SSI IN THE ENERGY SECTOR: A STUDY

PROJECT MANAGERS:
Sebastiaan Coppenholle and Kai Schmied, Elia Group

WRITERS:
Vincent Gramlich, Dr. Marc-Fabian Körner, Anne Michaelis and Prof. Dr. Jens Strüker, Branch Business & Informations System Engineering, Fraunhofer Institute of Applied Information Technology FIT

CONTRIBUTORS:
Energy Web

01 EXECUTIVE SUMMARY

As the energy landscape becomes increasingly and rapidly decentralised, Elia Group recognises the potential for self-sovereign identity (SSI) technology to fulfil the pressing need for a secure and efficient way to verify participant identities. This paper highlights the transformative power that SSI holds. It outlines several SSI use cases, exemplifying how SSI can be employed to redefine identity management and data exchanges across the sector.

Unlocking the potential of SSI will require deliberate, collaborative action to be taken. To ensure SSI is widely adopted, Elia Group believes it is imperative to bring together regulators, industry consortia and forward-thinking companies to create standards, address interoperability issues and manage regulatory uncertainties. As an initiator of such discussions, Elia Group is calling for unity and strategic foresight from stakeholders as they join hands on this transformative journey. Through the adoption of an ecosystem approach, the energy sector can make good on the promise of SSI, enabling a future that is more efficient, secure, and prioritises individual sovereignty in the digital world.

02 BUILDING THE ENERGY SECTOR OF THE FUTURE

The global energy landscape is undergoing a profound transformation: energy systems are having increasing amounts of decentralised renewable sources integrated into them. Millions of distributed energy resources (DERs) – from household devices such as heat pumps and solar panels through to wind farms – are contributing to more sustainable, renewable energy systems. These complex, interconnected systems require extensive information exchange to be facilitated between numerous parties: people, corporate entities and devices. One key challenge lies in ensuring that this swapping of information can occur in both an efficient and stable manner, with parties being able to trust each other and the information they send and receive.

Consider a homeowner named Anna who is a prosumer: she both produces and consumes electricity. Anna's smart home is fitted with solar panels, a home battery, a charger for her electric vehicle (EV) and an energy management system. Surplus electricity generated by Anna's solar panels is fed back into the grid. Anna wants to charge her EV with the green energy she has fed into the grid, ensuring that the energy it consumes originates from renewable sources. When her EV doesn't need charging, Anna wants to make the most out of the energy she generates by, for example, selling it on the wholesale market or selling it to her mother (who lives elsewhere), or by using her battery to stabilise the grid.

Anna's case highlights the complexity of a decentralised energy landscape. There is a critical need to accurately identify and verify the multiple entities involved in the transactions she wants to initiate, from Anna herself through to the assets she owns and the other parties across the system. Trusted, verifiable information about these entities, including details about charging tariffs, technical specifications, contracts, and personal information, is crucial for the system to function correctly.

This paper explores one possible way that decentralised assets can be enabled to participate in the broader energy system: self-sovereign identity (SSI). This technology provides a digital identity model which, similar to digital passports, provides identities for asset owners and the assets themselves and allows statements about these entities to be validated. SSI ensures that entities can be securely and efficiently identified, verified and integrated into a dynamic, decentralised environment.

DECENTRALISATION IN THE ENERGY LANDSCAPE

03

The millions of DERs that need to be integrated into our energy systems have the potential to contribute to their smooth functioning and could significantly facilitate the many areas that need to be managed by transmission system operators (TSO) such as Elia and 50Hertz. Recognising this, Elia Group has launched several projects which aim to facilitate the shift to a more decentralised, consumer-centric energy system.

1. Energy market and flexible supplier switching:

The most immediate use case involves enabling DERs to participate in energy markets. At the moment, regulatory hurdles – including those relating to the exchange of energy – are hampering smaller players from entering the market. In response to these challenges, Elia Group launched its Consumer-Centric Market Design (CCMD) in 2019[1]. Its goal is to enable all participants to exchange energy with consumers or producers located in the same zone as them, with the amount they sell this energy for being deducted from their main energy bill. This flexibility will enable responsibilities to be allocated dynamically, will enable energy tariffs to be established for specific devices, and will enable consumers to switch suppliers. As a result, consumers will be able to seamlessly switch suppliers or have different suppliers for different assets.

Under the CCMD, Anna would be able to seamlessly switch energy supplier, picking the one that suits her best, or have different suppliers for the different assets she uses. Anna could have two suppliers: one that offers her the best tariffs for her non-flexible assets, and a second that offers her a flexible tariff which she can use to optimise the use of her flexible assets.

2. Grid operations support and balancing power:

DERs can also provide valuable support for grid operations, especially in terms of frequency control. As we move away from relying on centralised thermal power plants for our energy to relying on intermittent renewable energy sources, decentralised demand assets must be enlisted to provide flexibility services, such as those offered up as part of the Frequency Containment Reserve (FCR), Automatic Frequency Restoration Reserve (aFRR) and manual Frequency Restoration Reserve (mFRR) processes. In such cases, DERs need to be identified in order to quickly react and provide services to the grid.

In the future, Anna could be remunerated for charging her battery (so increasing demand) or injecting power back into the grid from her battery at times when the grid needs it. However, for the average prosumer, the hurdles to overcome need to be very low and the benefits must be clear and appealing.

[1] Consumer-Centric Market Design (CCMD), Elia Group: https://www.eliagroup.eu/en/ccmd

3. Adequacy and capacity remuneration mechanism (CRM):

As the number of DERs continues to grow, they can play a part in providing adequacy services – through participating in the Belgian CRM, for example[2]. The CRM, which is enshrined in Belgian legislation, aims to ensure the country's long-term security of supply by incorporating supply-side flexibility into the capacity market. Such mechanisms are vital for maintaining system stability as the generation mix becomes increasingly diverse.

Just as for the provision of flexibility services, in the future, Anna could also be remunerated for providing capacity to the grid via her battery. However, she would need to be able to do this without much effort, or without her levels of comfort being limited.

4. Energy communities and home energy management:

The rise of prosumers needs consumption and peer interactions to be optimised to enable energy sharing to occur within communities. Home energy management systems gather together and share metering data from household devices, enabling data-driven decision-making related to the optimisation of an individual's energy use.

In Anna's case, this would mean her home would autonomously adjust its energy consumption patterns in line with the needs of the local grid, and Anna would also be able to share or sell surplus energy to her mother, ensuring she gets the most out of her energy investments without needing to manually interfere in the process.

5. Granular certificates of origin:

A number of projects are underway to develop certificates that verify the origin of energy, empowering consumers to make more informed decisions about the electricity they consume and stimulate demand for green energy.

Through such a scheme, Anna would have access to transparent information relating to the energy she uses. It would enable her to confidently claim that the energy she consumes is green, in line with her environmental beliefs and possibly allowing her to avail of benefits or incentives associated with sustainable consumption.

For all these use cases to work efficiently and effectively, the onboarding, communication, planning, and optimisation processes need to be digitalised.

Finally, trust must form the foundation of any decentralised energy model. There must be trust in data authenticity, entity identity, and transactions. Achieving this trust requires a secure, reliable solution for verifying entity information and participation. Each of the aforementioned use cases would therefore only work if a solution providing trust is in place. SSI is one such solution.

[2] Capacity Remuneration Mechanism, Elia: https://www.elia.be/en/electricity-market-and-system/adequacy/capacity-remuneration-mechanism

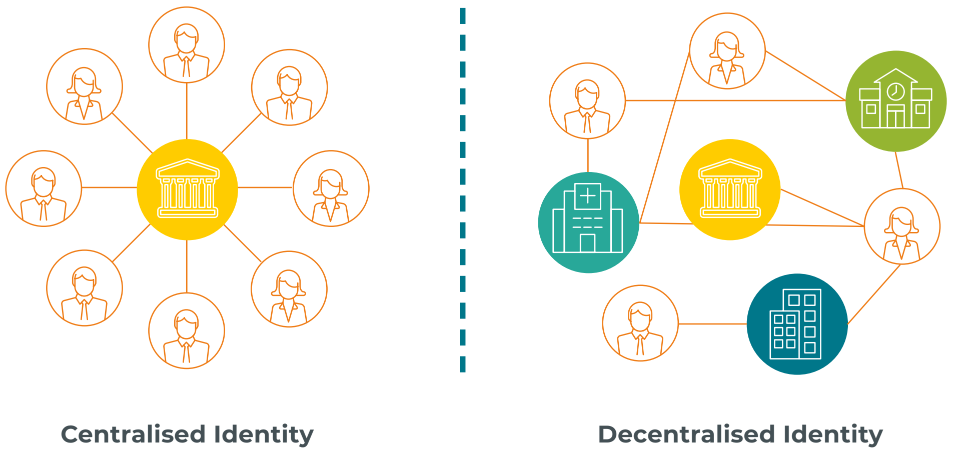
SSI: A USER-CENTRIC APPROACH TO IDENTITY MANAGEMENT 04

As the energy system becomes increasingly decentralised, certain processes – customer authentication, contract services, consent management, asset registries, and metering data access – need to be redesigned for scalability to accommodate millions of users. These processes currently lack efficiency and rely heavily on manual input. SSI could provide secure, scalable and decentralised solutions for this, aiding the energy sector's digital transformation.

SSI is one approach to digital identity management that tries to maximise the control individuals have over the use of their own information. It is a form of decentralised identity management, since it tries to differentiate itself from centralised identity solutions like single sign-on (SSO) schemes, as part of which data is held and controlled by a third party (such as a big tech company, for example).

The data involved in SSI transactions is not limited to details included in traditional documents like passports or ID cards, but can cover a whole spectrum of information, from personal attributes through to memberships and qualifications. Digital identities can be assigned to individuals, corporations, machines or products.

FIGURE 1: COMPARISON BETWEEN CENTRALISED AND DECENTRALISED IDENTITY MANAGEMENT SCHEMES[3]



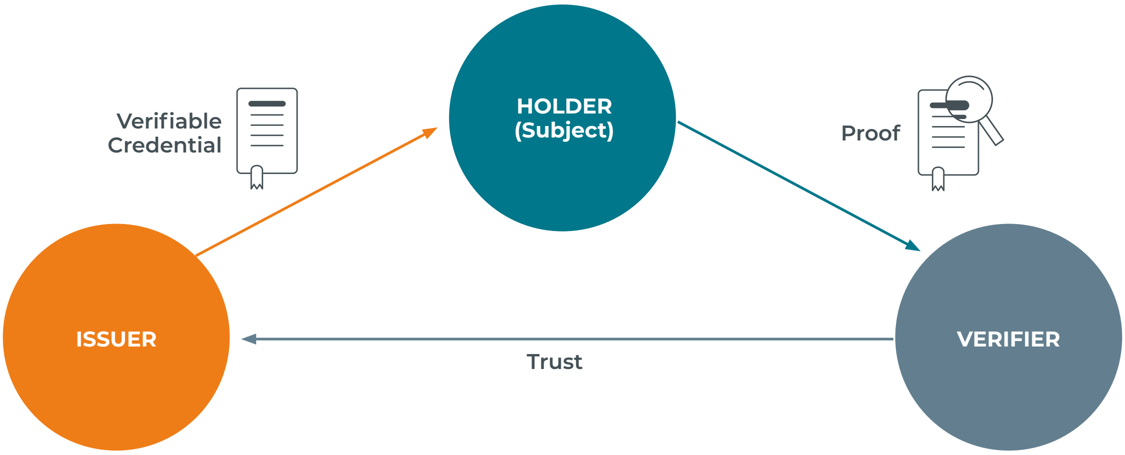
[3] How GCOM's Decentralized Identity Solution Compares to Existing Digital ID Solutions, GCOM: https://www.gcomsoft.com/insights/how-gcoms-decentralized-identity-solution-compares-to-existing-digital-id-solutions/

CORE ROLES IN SSI

There are three core roles in an SSI system. The first role is that of **the holder** - a user or identity owner who is responsible for managing their own data in their wallet. The second is that of **the issuer**, who is responsible for issuing verifiable credentials (VCs) which are linked to a holder's identity data; issuers do this by embedding identity-related data on a VC and issuing this to the holder, which the holder can then store in their wallet. The third role is that of **the verifier**, or requester of identity-related data. Holders present different VCs to verifiers in line with the latter's needs, confirming their identity as part of a process known as a Verifiable Presentation (VP).

As displayed in Figure 2, the holder, issuer and verifier form an SSI verification process called a 'trust triangle'; the holder is at the centre of this triangle, receiving VCs from issuers and presenting VPs to verifiers. No direct communication takes place between the verifier and issuer, meaning that holders have more control over their data, enjoy increased privacy, and can be selective about which specific bits of data they wish to disclose to different verifiers. For example, a holder can choose to share the details of their energy contract with a verifier whilst withholding information about their last metering position.

FIGURE 2: TRUST TRIANGLE[4]



[4] Strüker, J., Urbach, N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Schlatt, V., Sedlmeir, J., Stoetzer, J.-C., Völter, F. (2021): Self-Sovereign Identity - Foundations, applications, and potentials of portable digital identities. Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT, Bayreuth

A DETAILED LOOK AT THE AUTHENTICATION PROCESS

The lifecycle of a VC provides more information about how SSI works. VCs store identity information in the form of attributes, which are unique identifiers of the holder. These attributes are signed using a form of encryption known as 'asymmetric key cryptography' or 'public-key cryptography'. Each attribute is associated with a decentralised identifier (DID) and is linked to key pairs: a public key for encryption (which is published) and a private (secret) key to unlock the public key and access the data. Data that is encrypted with the public key can only be decrypted with its corresponding private key[5].

Once the issuer issues a verifiable credential to the holder, the holder can use it to confirm specific information about their identity to verifiers as part of the VP process. Verifiers confirm the origin and integrity of DIDs through the use of public key infrastructure (PKI) and by checking the issuer's signature. This process is carried out via secure communication channels.

Besides digitalising and automating the process of verifying identity-related information, the SSI approach allows holders to select which credentials they would like to share with verifiers: if they wish, they can disclose individual DIDs instead of an entire VC[6]. In real situations today, ID card holders have to reveal all of the data held on their ID cards when showing them to a cashier in a shop or using them to prove their identity online. In the hypothetical situation described below, however, holders can choose to disclose data in a selective manner, only revealing the information that the verifier needs at a particular moment in time, such as the holder's age - or even just the fact that the holder is old enough to buy a particular product.

Let us consider a hypothetical trust triangle involving:

- the issuer of Anna´s ID card - her local passport office or town hall;
- Anna, as the holder of the ID card;
- a verifier, such as an online shop that sells age-restricted goods.

Anna is able to use the VC that represents her digital ID card to undertake a VP, based on which the online shop can verify that she is above the required age and that the certificate has been issued by a governmental body. Anna chooses to only declare her age to the online shop and chooses to omit all other information that is held on her ID card.

REVOCATION REGISTRY

In systems like SSI, issuers must have a way to revoke the VCs they have issued in the past, since identity information can become outdated. A revocation registry is therefore necessary; this enables issuers to issue signed messages that revoke or alter certain VCs. This registry must be accessible to all potential verifiers to check the revocation status of a VC. This requirement could be achieved through various means, with one possibility being via a blockchain operated by different issuers in the SSI ecosystem.

WALLETS AND STANDARDS

Facilitating SSI processes (the issuing, holding, presentation, and verification of VCs) requires secure communication channels and the management of cryptographic key pairs, all of which are facilitated by wallets. Wallets are available in various forms and can be digital wallets or hardware wallets, which store cryptographic keys onto dedicated hardware.

Data exchange within an SSI ecosystem must be standardised, since wallets must be able to recognise data formats and communication protocols in order to handle them. Global VC standards are necessary to achieve the interoperability potential of SSI, allowing VCs to be used across different domains. Currently, the lack of these standards is preventing the widespread adoption and seamless interaction of SSI systems across different domains.

[5] Public key cryptography – IBM documentation

[6] This selectivity is facilitated through signature schemes like Camenisch Lysyanskaya (CL) or Boneh-Boyen-Shacham (BBS+), or by using general purpose zero-knowledge proofs (e.g. SNARKs)

05

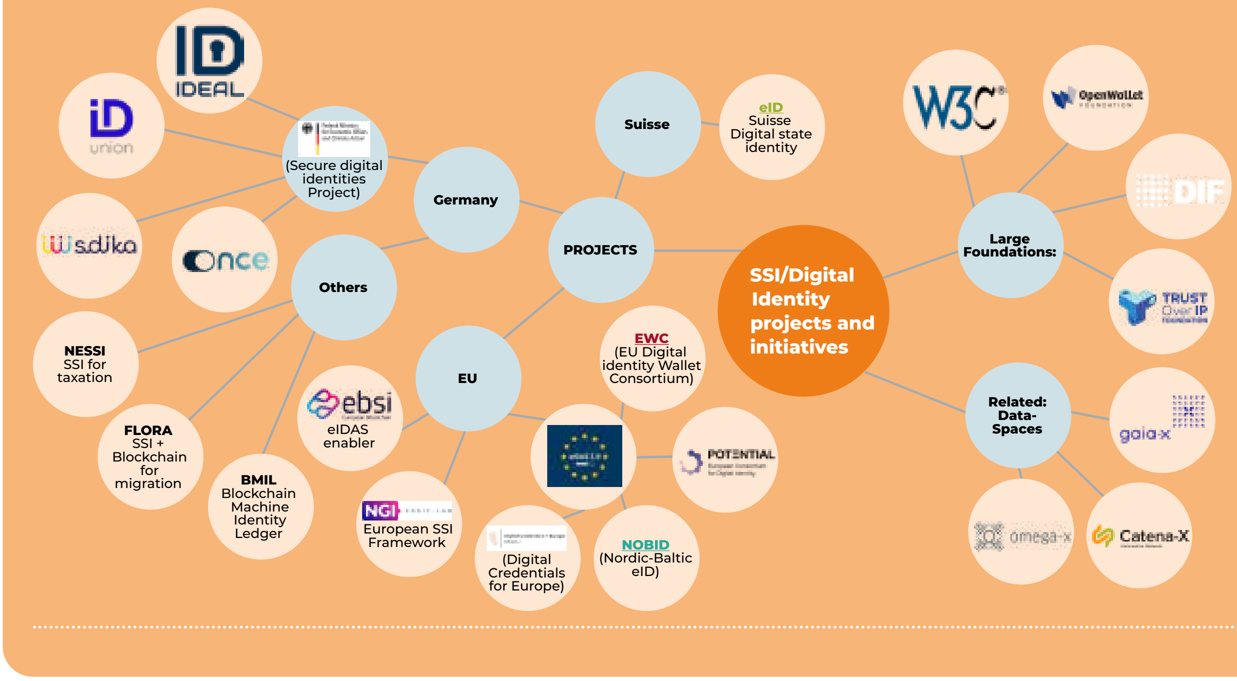
CURRENT STATUS OF SSI

The field of SSI is gaining importance as different sectors are digitalised. The proliferation of digital identities requires highly secure and user-friendly verification methods to be employed. Governments and private companies are actively seeking out solutions that leverage SSI or similar digital identity management approaches.

eIDAS 2.0 Regulation: As a comprehensive European regulation that covers electronic identification and trust services, eIDAS 2.0 seeks to increase security and reliability levels in digital identification processes. It sets specific technical standards and requirements that EU Member States must meet, which are outlined in the 'European Digital Identity Architecture and Reference Framework' (EUDI ARF)[7]. The regulation mandates that all Member States provide digital identity wallets to their citizens and companies. By the end of 2023, every EU citizen should have access to a government-provided digital wallet.

Publicly funded projects: As seen in Figure 3 below, various projects funded by public authorities have been instrumental in establishing digital identity ecosystems. These include Europe-wide projects, such as the European Blockchain Services Infrastructure (EBSI) and Next Generation Internet (NGI) and also those funded by individual Member States. Notably, four large-scale projects focusing on the eIDAS 2.0 Regulation aim to convert the regulatory framework into tangible products. Additionally, the Blockchain Machine Identity Ledger (BMIL), which was funded by the German Federal Ministry for Economic Affairs and Climate Action, aimed to implement scalable and trustworthy asset identification in the energy sector using SSI-based machine identities.

FIGURE 3: OVERVIEW OF DIGITAL IDENTITY PROJECTS AND INITIATIVES


IDEAL
iD union
(Secure digital identities Project)
Germany
Suisse
eID Suisse Digital state identity
PROJECTS
SSI/Digital Identity projects and initiatives
wsdika
Once
Others
NESSI SSI for taxation
FLORA SSI + Blockchain for migration
BMIL Blockchain Machine Identity Ledger
ebsi eIDAS enabler
EU
NGI European SSI Framework
(Digital Credentials for Europe)
EWC (EU Digital identity Wallet Consortium)
POTENTIAL
NOBID (Nordic-Baltic eID)
W3C
OpenWallet FOUNDATION
DIF
Large Foundations:
TRUST Over IP FOUNDATION
Related: Data-Spaces
gaia-x
omega-x
Catena-X

[7] European Digital Identity Architecture and Reference Framework – Outline, European Commission: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline

Industry-funded work: Many companies are exploring SSI solutions due to their potential business value. Tech giants like IBM, Microsoft and Google, as well as European companies such as Bosch and Siemens, have invested in the development or integration of SSI-based solutions. Besides their involvement in publicly funded projects, these companies also fund their own SSI projects, often in collaboration with leading research organisations and technology firms. A good example of this is the project being worked on by KBC and the University of Applied Sciences in West Flanders, which involves launching the very first digital student card which will enable students to prove their student status more easily via digital means, whilst enjoying enhanced privacy protection[8].

Elia Group: As part of the ReBeam project, Elia Group, the Energy Web Foundation and Bloxmove aimed to allow individual charging processes to be registered, allowing customers to select a supplier when charging their EVs at public charging stations. ReBeam involved the use of a virtual balancing area (VBA) to settle the energy amounts involved. SSI was used to create trust among each party and trust in the exchange of data. This led to leaner processes, fewer intermediaries, more flexibility being delivered for end users and an effective and targeted integration of charging processes into the network. Based on the takeaways from the project, Elia Group is currently supporting the DENA BMIL project, which is focused on the creation of a blockchain machine identity ledger which can be used for the registration of energy assets.

Digital identities and data spaces: Research about data spaces – or ecosystems for cross-organisational data sharing – is closely connected to digital identities and SSI. Data spaces require standardisation and data sharing infrastructure which is similar to those needed for a digital identity ecosystem. Projects such as Gaia-X and sector-specific initiatives like Omega-X and Catena-X are exploring these areas.

In conclusion, while digital identities and SSI carry immense amounts of potential, their widescale implementation requires further technological development and end user acceptance. The establishment of standards for different data formats and communication protocols is crucial for the creation of comprehensive digital identity ecosystems. While some standards are being set, as can be seen from work on the eIDAS 2.0 Regulation, the development of industry-specific use cases varies. Lastly, these identification processes must be integrated into existing business and administrative structures while ensuring end user comfort. Since consumer responsibility will increase significantly, end user acceptance will need to be encouraged[9].

[8] Howest and KBC will be launching Europe's first digital student card during the 2023-24 academic year, KBC Group: https://newsroom.kbc.com/howest-and-kbc-will-be-launching-europes-first-digital-student-card-in-the-coming-academic-year

[9] End users will, for instance, be asked to keep their private key safe; should they lose their private key, there will be no way to retrieve it

06 THE BUILDING BLOCKS NEEDED TO ENABLE A DECENTRALISED APPROACH

In order to identify possible industry applications for SSI, Elia Group has identified certain needs, or building blocks, which have to be established as we shift towards more decentralised energy systems. These building blocks are outlined below. Their implementation will vary depending on whether the system involved is a high-voltage or a low-voltage one, and how many users they affect. As previously mentioned, SSI could play a key role in facilitating the scalability of different processes with regard to the onboarding of millions of new users and their distributed energy assets.

CUSTOMER AUTHENTICATION: In high-voltage systems, customer authentication is often carried out through labour-intensive manual processes that cover information such as company data, VAT numbers and financial background checks. In low-voltage markets, existing identity providers are used, but the process still requires manual verification, meaning there is a significant gap to be filled in terms of automation and efficiency.

CONTRACT SERVICES: In high-voltage systems, customers and grid operators sign direct contracts with each other. However, in low-voltage markets, contracts are established between customers and their distribution system operators (DSOs) or energy service providers (ESPs). For instance, currently, if a party wishes to provide balancing services, they must provide a series of documents that includes a signed version of the grid user declaration, information about the connection point, flexibility provision and information with regards to the recuperation of energy. A streamlined contract management process that can handle a large number of customers efficiently would, particularly in low-voltage markets, speed up this process.

CONSENT MANAGEMENT: In high-voltage systems, consent management is built into automatic transactions, while customers in low-voltage markets manually give their consent to data holders and receivers. This method is inefficient, prone to errors, and often results in outdated permissions being used, leading to potential data protection violations. A more dynamic, automated, and reliable consent management system would make current processes more efficient.

ASSET REGISTRIES: In high-voltage systems, a centralised asset registry efficiently manages and tracks assets linked to access points and meters. For non-registry linked assets, such as decentralised energy resources, a new but labour-intensive onboarding process is required. In low-voltage markets, a scalable solution for managing an increasing number of assets is currently missing.

METERING DATA ACCESS: In high-voltage systems, grid operators can directly access metering data. In low-voltage markets, this can vary. In some regions, grid operators have direct access to smart meter data, while in others, the data is collected by DSOs and then forwarded to relevant parties, in line with user permissions. A comprehensive and up-to-date permission management system would greatly enhance the efficiency of data sharing and receiving.

While these building blocks are already in place in certain high-voltage systems, they are more urgently needed in low-voltage markets due to the larger number of users and the greater need for product automation. These building blocks would benefit from the integration of secure, scalable, and decentralised solutions like SSI to enhance efficiency and ensure trust in the energy sector's digital transformation.

07 APPLYING SSI TO ENERGY SECTOR PROJECTS AND PRODUCTS

In order to scale up the impact of SSI on these building blocks, Elia Group and the Fraunhofer Institute of Applied Information Technology (FIT) analysed the possibilities that exist in terms of applying SSI to the Group´s projects and products. Their conclusions led them to explore the potential held in streamlining the automated onboarding of customers and assets within registries for high and low-voltage markets. Moreover, they concluded that an enhanced verification of customer information can contribute to more reliable contract services by improving the efficiency of contract management and providing more accurate financial background checks. Similarly, interoperable and continuous permission management matches the need for a dynamic and automated consent management system and comprehensive metering data access, reducing the risk of data protection violations and improving the efficiency of data sharing.

As described above, SSI is still an emerging technology – making it perfect for integration into up-and-coming use cases that would greatly benefit from its qualities. To illustrate this, Elia Group focused on the three use cases below, as part of which the impact and potential of SSI was further explored.

AUTOMATED ONBOARDING OF CUSTOMERS

The first use case covers the identification of new customers, including businesses like DSOs, ESPs (or high-voltage clients) and individuals, such as end consumers that could have a direct or indirect business relationship with Elia Group.

Elia Group's interaction with low-voltage markets is increasing due to the latter's growing importance in the delivery of flexibility and the emergence of many new business models. This means that the number of individual customers and ESPs with which Elia Group interacts will grow immensely. Simultaneously, these identification processes currently depend on third party service providers such as *itsme* in Belgium, and still involve a lot of manual effort to be undertaken by both sides.

SSI-based customer authentication has the potential to provide verifiable identity information while eliminating the need for manual intervention, so providing a solution that could solve the issues in low-voltage markets. By leveraging digital identities and SSI, customers could hold their own identity credentials that would be issued by existing or new trustworthy identity providers (such as *itsme* and government agencies). When registering new customers, Elia Group would then be able to send a request for proof alongside the specific information it requires from its customers, which could be met with a VP from the customer that includes this information (based on the identity credentials the customer holds). Elia Group would consequently be able to verify the integrity of the data and check whether the information had been corroborated by a trustworthy issuer. Furthermore, this application could be extended to cover other bits of information like credit ratings, which could, for example, be confirmed by a bank.

This use case therefore proposes an automatable process for onboarding all of Elia Group's customers. This would enhance data privacy by involving the receipt and verification of specific bits of information that are required for specific customers.

MACHINE IDENTIFICATION OF ASSET REGISTRATION

The second use case relates to the identification of assets and their meters. This covers assets which consume and can re-inject electricity back into low- and high-voltage grids. Just as for the identification of new customers, the number of assets in low-voltage markets is several orders of magnitude larger than it is in high-voltage markets, resulting in dramatically larger requirements regarding the automation and scalability of onboarding processes. This has led to the current situation, in which the flexibility inherent in high-voltage assets is already being harnessed, whilst the harnessing of flexibility held by low-voltage assets is only just in the early stages of being explored. This discrepancy can be attributed to the fact that there is currently no suitable solution for onboarding low-voltage assets. However, unlocking these flexible, low-voltage assets is crucial for Elia Group's primary task: that of ensuring grid stability.

SSI-based machine identities can be used for the identification of assets and their meters, as also identified by the DENA BMIL project. As explained previously, digital identities can be assigned to legal entities, individuals and machines, so that their identity information (or master data) can be managed. In the case of assets and their meters, these could be equipped with machine identities that would include the data that is required for the onboarding of new assets, such as technical information, their location and ownership. The certificates that verify this information could be issued by the OEM of the asset, the meter, an installer, or auditor. The latter could then confirm that the asset had been correctly installed - in other words, that a metering device was indeed connected to a solar panel and not a diesel generator. These certificates could then be used by the asset itself or its owner to present the information Elia Group requires as part of the asset's registration process. Elia Group could, in turn, automatically verify the integrity of the data and the asset itself. Additionally, to make the process even safer, installers or auditors would be given the option to be certified by universally trustworthy institutions, such as the Federal Network Agency (Bundesnetzagentur) in Germany. This decentralised management process would enable a seamless and interoperable usage of asset master data for the asset owner, allowing them to use their asset and its data for all kinds of different applications instead of being bound to one centralised database and its operator.

Through this process, Elia Group would receive all the information it requires in an automatic and verifiable way. Thus, the use of SSI in asset identification presents a solution that would match the scalability requirements of low-voltage markets and eliminate the problem of faulty data due to malicious behaviour or human error (which tends to be a bigger problem in low-voltage markets).

CREDENTIALS AND REVOCATIONS IN PERMISSION MANAGEMENT

The third use case targets the third building block that is currently lacking in low-voltage markets: the management of permissions relating to data forwarding or usage.

Permission management is required since data transactions in the energy sector typically involve three roles: an owner of data (for example, Elia Group's ownership of metering data); a data holder (Elia Group's IT department); and a data user or receiver (asset owner/consumer). Elia Group may be a data holder in some cases and a data receiver in others. Permissions to share data with a receiver or forward it to other parties need to be granted by the data owner. Permission management is critical for almost all of the products and projects Elia Group is working on, and while it is already covered in contracts signed in high-voltage markets, this is not the case in low-voltage markets, due to the complexity of processes and systems currently in place.

Currently, the permission management process involves a manual approach that is carried out in data silos by different data holders and users in energy markets. This leads to situations in which a data owner might need to grant permissions for the same data, both to the holder, to allow the data to be forwarded to them, and to the user, entitling them to request and receive the data. Additionally, updating permissions (for example, if the ownership of an asset changes) is a complex process, meaning outdated permissions often arise.

By using SSI, permissions could be issued by the data owner in the form of VCs and be handed to the data holder or receiver. The recipient of the credential could present the information to the other party, which could in turn verify the validity of the permission, including both the integrity of the credential and other relevant details. Moreover, the VC could also be linked to proof that it was issued by the owner of the asset to which the data belongs, which would enable the verification of the permission's authenticity. Furthermore, a revocations registry could be used to store and display changes to permissions regarding the sharing of information. Managing this revocations registry would enable the asset owner and other authorised parties (such as a car certification authority if the asset is an EV) to change or revoke permissions.

Through the use of SSI, an interoperable permission management system with automatic verification and flexible permission revocation which matches current requirements could be released, especially in low-voltage markets.

CONCLUSION

In order for our decentralised energy system to function effectively, foundational building blocks must be put in place. The need for automated customer authentication, streamlined contract services, efficient consent management processes, comprehensive asset registries, and accessible metering data is paramount. Elia Group and the Fraunhofer Institute recognise the potential held in SSI to address these challenges; as the use cases above outline, it will ensure efficiency, reliability and trust.

However, implementing SSI could entail significant risks. It is only through collaboration that these can be mitigated. Players from across the energy value chain must come together to develop SSI standards, address interoperability issues and successfully weather regulatory uncertainty. We at Elia Group will gladly drive the formation and work of such a partnership, allowing us to collectively test out and shape solid standards and a functional SSI ecosystem that supports a smooth user experience.

We would therefore like to invite original equipment manufacturers (OEMs), distribution system operators (DSOs) and energy service providers (ESPs) and any other entities to join us in a collaborative effort to develop and test interoperable systems and improved user experiences. Elia Group believes that in an era of digitisation, embracing SSI is not merely a technological progression but a calculated leap that could significantly alter business operations.