet.peregrine.kilt.io/

6 A Schema describes the list of variables in which the OEM and the DSO can attest their values for a user and issue VC on this variables.

7 This is done with the instruction AddUser EndPoint following the instruction CreateUserDID EndPoint to create a DID for each user in the KILT Parachain.

regular update helps to maintain the security and integrity of the wallets when deployed to a field test to ensure that users private data are well secured. For all these reasons, the solution developed also complies with the requirements of Data Security and Privacy and Regulatory Compliance identified in section 3.

9.2 Data Privacy and Access Control

The developed model enables participants to exercise granular control over access to their energy usage data using DIDs, enhancing data privacy in Selective Data Sharing and Pseudonymous Identity.

a. Selective Data Sharing: Participants can choose to share specific energy data with designated entities. For instance, a prosumer may provide energy production data to the central hub for grid stability monitoring while withholding it from other participants.

b. Pseudonymous Identity: As DIDs are pseudonymous, the identity of the holder of a particular verifiable credential (VC) remains unknown to the market operator managing the central hub. However, the operator can verify the validity of the VC to confirm the participant's eligibility for energy trading. This ensures privacy while maintaining operational transparency.

9.3 Regulatory Compliance and Data Auditability

The decentralized KILT protocol offers mechanisms to ensure compliance with local energy regulations

while preserving individual privacy in Auditable Transaction Records and Eligibility Verification.

a. **Auditable Transaction Records**: Energy transaction data can be anonymized and made available for regulatory auditing, allowing oversight bodies to verify compliance without compromising participants' privacy.

b. **Eligibility Verification**: Regulatory authorities can verify participants' eligibility to trade electricity through the examination of anonymized credentials, further ensuring adherence to regulatory requirements.

9.4 Double Triangle of Trust

The model incorporates a "double triangle of trust" framework, which enhances the credibility and operational efficiency of the energy trading system by Device Verification and Market Participation. The double triangle of trust provides an opportunity for the device owners to prove the eligibility of their devices to participate in the microgrid energy trading and at the same time give the DSO to control the power and energy traded within the microgrid to avoid causing uncontrollable local congestion. The first verifiable credential (VC1) provides an opportunity for the DSO to know the capacity and originality of the devices willing to participate in the microgrid energy trading. This also includes the validity of the devices. Hence, since the DSO trusts the OEMs who are the device manufacturers, they can verify that the credential was issued by OEM through secured verification and issue verifiable credentials (VC2) to the participants based on the information verified from VC1. In the same way, the market operator can verify that the participant is allowed or permitted to participate in the microgrid energy market by verifying the details of VC2 before entering the bid/offer into the ordered book. This prevents the market participants from bidding on what they cannot consume or offering what they cannot produce in the market platform and thereby discourage gaming of the market.

a. **Device Verification**: The first VC (VC1) enables the Distribution System Operator (DSO) to validate the capacity, originality, and operational validity of devices willing to participate in the microgrid. Since the DSO trusts the Original Equipment Manufacturer (OEM), it can verify that the VC1 was issued by the OEM. Based on this verified information, the DSO issues a second VC (VC2) to participants, certifying their devices for energy trading.

b. **Market Participation**: The market operator uses VC2 to verify that participants are eligible to trade within the microgrid. This prevents participants from submitting bids or offers that exceed their production or consumption capacity, mitigating potential market manipulation and gaming. This dual-layered trust structure ensures that only compliant and verified devices and participants engage in energy trading, reducing the risk of congestion and maintaining grid stability.

9.5 Security and Threat Mitigation

The protocol implemented and its associated DID management system provide robust protection against security threats by Regular Security Updates and Field-Test Readiness.

a. **Regular Security Updates**: The model supports regular updates to address emerging security vulnerabilities. These updates maintain the integrity and security of participants' wallets and data.

b. **Field-Test Readiness**: The model is designed to withstand security challenges in field test scenarios, ensuring the protection of private user data during practical deployments. The results demonstrate that the developed model successfully integrates privacy, security, and regulatory compliance within a decentralized energy trading framework. Through its pseudonymous DID system, trust mechanisms, and robust security measures, the model is well-suited for deployment in real-world microgrid energy markets, addressing both operational and regulatory requirements.

10 Conclusion

The main objective of this specification is the analysis, design, and development of an SSI-based DIM for the energy sector, along with its application and testing in a microgrid case study. To achieve this, the work investigates the requirements of DIM and compares different SSI-based DIM solutions for energy use cases, selecting the most suitable framework solution. This solution demonstrates superior performance when evaluated against typical functional and non-functional requirements of energy applications, owing to its inherent features such as decentralization, interoperability, security architecture, and an active community.

Subsequently, this work enabled the development of the DIM model based on SSI technology, which was successfully implemented and tested in a laboratory environment simulating a microgrid with four users. The hardware-in-the-loop test was conducted successfully, meeting most of the identified requirements regarding interoperability, developer community ecosystem, decentralization, performance and reliability, security and privacy, and regulatory compliance. Furthermore, security, privacy, and regulatory compliance were analyzed in detail, given their critical importance in the context of DIM.

The main contributions of this work have been: The development, implementation and test of a new DIM system tailored to the needs of energy use cases; The development and validation of the double triangle of trust to solve the trust problem; The hardware-in-the-loop test of a microgrid in the Reutlingen University Energy systems laboratory for validating the both developments; The successful identification and qualification of users to participate in energy trading activities and; The validation of the fulfillment of DIM requirements of energy use cases in the solution developed.

The main contributions of this work are:

- The development, implementation, and testing of a new DIM system tailored to the needs of energy use cases;
- The development and validation of the double triangle of trust model to address the trust challenge;
- The hardware-in-the-loop testing of a microgrid at the Reutlingen University Energy Systems Laboratory to validate both developments;
- The successful identification and qualification of users to participate in energy trading activities; and
- The validation of the solution’s fulfillment of DIM requirements for energy use cases.

The results demonstrate that the developed model can effectively identify users and facilitate transactions in energy use cases. The primary benefits of the model include enhancing user security, granting users autonomy over their data, and enabling secure sharing of data with selected partners. Future work will focus on extending the model to a field test scenario, where its scalability and robustness can be comprehensively evaluated.

One of the primary challenges in this domain is the limited availability of standardized protocols and frameworks. The solution presented herein constitutes one viable approach. Nonetheless, alternative solutions exist, and it is imperative that standardization bodies evaluate and validate multiple approaches across diverse energy use cases to determine the most appropriate and effective solution.

Annex A
Analysis of DIM requirements for energy sector

In table A.1 are presented the results of the in-deep comparison of the four SSI Solutions based on the DIM requirements for the energy sector.

Table A.1 – Comparison of SSI solutions based on the DIM requirements for energy sector use

Requirements	SSI-F Type 1	SSI-F Type 2	SSI-F Type 3	SSI-F Type 4
Decentralization	**DIDs Support**: Fully supports DIDs and VCs. **Blockchain Integration**: Built on i.e. Polkadot, providing strong decentralization and cross-chain capabilities.	**DIDs Support**: Strong support for DIDs and VCs. **Blockchain Integration**: Requires additional blockchain layers but offers strong identity capabilities.	**DIDs Support**: Focuses more on privacy; limited emphasis on DIDs. **Blockchain Integration**: Not inherently blockchain based, primarily a privacy focused platform.	**DIDs Support**: Native blockchain solution with full support for DIDs and VCs. **Blockchain Integration**: Designed for blockchain-based identity management.
Usability and accessibility	**User-Friendly Interfaces**: Provides comprehensive tools and documentation for users and developers. **Developer Tools and Documentation**: Strong community support.	**User-Friendly Interfaces**: Offers flexible tools for integration and development. **Developer Tools and Documentation**: Strong support i.e. from Hyperledger community.	**User-Friendly Interfaces**: Privacy centric-tools are user-friendly but less focussed on identity management. **Developer Tools and Documentation**: moderate resources available.	**User-Friendly Interfaces**: Simple and intuitive APIs and tools. **Developer Tools and Documentation**: Good support for developers.
Security and Privacy	**Data privacy**: Strong focus on privacy with features like selective disclosure. **Cryptographic Security**: Uses robust cryptographic methods. **Authentication and Authorization**: Strong mechanism.	**Data privacy**: Supports privacy through secure messaging and VCs. **Cryptographic Security**: Very strong. **Authentication and Authorization**: Robust SSI methods.	**Data privacy**: High emphasis on privacy, using encryption and consent management. **Cryptographic Security**: Very strong. **Authentication and Authorization**: Focus on privacy over decentralized identity.	**Data privacy**: Emphasizes secure access control. **Cryptographic Security**: Uses blockchain security principles. **Authentication and Authorization**: Strong.
Scalability	**Handling Large volumes**: Scalable due to i.e. Polkadot's architecture. **Efficient Transaction Processing**: Efficient with blockchain scalability features.	**Handling Large volumes**: Scalability can vary based on implementation, suitable for decentralized application. **Efficient Transaction Processing**: Can be efficient with proper setup.	**Handling Large volumes**: Not specifically designed for scalability in decentralized markets. **Efficient Transaction Processing**: Primarily focused on data privacy, not scalability.	**Handling Large volumes**: Designed for scalability, with blockchain support. **Efficient Transaction Processing**: Efficient especially for credential verification.
Community	**Active community engagement**: Strong community with support from the Polkadot's ecosystem. **Partnership and collaborations**: Active collaboration within the energy sector.	**Active community engagement**: Strong support from i.e. Hyperledger community. **Partnership and collaborations**: Broad industry engagement.	**Active community engagement**: moderate, focused on privacy. **Partnership and collaborations**: Limited to privacy-centric organization.	**Active community engagement**: Growing community support on security. **Partnership and collaborations**: Engaging with multiple sectors.

Requirements	SSI-F Type 1	SSI-F Type 2	SSI-F Type 3	SSI-F Type 4
Performance and reliability	**Availability**: Designed for high availability through Polkadot's infrastructure. **Reliability and Fault Tolerance**: Robust, leveraging on blockchain technology.	**Availability**: Good availability with proper setup. **Reliability and Fault Tolerance**: Strong due to modularity and interoperability.	**Availability**: Focus on privacy, availability is moderate. **Reliability and Fault Tolerance**: Reliable for privacy but not for decentralized identity.	**Availability**: Designed for reliable performance with blockchain. **Reliability and Fault Tolerance**: Robust for credential management.

Annex B
Laboratory experiment

The proposed model was evaluated through a hardware-in-the-loop (HIL) laboratory test conducted in the Energy Systems Laboratory at Reutlingen University. The test environment emulated a simple microgrid consisting of four users. Each household device within the microgrid was represented using a Raspberry Pi. The developed distributed identity management (DIM) model was deployed on a cloud-based virtual machine to facilitate seamless communication via an application programming interface (API) and to simulate a setup that closely resembles a real-world field test scenario. Fig. B.1 presents an overview of the architecture used. The application follows the REST API architecture and was programmed on the express.js web application framework.

As database, the experiment makes use of MongoDB for persistent data like admin, user or bid data. The blockchain-based credential management is implemented through the KILT protocol.

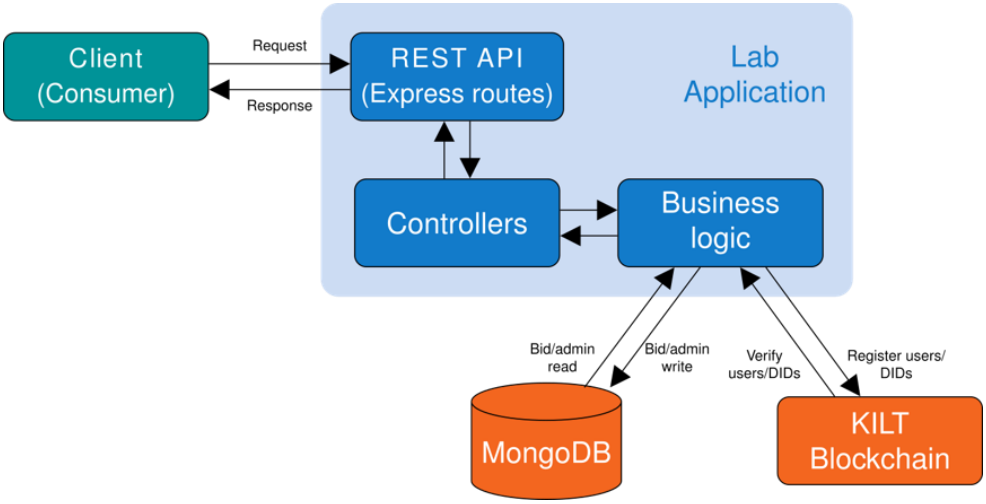

Figure B.1 – Architectural overview of the implemented laboratory experiment

B.1 Laboratory Setup and Endpoints

The implemented lab experiment exposes a REST API that enables the management of users, decentralized identities (DIDs), verifiable credentials, schemas, and bid-related information. Figure B.2 shows an overview of the exposed endpoints, to which the test client (in the case of this lab experiment, the postman app) can post or get information. The exposed endpoints and their methods and descriptions are given in the following sections.

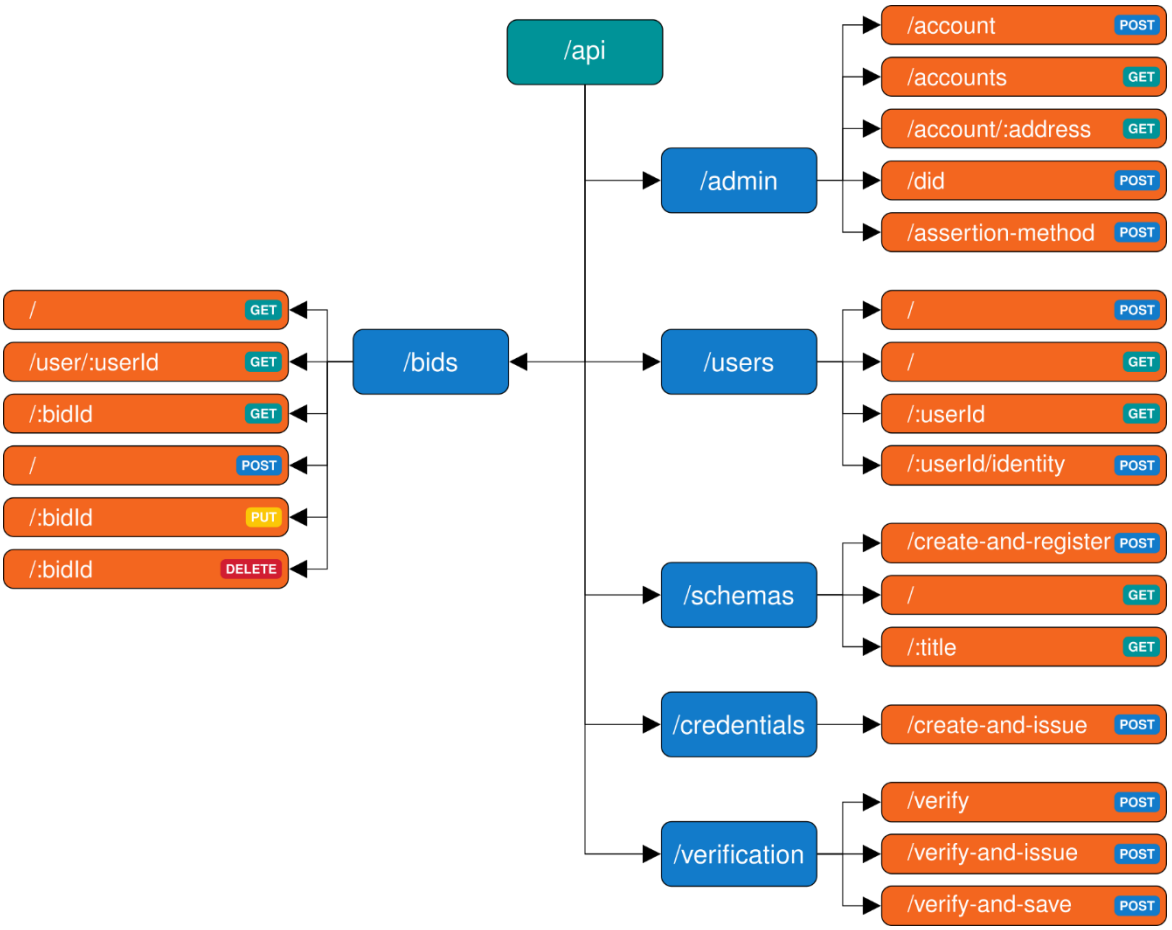

Figure B.2 – Graphical overview representation of the implemented API endpoints

B.1.1 Administration Endpoints

Method	Endpoint	Description
POST	`/api/admin/account`	Creates a new administrator account.
GET	`/api/admin/accounts`	Retrieves all registered administrator accounts.
GET	`/api/admin/account/:address`	Retrieves the details of an administrator identified by its blockchain *:address*.
POST	`/api/admin/did`	Creates a Decentralized Identifier (DID) for an administrator.
POST	`/api/admin/assertion-method`	Adds an assertion method (signing capability) to an administrator's DID.

B.1.2 User Endpoints

Method	Endpoint	Description
POST	`/api/users`	Registers a new user in the system.
GET	`/api/users`	Retrieves all registered users.
GET	`/api/users/:userId`	Retrieves information about a specific *:userId*.
POST	`/api/users/:userId/identity`	Creates a Decentralized Identifier (DID) for the specified *:userId*.

B.1.3 Schema Endpoints

Method	Endpoint	Description
POST	`/api/schemas/create-and-register`	Creates and registers a new CType schema on the KILT blockchain.
GET	`/api/schemas`	Retrieves all registered schemas.
GET	`/api/schemas/:title`	Retrieves a schema by its *:title*.

B.1.4 Credential Endpoints

Method	Endpoint	Description
POST	`/api/credentials/create-and-issue`	Creates and issues a Verifiable Credential for a user.

B.1.5 Verification Endpoints

Method	Endpoint	Description
POST	`/api/verification/verify`	Verifies the authenticity and validity of a Verifiable Credential.
POST	`/api/verification/verify-and-issue`	Verifies a credential and, if valid, issues a new credential.
POST	`/api/verification/verify-and-save`	Verifies a credential and stores the associated bid information.

B.1.6 Bid Management Endpoints

Method	Endpoint	Description
GET	`/api/bids`	Retrieves all stored bids.
GET	`/api/bids/user/:userId`	Retrieves all bids associated with a specific *:userId*.
GET	`/api/bids/:bidId`	Retrieves a specific bid by its identifier (*:bidid*).
POST	`/api/bids`	Creates a new bid.
PUT	`/api/bids/:bidId`	Updates an existing *:bidId*.
DELETE	`/api/bids/:bidId`	Deletes an existing *:bidId*.

B.2 Step-by-Step Evaluation of the On-boarding and Energy Exchange Model

This section provides a Step-by-Step guidance to the process of On-boarding and Energy Exchange Model.

B.2.1 OEM and DSO Registration

This subsection outlines a systematic evaluation of the on-boarding process and energy exchange within a smart microgrid system, focusing on the technical and procedural steps involved in setting up participants and enabling energy transactions. Two administrative accounts were established for the Original Equipment Manufacturer (OEM) and the Distribution System Operator (DSO) using the Create Admin KeyPair EndPoint. The Create Admin KeyPair EndPoint requires no input. The output is an adminId, public address, mnemonic and confirmation message as shown in Fig. B.2.

The accounts, categorized as admin accounts and represented by unique addresses, were funded with Faucet KILT coins obtained from Faucet Peregrine using their address. Subsequently, Decentralized Identifiers (DIDs) were created for both accounts using Create Admin DID endpoint as shown in Fig. B.3. The input to the Create Admin DID endpoint is the admin address. The output is the admin address, DID and confirmation message.

Schema Creation for OEM

The OEM DID was employed to create and store a schema on the blockchain. This schema specifies variables that the OEM can attest to when issuing verifiable credentials (VC1) for a particular user. The OEM schema included:

- Device name
- Device serial number
- Device ID
- Maximum voltage
- Rated power
- Device OEM
- Electronic description
- Device validity

Schema Creation for DSO

Similarly, the DSO DID was used to create and store its schema on the blockchain. This schema was utilized to issue verifiable credentials (VC2) and included:

- Device ID
- Device validity
- Maximum allowed power
- Rated power
- Device type

The endpoint `/api/schemas/create-and-register` was used for schema creation. The only difference is that the owner of the schema needs to be specified by adding the did and mnemonic of the owner at the input. Before any admin account will be allowed to create a schema, the account needs to be given permission to do that by using the `/api/admin/assertion-method` endpoint. This endpoint requires the admin address as the input and the output is a confirmation message.

B.2.2 User Registration

Four electricity traders on the microgrid were represented by individual Raspberry Pi devices. These users initiated the on-boarding process by submitting their household details via the POST `/api/users` endpoint. The inputs of the endpoint are the user's serialNumber, deviceId, Name, and email as strings in JSON format. The output of this endpoint is the userId and a confirmation message.

Following successful registration, DIDs were created for each user using the `/api/users/:userId/identity` with the Administrator address and *:userId* (output of the Add User Endpoint) as the input. The outputs of this endpoint are a *userIdentity* JSON object and a confirmation message. The *userIdentity* includes the user mnemonic, publicKey, DID, and an empty bracket for credentials. At this stage, users were fully registered but not authorized to participate in energy exchange on the platform as the users still have no credentials.

B.2.3 Device Certification

Each household then submitted a certification request to the OEM address to validate their devices for participation in energy trading. Using the `/api/credentials/create-and-issue` endpoint, the OEM issued verifiable credentials (VC1) to each household, as defined by the schema stored on the blockchain. The input to the `/api/credentials/create-and-issue` endpoint is the userId, adminaddress, ctypeTitle and credential data.

The response of the endpoint is a confirmation message, credentials details, proof and salt. At this point, the credentials can be seen at the user wallet using the `/api/users` or `/api/users/:userId` endpoints.

B.2.4 Claim Creation

To become active participants in the microgrid, the households submitted claims to the DSO. These claims included the VC1 issued by the OEM. The `/api/verification/verify-and-issue` endpoint was used to process these claims by verifying the submitted credentials and issuing another verifiable credential (VC2) for each household. The VC2 serves as proof of the household's eligibility to participate in the microgrid's energy exchange. The inputs are the userId, credentialsId (this is the Id if VC1 that needs to be verified), adminaddress(this is the address of DSO), ctypeTitle (the DSO credentials schema), credentials data and proofOptions. The credentials data is the data of the new credentials (VC2) that will be issued by the DSO. The proofOptions are the details of the VC1 that needed to be verified. The response of this call is the details of VC2 issued to the user with the userId.

B.2.5 Service Access and Energy Exchange

With verified credentials in place, participants gained access to the microgrid energy trading system. Households submitted bids and offers for energy trading using the `/api/verification/verify-and-save` endpoint. The platform successfully verified and recorded these transactions. During energy exchange, the user agent on each household's Raspberry Pi device calculated the available energy for trade. This value, along with the VC2, was transmitted to the platform via the Raspberry Pi. The energy exchange process was executed for each market slot, ensuring accurate identity verification and transaction recording. The inputs to this endpoint are the userId, credentialsId (VC2), proofOptions, and bid. proofOptions are the details of VC2 that needed to be verified by MO before accepting the bid or offers for matching. The response of the EndPoint are the proof of the successful verification of VC2 and the stored bid or offer.

Bibliography

[1] I. Security, Cost of a data breach report 2023, Accessed: Sep. 17, 2024, 2023. [Online]. Available: https://www.ibm.com/security/data-breach .

[2] O. N. G. Zyskind and A. Pentland, „Decentralizing privacy: Using blockchain to protect personal data“, in 2015, pp. 180–184. DOI: 10.1109/SPW.2015.27. [Online]. Available: https://doi.org/10.1109/SPW.2015.27.

[3] E. Union, General data protection regulation (gdpr), Accessed: Sep. 17, 2024, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[4] C. Cachin and M. Vukolić, Blockchain consensus protocols in the wild, Accessed: Sep. 17, 2024, 2017. [Online]. Available: https://arxiv.org/abs/1707.01873.

[5] A. Tobin and D. Reed, The inevitable rise of self-sovereign identity, Accessed: Sep. 17, 2024, 2017. [Online]. Available: https : / / sovrin . org / wp - content / uploads / 2018 / 03 / The - Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

[6] M. Swan, Blockchain: Blueprint for a New Economy. O'Reilly, 2015, ISBN: 9781491920473. [Online]. Available: https://books.google.de/books?id=RHJmBgAAQBAJ.

[7] W. W. W. C. (W3C), Decentralized identifiers (dids) v1.0, Accessed: Oct. 14, 2024, 2021. [Online]. Available: https://www.w3.org/TR/did-core/.

[8] W. W. W. C. (W3C), Verifiable credentials data model 1.0, Accessed: Oct. 20, 2024, 2019. [Online]. Available: https://www.w3.org/TR/vc-data-model/.

[9] A. M. Buttar, M. A. Shahid, M. N. Arshad, and M. A. Akbar, „Decentralized identity management using blockchain technology: Challenges and solutions“, in Blockchain Transformations: Navigating the Decentralized Protocols Era, S. M. Idrees and M. Nowostawski, Eds. Cham: Springer Nature Switzerland, 2024, pp. 131–166, ISBN: 978-3-031-49593-9. DOI: 10.1007/978- 3-031-49593-9_8. [Online]. Available: https://doi.org/10.1007/978-3-031-49593-9_8.

[10] D. Coll-Mayor and A. Notholt, „Distributed ledger technologies for the energy sector: Facilitating interoperability analysis“, IEEE Open Access Journal of Power and Energy, vol. 10, pp. 593–604, 2023. DOI: 10.1109/OAJPE.2023.3297199.

[11] E. Samir, H. Wu, M. Azab, C. Xin, and Q. Zhang, „Dt-ssim: A decentralized trustworthy selfsovereign identity management framework“, IEEE Internet of Things Journal, vol. 9, no. 11, pp. 7972–7988, 2022. DOI: 10.1109/JIOT.2021.3112537.

[12] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. Raymond Choo, „Blockchain-based identity management systems: A review“, Journal of Network and Computer Applications, vol. 166, p. 102 731, 2020, ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2020.102731. [Online]. Available: https : / / www . sciencedirect . com / science / article / pii / S1084804520302058.

[13] X. Feng, L. Wang, X. Bai, and P. Yang, „Distributed identity management mechanism based on improved block-chain certificateless encryption algorithm“, Physical Communication, vol. 65, p. 102 341, 2024, ISSN: 1874-4907. DOI: https : / / doi . org / 10 . 1016 / j . phycom . 2024 . 102341. [Online]. Available: https : / / www . sciencedirect . com / science / article / pii / S1874490724000594.

[14] P. Dunphy and F. A. Petitcolas, „A first look at identity management schemes on the blockchain“, IEEE Security & Privacy, vol. 16, no. 4, pp. 20–29, 2018. DOI: 10.1109/MSP.2018.3111247.

[15] V. Dehalwar, M. L. Kolhe, S. Deoli, and M. K. Jhariya, „Blockchain-based trust management and authentication of devices in smart grid“, Cleaner Engineering and Technology, vol. 8, p. 100 481, 2022, ISSN: 2666-7908. DOI: https://doi.org/10.1016/j.clet.2022. 100481. [Online]. Available: https : / / www . sciencedirect . com / science / article / pii / S2666790822000866.

[16] A. Dua, S. S. Barpanda, N. Kumar, and S. Tanwar, „Trustful: A decentralized public key infrastructure and identity management system“, in 2020 IEEE Globecom Workshops (GC Wkshps, 2020, pp. 1–6. DOI: 10.1109/GCWkshps50303.2020.9367444.

[17] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, „Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey“, IEEE Access, vol. 10, pp. 113 436–113 481, 2022. DOI: 10.1109/ACCESS.2022.3216643.

[18] C. N. Butincu and A. Alexandrescu, „Design aspects of decentralized identifiers and selfsovereign identity systems“, IEEE Access, vol. 12, pp. 60 928–60 942, 2024. DOI: 10 . 1109 / ACCESS.2024.3394537.

[19] E. Zeydan, L. Blanco, J. Mangues-Bafalluy, et al., „Blockchain-based self-sovereign identity: Taking control of identity in federated learning“, IEEE Open Journal of the Communications Society, vol. 5, pp. 5764–5781, 2024. DOI: 10.1109/OJCOMS.2024.3449692.

[20] M. Volkmann, S. S. Tripathi, S. Kaven, C. Frank, and V. Skwarek, „Privacy in local energy markets: A framework for a self-sovereign identity based p2p-trading authentication system“, in 2023 IEEE 21st International Conference on Industrial Informatics (INDIN), 2023, pp. 1–7. DOI: 10.1109/INDIN51400.2023.10218046.

[21] J. M. Bernabé Murcia, E. Cánovas, J. García-Rodríguez, A. M. Zarca, and A. Skarmeta, „Decentralised identity management solution for zero-trust multi-domain computing continuum frameworks“, Future Generation Computer Systems, vol. 162, p. 107 479, 2025, ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2024.08.003. [Online]. Available: https: //www.sciencedirect.com/science/article/pii/S0167739X24004291.

[22] M. S. Ferdous, U. Cali, U. Halden, and W. Prinz, „Leveraging self-sovereign identity & distributed ledger technology in renewable energy certificate ecosystems“, Journal of Cleaner Production, vol. 422, p. 138 355, 2023, ISSN: 0959-6526. DOI: https://doi.org/10.1016/ j.jclepro.2023.138355. [Online]. Available: https://www.sciencedirect.com/science/ article/pii/S0959652623025131.

[23] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, „Blockchain-enabled smart contracts: Architecture, applications, and future trends“, IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 11, pp. 2266–2277, 2019. DOI: 10.1109/TSMC.2019.2895123.

[24] M. Zecchini, M. Sober, S. Schulte, and A. Vitaletti, „Building a cross-chain identity: A selfsovereign identity-based framework“, in 2023 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), 2023, pp. 149–156. DOI: 10 . 1109 / DAPPS57946 . 2023.00029.

[25] B. Alzahrani, „An information-centric networking based registry for decentralized identifiers and verifiable credentials“, IEEE Access, vol. 8, pp. 137 198–137 208, 2020. DOI: 10 . 1109 / ACCESS.2020.3011656.

[26] A. Ahl, M. Goto, M. Yarime, K. Tanaka, and D. Sagawa, „Challenges and opportunities of blockchain energy applications: Interrelatedness among technological, economic, social, environmental, and institutional dimensions“, Renewable and Sustainable Energy Reviews, vol. 166, p. 112 623, 2022, ISSN: 1364-0321. DOI: https://doi.org/10.1016/j.rser.2022. 112623. [Online]. Available: https : / / www . sciencedirect . com / science / article / pii / S1364032122005172.

[27] B. Cremonezi, A. B. Vieira, J. Nacif, E. F. Silva, and M. Nogueira, „Identity management for internet of things: Concepts, challenges and opportunities“, Computer Communications, vol. 224, pp. 72–94, 2024, ISSN: 0140-3664. DOI: https : / / doi . org / 10 . 1016 / j . comcom . 2024.05.014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366424001889.

[28] Y. Wang, X. Jia, Y. Xia, M. K. Khan, and D. He, „A blockchain-based conditional privacy preserving authentication scheme for edge computing services“, Journal of Information Security and Applications, vol. 70, p. 103 334, 2022, ISSN: 2214-2126. DOI: https://doi.org/10. 1016/j.jisa.2022.103334. [Online]. Available: https://www.sciencedirect.com/science/ article/pii/S221421262200179X.

[29] W. Zhu, X. Chen, and L. Jiang, „A secure and efficient authentication key agreement scheme for industrial internet of things based on edge computing“, Alexandria Engineering Journal, vol. 101, pp. 52–61, 2024, ISSN: 1110-0168. DOI: https://doi.org/10.1016/j.aej.2024. 05 . 036. [Online]. Available: https : / / www . sciencedirect . com / science / article / pii / S1110016824005064.

[30] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, „Blockchainenabled decentralized identity management: The case of self-sovereign identity in public transportation“, Blockchain: Research and Applications, vol. 2, no. 2, p. 100 014, 2021, ISSN: 2096-7209. DOI: https : / / doi . org / 10 . 1016 / j . bcra . 2021 . 100014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2096720921000099.

[31] KILT, What is kilt?, Accessed: Aug. 12, 2024. [Online]. Available: https://docs.kilt.io/docs/ concepts/what-is-kilt/.

[32] Polkadot, Defy what's possible, Accessed: Aug. 12, 2024. [Online]. Available: https : //polkadot.com/.

[33] R. A. Pava-Díaz, J. Gil-Ruiz, and D. A. López-Sarmiento, „Self-sovereign identity on the blockchain: Contextual analysis and quantification of ssi principles implementation“, Frontiers in Blockchain, vol. 7, 2024, ISSN: 2624-7852. DOI: 10.3389/fbloc.2024.1443362. [Online]. Available: https://www.frontiersin.org/journals/blockchain/articles/10. 3389/fbloc.2024.1443362.

[34] KILT, Enterprise-use case, Accessed: Nov. 07, 2024, 2024. [Online]. Available: https://www.kilt.io/enterprise/use-cases.

[35] H. foundation, Hyperledger foundation projects aries, Accessed: Aug. 22, 2024, 2024. [Online]. Available: https://www.hyperledger.org/projects/aries.

[36] D. Li, W. E. Wong, and J. Guo, „A survey on blockchain for enterprise using hyperledger fabric and composer“, in 2019 6th International Conference on Dependable Systems and Their Applications (DSA), 2020, pp. 71–80. DOI: 10.1109/DSA.2019.00017.

[37] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. Habib ur Rehman, and C. A. Kerrache, „The case of hyperledger fabric as a blockchain solution for healthcare applications“, Blockchain: Research and Applications, vol. 2, no. 1, p. 100 012, 2021, ISSN: 2096-7209. DOI: https://doi.org/10.1016/j.bcra.2021.100012. [Online]. Available: https://www.sciencedirect.com/ science/article/pii/S2096720921000075.

[38] Privado.ID, Building digital identity, Accessed: Aug. 22, 2024, 2024. [Online]. Available: https://www.privado.id/.

[39] E. Hotta, Self-sovereign identity use cases, Accessed: Nov. 10, 2024, 2022. [Online]. Available: https://cheqd.io/blog/self-sovereign-identity-use-cases/.

[40] J. Cole, Use cases of ssi in everyday life, Accessed: Nov. 10, 2024, 2024. [Online]. Available: https://blockapps.net/blog/use-cases-of-ssi-in-everyday-life/.

[41] Dock, Self-sovereign identity: The ultimate guide 2024, Accessed: Aug. 22, 2024, 2024. [Online]. Available: https://www.dock.io/post/self-sovereign-identity.

[42] M. Heinig, How self-sovereign identity improves online trust, Accessed: Nov. 10, 2024. [Online]. Available: https : / / www . sap . com / germany / insights / viewpoints / ext - how - ssi - improves-online-trust.html.

[43] M. H. Saeed, W. Fangzong, B. A. Kalwar, and S. Iqbal, „A review on microgrids' challenges & perspectives“, IEEE Access, vol. 9, pp. 166 502–166 517, 2021. DOI: 10.1109/ACCESS.2021.3135083.

[44] D. T. Ton and M. A. Smith, „The u.s. department of energy's microgrid initiative“, The Electricity Journal, vol. 25, no. 8, pp. 84–94, 2012, ISSN: 1040-6190. DOI: https://doi.org/10.1016/j.tej.2012.09.013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1040619012002254.

[45] G. C. Okwuibe, T. Brenner, M. Yahya, P. Tzscheutschler, and T. Hamacher, „Design and evaluation of architectural framework for a secured local energy market model based on distributed ledger technologies“, IET Energy Systems Integration, vol. n/a, no. n/a, 2024. DOI: https://doi.org/10.1049/esi2.12136. eprint: https://ietresearch.onlinelibrary. wiley . com / doi / pdf / 10 . 1049 / esi2 . 12136. [Online]. Available: https : / / ietresearch . onlinelibrary.wiley.com/doi/abs/10.1049/esi2.12136.

[46] Introducing Polygon ID, Zero-Knowledge Identity for Web3. Accessed: Jul. 2, 2025. [Online]. Available: https://polygon.technology/blog/introducing-polygon-id-zero-knowledge-own-your-identity-for-web3

[47] Supercharging the IDtech Category: Trinsic’s Vision for the Future. Accessed: Jul. 2, 2025. [Online]. Available: https://trinsic.id/tag/ssi/

[48] Seamless Portable Identities. Market-leading decentralized identity and Verifiable Credential solutions for streamlined authentication, access management, and more. Accessed: Jul. 2, 2025. [Online]. Available: https://indicio.tech/

[49] ION. Accessed: Jul. 2, 2025. [Online]. Available: https://identity.foundation/ion/

[50] What Is Hyperledger Indy? Accessed: Jul. 2, 2025. [Online]. Available: https://sovrin.org/faq/what-is-hyperledger-indy/

VDE Verband der Elektrotechnik
Elektronik Informationstechnik e. V.

Merianstraße 28
63069 Offenbach am Main
Germany
Phone +49 69 6308-0
service@vde.com
www.vde.com

VDE