24th International Conference on Business Information Systems (BIS 2021)
Smart Infrastructures
https://doi.org/10.52825/bis.v1i.68

Published: 02 July 2021

Exploring Potential Impacts of Self-Sovereign Identity on Smart Service Systems

An Analysis of Electric Vehicle Charging Services

Daniel Richter[1] [https://orcid.org/0000-0003-1549-5467], and Jürgen Anke[1] [https://orcid.org/0000-0002-9324-9387]

[1] Digital Service Systems Group, HTW Dresden, Germany

Abstract. Self-sovereign identity (SSI) is a new paradigm, which puts users back in control of their own digital identity. This does not only strengthen the position of the users but implies new interaction schemes that may improve interoperability and usability. Smart services systems enable the integration of resources and activities and use smart products as boundary objects. As such systems typically involve digital interactions between multiple actors, it can be assumed that utilising SSI has a positive impact on them. To investigate how these potential improvements manifest themselves, we investigate electric vehicle charging as example of a smart service system. At the core of our conceptual analysis is the service process, which we extract from a reference model. Based on a SWOT analysis, we identify areas for transformation and derive an SSI-enabled interaction model for an electric vehicle charging service. The evaluation of the new process shows that SSI can reduce complexity of integration with partners and can provide a better customer experience through simplified registration and authentication. Moreover, SSI might even lead to the disintermediation of actors in the service system. Although SSI is still emerging, our findings underline its relevance as a mechanism to establish trust in smart service systems through the seamless and standardised integration of digital identities for humans, organisations, and things.

Keywords: Self-Sovereign Identity, E-Mobility, Service Design, Smart Service Systems, Service Process

1 Introduction

1.1 Motivation

Digital services require trust between the involved parties. Therefore, participants in transactions need to prove their identity in some way. As the internet has no built-in identity protocol [1], various approaches have been developed in the past. In the isolated model, online services are at the centre of the identity ecosystem, as each one requires users to register a user account with them, which then can be used together with a password to log in [2]. This leads to many user accounts (“logins”), which are spread among various service providers. In the federated model, dedicated identity providers are utilised, where the user registers once. Afterwards, their identity can be verified at online services that support the respective identity provider [2]. Popular examples include so-called social logins, such as the ones offered by Google, Facebook, and Microsoft. Their major drawback is the dependency of both the user and the service on identity providers [3] as well as the potential tracking of the usage behaviour [4] to create detailed user profiles. These might become part of data-driven business models such as targeted advertising [5]. Additionally, they are attractive targets for identity theft [4].

Self-sovereign identity (SSI) is the most recent approach and enables users to manage their digital identities on their own [2], [6]. In addition to strengthening users, SSI could also provide benefits from an interoperability and process perspective [4]. The SSI approach has mainly been discussed within the field of security, privacy, and distributed system but barely within information systems research. At present, there are only few academic papers on the application of SSI in business scenarios. They include the application of SSI in "know-your-customer" processes in banking [7], access to public health services [8], remote management of industrial equipment [3], payback programmes in retail [9], student exchange [10], e-petitions [11], assigning medical information to persons without regular identity, e.g. to fight Covid-19 [12]. Most of these scenarios represent typical business process or digital services.

In this paper, we aim to identify potential impacts of SSI in smart service systems, which can be defined as "service systems in which smart products are boundary-objects that integrate resources and activities of the involved actors for mutual benefit" [13, p. 12]. Examples for smart services include car sharing, pay-per-use models for industrial equipment, and remote diagnostics for household appliances [13], [14]. Digital identities are relevant to smart service systems as they need mechanisms for establishing trust between the involved actors. Typically, this requires the development of proprietary apps, individual customer registration processes, and legally compliant management of personally identifiable data (PII). Moreover, these measures need to be reconciled between all actors in the service ecosystem, which causes interoperability challenges. At the same time, users are confronted with complicated tasks like registration, managing passwords, setting up multi-factor authentication that impede the adoption of such services [15]. SSI promises lower usage barriers through simplified verification of identities and thus fewer steps for registration and authentication. Both privacy as well as ease of use have been found to have a positive impact on customer experience of smart services [14].

For our study, we have chosen the smart service system of contractual electric vehicle (EV) charging with roaming capabilities. In this domain, there are multiple actors involved in both the operation of charging points and the billing of the charging. Roaming providers act as intermediaries to simplify access to charging points in different regions. Existing research on electric mobility highlights the problem of interoperability and complexity [16], e.g., through a model-based framework [17]. Therefore, we have posed following research questions:

- RQ1: How can SSI improve the design of an EV charging service (EVCS) system with roaming capabilities?
- RQ2: What are implications of these changes for actors involved in the service system?

Our expected result are (1) a set of areas in which smart service systems can benefit from SSI, and (2) implications for involved actors, if SSI is used in such systems. With that, we aim to create an initial understanding of the potential that SSI might provide for the design of smart service systems. Furthermore, we strive to uncover future research opportunities in this field.

1.2 Methodology

Our *research objective* is to understand the implications of applying SSI to smart service systems. As SSI has not been widely used yet, we intended to explore the potential impacts of SSI on the specific use case of roaming in EVCS using a conceptual analysis of a reference process. For that, we have chosen the following *research approach:*

1. Identify characteristics of SSI from literature that are relevant for service system design,
2. Extract reference model of service system from roaming standards as a basis for a qualitative comparison,
3. Perform a SWOT analysis to identify potential areas of improvement of the service system through the exploitation of potential benefits created by SSI,
4. Derive an improved model of SSI-enabled EV charging with roaming capabilities,
5. Discuss the implications for the involved actors resulting from these changes.

2 Conceptual Foundation

2.1 Application of Self-Sovereign Identities in Business Scenarios

The paradigm of SSI puts the user at the centre of the identity ecosystem and back in control of his or her identity data. Identities for various subjects can be registered, resolved, updated or revoked without a central authority [4]. Identities are rooted in immutable data registries, which are also not necessarily controlled by a central authority like a government or a private company [4], [6]. Such registries are typically implemented using distributed ledger technologies (DLT) [18]. Using a software client called “wallet”, the user can collect cryptographically secured claims (credentials) about various attributes of his or her identity, which are provided by trustworthy institutions (issuers). The user (holder) can then present a subset of these attributes to service providers (verifiers) upon request [4], [6] in a peer-to-peer (P2P) communication, i.e., without an intermediary. As the credential is cryptographically verifiable, the issuer does not need to be contacted, which prevents tracking and correlation of user activities. Finally, digital identities are not only applicable to persons, but also to organisations and objects, e.g., technical products [3].

There is an ongoing effort to increase the interoperability of SSI-based solutions through standards. Most notably are the W3C standards ”Decentralized Identifiers” (DID) [19] and ”Verifiable Credential” (VC) [20]. A DID is an identifier according to the Uniform Resource Identifier specification, which uniquely identifies a DID subject. A DID refers to a DID document that defines service endpoints, which can be used to interact with the DID subject. It is common practice to create a new DID for each new business relationship, which prevents correlation of user data and thus ensures a high level of data protection [11]. VCs allow for complex interactions between participating entities, which are identified by their DIDs. The authenticity of a VC’s contents is verifiable by cryptographic methods. Furthermore, the integrity of a VC can be proven by persisting a hash in an immutable data registry serving as a fingerprint.

In the existing literature on SSI in business scenarios, the following benefits are mentioned:

- User data does not need to be stored at the service provider [7]
- Identity issuer is not involved in identity access, verification, and resolution [7], [8], [10]
- Identity data integrity and availability is ensured [7]
- Privacy of users is ensured [7]–[12]
- Users can trade their data for rewards [9]
- Users can link different identity attributes from various issuers on their own [10]
- Anonymous participation in transactions [11], [12]

Besides these, also critical issues were raised that limit the adoption of SSI:

- Lack of effective key management [7]
- Insufficient knowledge on alignment of technical, institutional, and societal aspects [12]
- Frameworks are not production-ready and prone to feature changes [3]
- SSI is in early stage and lacks of widespread adoption [3]
- Incomplete standardisation hampers interoperability [3]

2.2 Electric Vehicle Charging Services

EVCS are embedded in a larger ecosystem of smart energy and mobility services. The diverse actors within this ecosystem are characterised by different goals and business models. These actors and their relationships are described by the E-Mobility Systems Architecture (EMSA) [17] as well as the industry standard Open Charge Point Interface (OCPI) [21]. We used these as a theoretical foundation to derive an exemplary model of an EVCS with roaming capabilities. Roaming can be understood as a special feature of such services allowing a customer to charge at a multitude of charging stations of operators they have no direct contractual relationship with [22]. Services without explicit contractual relationships such as ad-hoc charging were out of scope of our research.

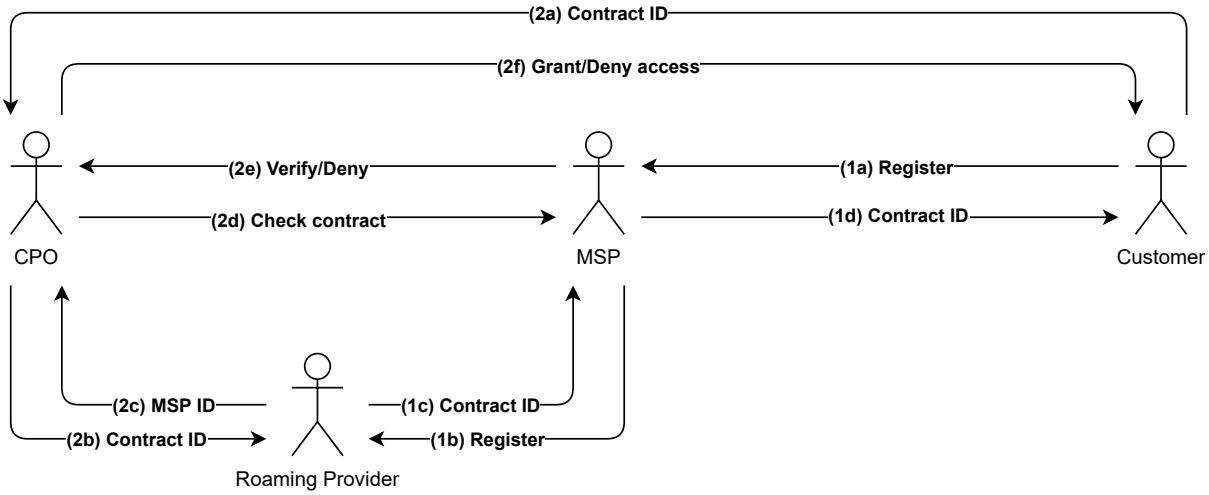

Figure 1. Interactions during registration and authentication of customers in an EVCS

2.2.1 Common Roles in Roaming Scenarios

There are four main roles in EVCS systems as described in EMSA [17] and OCPI 2.2 [21]. The descriptions given below are based on the assumption of a hub-based service topology for the exchange of contractual data [21], to provide an EVCS with roaming capabilities.

The **Charging Point Operator (CPO)** manages and operates charging points. CPOs enable potential customers to recharge their EVs. However, CPOs are geographically limited in acquiring new customers and compete locally with other CPOs. As a result, CPOs depend on MSPs as brokers to market their charging services and reach customers outside their main region of activity, in order to gain a competitive advantage.

The **Mobility Service Provider (MSP)** provides customers with services to enhance personal mobility, including access to charging points of several CPOs under a common contract. This simplifies billing for customers since the MSP handles the payment processing with involved partners. Furthermore, by aggregating demand, MSPs may offer lower prices to customers. The role of MSP may also be assumed by a CPO that is active in multiple regions.

The **Roaming Provider** acts as intermediary between MSPs and CPOs and manages a business technology platform for the uniform exchange of charging authorisations. Roaming providers form regional ecosystems for technological cooperation and creation of common standards.

The **Customer** initiates the charging session, confirms its completion, and pays for the process. Furthermore, a customer enters contractual relationships with an MSP to take advantage of mobility options or alternative billing models. Specifically in roaming scenarios, a customer only indirectly pays for the charging provided by the CPO via the MSP. In the domain of electric mobility, the customers experience regarding the relationship to service providers was described as negative, especially mentioning a lack of integration [14].

2.2.2 Interactions during Roaming Scenario

Using the specifications from OCPI 2.2 [21], we examined the following three processes to describe a roaming scenario in an EVCS system:

1. Registration of CPO and MSP to the roaming platform
2. Registration of customer to an MSP
3. Authentication of customer at a charging point

For clarity, we modelled the interactions within these processes in figure 1 without the initial registration of CPO and MSP to the roaming platform.

During registration, the customer provides the selected MSP with PII data that is relevant to invoicing. Once the customer has decided on a tariff, the contract information is transmitted to the roaming platform. It generates an identifier, which allows the mapping of the customer to possible CPOs according to the selected tariff. Finally, the customer is provided with the identifier, which can be presented at the charging points as stipulated in the service agreements. The contract identifier is further passed on by the corresponding CPO to the roaming platform, which locates the associated MSP. The MSP is then contacted by the CPO regarding the validity of the contract corresponding to the presented identifier. If the authentication is successful, a confirmation message is sent that leads to the release of the charging point.

3 Results

3.1 Identification of Options for Applying SSI in EV Charging Services

To explore the expected impacts of SSI on EVCS systems, we conduct a SWOT analysis. The internal perspective is based on the analysis of the presented exemplary EVCS system. The external perspective is represented by the opportunities and threats associated with SSI as described in section 2.1. Figure 2 shows an overview of the analysis inputs.

First, roaming strengths as identified by analysis of the industry standard documents should be highlighted. Charging services with clearly defined and uniform interfaces for customer interactions have a high degree of maturity. If the service processes can be handled via an application issued by the MSP, a streamlined activity of registration can be assumed, as no physical documents have to be exchanged to establish the contract. At the service providers, the lack of a requirement to manage physical contract documents reduces to redundancies in master data. While agreeing on a common roaming platform simplifies the processes between MSPs and CPOs to a certain extent and responsibility can be handed over, weaknesses still arise from this intermediation scenario.

The quasi-standardisation by roaming platforms leads to an accumulation of market power. MSPs and CPOs are dependent on the roaming providers to effectively manage their services, as they can only easily enter into business relationships with partners who are on the same platform. Being active on several platforms is either not possible due to regional monopolies or is economically unreasonable. In a competitive scenario, this leads to a limitation of the number of charge points that can be used by a customer under a single contract and thus negatively impacts the added value provided by roaming roaming capabilities.

The opportunities for potential applications of SSI approaches can be taken directly and indirectly from the so-called ten principles of SSI defined by Allen [23]. The most important opportunity is also the eponymous property of the SSI paradigm: Users should gain sovereignty over the data they own and thus enable them to decide which data is shared with whom. In conjunction with zero-knowledge proofs, it is also possible to prove the correctness of data without disclosing its contents [7]. The use of zero-knowledge proofs could therefore contribute to a lower utilisation of networks and databases. This could also reduce risks associated with data theft and improve data security in general. The use of DLT to implement SSI solutions could also increase transaction security, as it records business activities immutably in a decentralised ledger. This immutability provides the basis for the verifiability of the integrity of data used for business purposes and thus enables the issuance of verifiable documents without involving third parties. Initial efforts to standardise data formats and processes related to the aforementioned opportunities potentially enable the production of a uniform protocol for identity data exchange that is independent of specialised providers.

Despite the many opportunities for customers and service providers, the SSI concept is still in its infancy. While key components of the SSI architecture have been clarified and standards such as DID and VC emerge, there are still uncertainties in the details related to specific use

SSI Opportunities	SSI Threats
• Service providers do not have to maintain user data • Identity issuer not involved in identity access, verification and resolution • Integrity and availability of identity data is ensured • Users can consciously employ data in transactions • Users can link different identity attributes independently • Anonymous transaction participation	• Lack of effective key management • Insufficient knowledge on alignment of technical, institutional and societal aspects • Low number of production-ready frameworks lead to investment uncertainties • Low rate of adoption among users and service providers • Incomplete standardisation hampers interoperability
EV Charging Services Strengths	**EV Charging Services Weaknesses**
• Defined authentication method per service provider • Unique identifiers for authentication of end customers • Coordinated business partners due to role model • (Proprietary) standards for IT handling of business processes • Potentially low number of customer interactions	• Dependencies between business partners • Complex, interdependent processes • Intransparent business network • Interoperability across standards not guaranteed • Cumbersome administration of tariffs • Closed ecosystems

Figure 2. SWOT analysis inputs

cases. For example, the schema of VCs must be defined in advance to ensure interoperability between business partners in an industry. Additionally, for each industry a set of authorised institutions must be maintained that are widely accepted as trustworthy issuers. This complicates the design of such use cases with SSI approaches, as assumptions have to be made under uncertainty. On the other hand, this flexibility, which is still present at the beginning, enables the introduction of well-founded proposals for improving the SSI ecosystem.

From the mutual consideration of SSI opportunities and threats as well as strengths and weaknesses associated with EVCS, we can derive four strategic options for the application of SSI in these kinds of service systems.

- **Option 1:** Integrating SSI approaches into the contract creation process could simplify registration and subsequent authentication processes.
- **Option 2:** Using DIDs and VCs, MSP and CPO could emancipate themselves from the roaming provider as a trusted source of business identities.
- **Option 3:** The use of existing ecosystems and protocols from the domain of EVCS could relieve uncertainties related to the SSI standards under development.
- **Option 4:** The gradual implementation of components and the exchange with industry partners could promote interoperability between providers and a smooth transition to the SSI paradigm.

Based on options 1 and 2, highlighting the opportunities of SSI, the main direction of an EVCS system utilising SSI can be derived. With SSI approaches dedicated providers of identities and associated data objects are no longer necessary. Thus the role of roaming provider becomes obsolete. Instead of using a central platform for the exchange of contract data, SSI assumes an actor-centric perspective. SSI techniques can be applied at two points in the scenario of roaming. First, customers, MSP, and CPO can create and manage their own business identities utilising DIDs. Second, the business relationships between customer and MSP and between MSP and CPO as well as the associated rights and obligations can be represented in the form of VCs.

Cooperation in a complex business network requires a high degree of coordination, which is illustrated in particular by options 3 and 4. Since the removal of a central business partner from the service ecosystem represents a drastic change, the distribution of roles and tasks of the actors also changes in order to convey the same value to a customer. In the following sections we focus on the interactions that are relevant to the service provisioning at its core. As such, the financial clearing of the consumed services will be out of scope.

3.2 An SSI-enabled EV Charging Service System

Applying SSI technologies to an exemplary roaming service system following the presented options leads to changes in the interaction structure of said system. With the elimination of the roaming platform provider three actors remain in the EVCS system leading to three possible interactions which we have conceptually examined. An overview of the issuance and presentation of the credentials involved in the SSI-based service is provided in figure 3. The details of the actors' interactions are explained in the subsequent sections.

3.2.1 Interactions between CPO and MSP

The CPO provides the central service to a customer in EV charging. Thus, the CPO commissions an MSP to mediate their charging points under certain conditions. With VCs, it is possible to map the relationship between customers and MSP in a verifiable and persistent way. Therefore, the CPO can create a VC with the authorisation for these mediation activities and sign it with their private key. This "Broker VC" may be secured against misuse by two measures. First, the DID of the MSP could be included in the VC schema. Only the specified MSP and third parties authorised by this MSP could then prove that the MSP is in control. Second, a hash function could be used to record a fingerprint of the VC in an immutable registry so that its issuance could be proven. Furthermore, this "Broker VC" could contain an automatic expiration date following the contractual agreements between MSP and CPO. After the VC issuance, the associated MSP can store it in a self-selected location. With this VC, the MSP can verifiably broker the CPOs charging points at their own pricing, which makes up the core of an EVCS with roaming capabilities. After this, the mediation activities of the MSP is be electronically authorised by the "Broker VC", which is used as proof in case the services are contested by any party.

3.2.2 Interactions between MSP and Customer

When customers decides to enter a contract for the roaming service, their software agents (wallet) create a DID with a corresponding DID document specifically for the business relationship with the MSP. Within the DID document, service endpoints are be specified which are necessary to interact with the customer within this specific business relationship. The mapping of the contractual relationship could be handled by using another VC. On a basic level, the VC issued by the MSP to the customer only need to contain a statement of being a customer of the MSP. The type of customer and therefore the type of contract would need to be defined by the VC type, which should be based on a common schema. Also, this "Service VC" could contain tariff regulations and the duration of the contract. Including the contract data in the same VC could lead to the sharing of data at the charging point, which is not necessary for plain authorisation. To enable selective disclosure of individual components of the "Service VC", the chosen signature procedure would need to include each individual attribute.

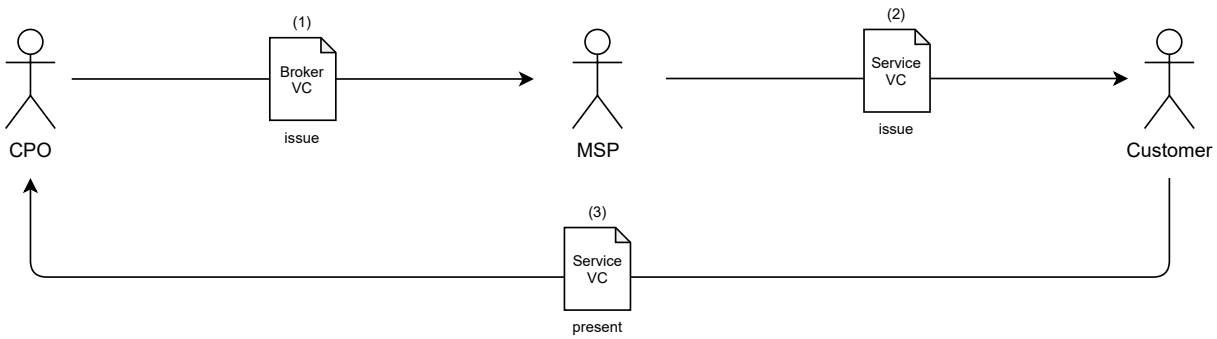

Figure 3. Issuance and presentations of broker and service credentials in SSI-enabled EV charging scenario

3.2.3 Interactions between Customer and CPO

Once the service VC is be issued, customers can authenticate themselves at the charging points of the partner CPOs mediated by the MSP. After physically connecting the vehicle to a charging point, the customer would be asked for authentication to start the charging process. For that, the charging station management sends a request to the CPO's backend to create a so-called challenge. This challenge may be displayed in the form of a QR code at the graphical user interface of the charging point. A scan of this code forwards the customers to their wallet application, wherein they can accept the request to present proof of a valid roaming contract. After selecting the corresponding attributes of the "Service VC" issued by the MSP, these are sent to the CPO backend using the smartphone's mobile data connection. The correct destination could either be stored directly with the challenge or could be determined by resolving a DID and accessing a dedicated service endpoint.

A total of three checks would have to be performed on the presented VC, in order to ensure a sufficient level of certainty about the correctness of the transmitted claims:

- **Integrity** This can be implemented by using the proof algorithms of VC and its presentation. A positive outcome of the presentation proves that no changes were made to the data. Since the included VC consists of derived attributes from the Service VC, a proof would include both the correctness of the stated claim of charging authorisation and the integrity of the underlying Service VC.
- **Validity** This would include a review of the expiration date to determine if the underlying contract is still effective. Furthermore, it could be checked whether a valid MSP can be found for the issuing DID.
- **Schematic correctness** The schema used by the VC would need to be compared with the schema definition agreed upon between MSP and CPO.

If these requirements are met, the customer is successfully authenticated and the requested charging process will be authorised. Otherwise, using an endpoint for messages from the customer's DID document or via the interfaces of the charging point, an error report should be sent, including suggestions for an alternative method for starting the charging process.

4 Discussion

Based on the results presented in the previous section, we discuss their impact for the design of smart service systems, as well as implications for the actors involved in service systems.

4.1 Impact of SSI on Smart Service System Design

With regards to the service system design, we can distinguish the impact on the service experience and customer experience. On the service experience, the major difference is the reduction of complexity through SSI as the standardised method for P2P credential exchange. It replaces commonly used registration processes, which result in additional processing steps for data verification and more complex customer data to be maintained. Another benefit of SSI is the improved interoperability of IT systems between different actors in a service system. Instead of expensive direct point-to-point communication between backend systems, the data exchange takes place via credential exchange via the customers' wallets.

This also has implications for the customer experience, as customers can directly authenticate themselves with IT systems of service providers using credentials from a trusted issuer, such as banks or municipalities. Avoiding complex registration processes makes services more accessible, as fewer steps are required for establishing a trusted relationship between the actors in the service system. Additionally, as such wallet apps are used in a variety of occasions, a growing number of users become familiar with their use. This is an improvement over today's situation in which the use of a new service requires the installation and setup of a service-

specific app. Overall, SSI contributes towards a seamless customer experience with fewer apps, less effort for learning the handling of unfamiliar apps, and simpler authentication of the user.

4.2 Implications of SSI for Involved Actors

From the changes in the smart service system outlined above, we can derive implications for the involved actors, which can be distinguished into customer, service provider, and broker (such as roaming providers).

Customer For customers, SSI-enabled smart service systems could offer a more comfortable enrolment and authentication process. If the customer already uses a digital wallet, he or she can provide a proof of his identity without a complex registration process. Once a connection to the service provider is established, authentication can be performed automatically and without passwords. This streamlines the overall customer experience. and satisfies customers needs for independence and easier integration [14]. Additionally, an SSI-enabled smart service might be preferred by customers as the exchange of data between customer and service provider is transparent and under control of the customer. This improves privacy, which is one of the most frequently mentioned benefits expected for business scenarios (see section 2.1).

Service Provider For service providers SSI can potentially lower the entry barrier for customer on-boarding and simplify the authentication for service usage. Besides, it makes the service more attractive through higher levels of privacy. However, this assumes that the customer already has an digital wallet and VCs for his or her identity from a trusted issuer in place.

Besides authentication, VCs can also be used for various purposes dealing with proving status or permissions to other parties. This offers an opportunity for businesses that strive for efficient coordination between companies to reduce their cost. The specific requirements of a use case are determined in the business practice itself and by external regulations. Considering the regulatory requirements for the official calibration of charging points' measurement equipment, SSI approaches could be used not only to identify customers, business partners, and contracts but also to ensure the integrity of charging data. A VC could be created that verifiably persists the relevant attributes, including duration and type of the charging process, a process identifier, as well as the power consumed in kilowatt-hours.

On the operational level, the cost for customer data processing might be reduced. As customers can provide verified and up-to-date identity data on demand, the cost on GDPR-compliant processing of customer data at the service provider is lowered. Furthermore, expensive procedures to ensure and maintain data quality of customer data are not required anymore. On the other hand, initial investments for enabling existing systems for SSI need to be considered.

Broker We can also observe changes to the overall service ecosystem. SSI provides the transformative capabilities to map and enrich different commercial structures. As SSI puts persons and organisations into control of their identity data, they can interact with other actors through P2P credential exchange. This weakens the position of platforms that act as broker between actors in a service ecosystem, which can eventually lead to their disintermediation.

Our EVCS example shows the emancipation of MSP and CPO from the roaming provider, which is therefore not needed anymore. This is mainly enabled by the secure P2P credential exchange between various actors. To offer a roaming service to a customer, MSP and CPO must agree on aspects such as pricing, internal billing, and the charging methods offered. Furthermore, a common schema for the contractual VCs must be defined and stored in a suitable location with verifiable integrity. These schemas form the basis for the data structures of the VCs used in the service process and decide to a large extent on the interoperability of the service offerings of actors in a service ecosystem. For each roaming service offered, a common

VC schema is required to verifiably map the authorisations and roles in the business scenario. To make this approach accessible to providers of other scenarios and thus to bring about an integration of the business network, coordination at the industry level is necessary.

4.3 Limitations

The insights gained in this paper are based on a single domain, which is commercial charging processes and the service architecture of roaming Therefore, the described disintermediation effects might not be transferable to other service systems. Another limitation is the characteristic of this work being a conceptual analysis. As the validation of the proposed concepts within a real roaming ecosystem was out of scope, our insights are based on a theoretical analysis. The actual impact of the application of SSI will be highly dependent on the concrete implementation and service design of real organisations and service ecosystems. Therefore, an empirical analysis is required to verify the effects in a real-world implementation of the presented concept.

4.4 Future research

Based on our study, we identified potentials for future research along four research topics:

Customer experience of smart services: There is a need to better understand the effects of SSI for the enrolment process, which essentially creates a ”bring your own identity” model. Here, interaction designs and customer experience should be systematically investigated to create design knowledge for smart service systems. Usability research has dealt with different enrolment processes, however they did not cover SSI yet [15]. Existing research on customer experience of smart service has yet to consider the effects of SSI, particularly on privacy, ease of use, accessibility, and controllability [14].

Interoperability: SSI changes the mechanism on how data is transferred between systems. Instead of direct communication, the user (identity holder) transfers data between systems via his or her wallet. This reduces the need for complex integration but requires consensus about the semantics of data in VCs. This can be achieved through credential schemata. Open questions in this area are related to the schema definition process, the selection of actors to issue schemata, as well as to their storing, resolving, and versioning.

Drivers and barriers for adoption: The introduction of SSI in smart service systems can reduce cost for proprietary apps, enrolment procedures, and GDPR-compliant handling of PII data. Enabling of existing applications for SSI on the other hand might be expensive due to a lack of reusable, production-ready components such as integration tools and software libraries. With regard to benefits, SSI can lower the entry barrier for new users and improve privacy. Therefore, cost-benefit analysis should be conducted to evaluate effects in real world cases to develop evaluation models which help practitioners to make informed decisions with respect to both, costs arising from the technical implementation as well as changing business models. Regarding the latter, SSI as a paradigm leads to a shift in the availability of data from service providers to customers. This enables selective disclosure and conscious transactions using this data from the customers perspective. It is yet to be examined from the service providers perspective whether potentially lowered costs in the handling of PII data outweighs the impacts on data utilisation as part of their business models.

Service ecosystems: The disruptive potential of SSI with regard to disintermediation of actors in service ecosystems needs to be studied from an economic as well as strategic management perspective. While SSI might make the service of certain actors less relevant, it can be assumed the it will also create the need for new ones, e.g., trusted issuers, quality assurers, operators of DLT infrastructure, wallet providers, and integration services. While roles in multi-actor smart service innovation have been a topic of recent research [24], it does neither consider the specifics of SSI nor the potential strategic options for actors threatened by disintermediation.

5 Conclusions

Establishing trust between actors in smart service system is a task that leads to various challenges with existing approaches. The inherent characteristics of self-sovereign identity promise to simplify the establishing of trust in services processes but also influence the overall design of the service system. Using the example of an EVCS, we gained an initial understanding of the impacts that SSI can have on smart service systems. Our findings underline the potential of SSI, which should therefore be considered in the design of such systems.

As an emerging concept, it is not surprising that academic works on the application of SSI in business scenarios is scarce, let alone in the context of smart service systems. With the ongoing proliferation of SSI in various industries and application domains, empirical research can be conducted to better understand how the expected benefits of SSI will manifest themselves.

[1] K. Cameron, "The laws of identity," 2005. [Online]. Available: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

[2] O. Avellaneda, A. Bachmann, A. Barbir, J. Brenan, P. Dingle, K. H. Duffy, E. Maler, D. Reed, and M. Sporny, "Decentralized identity: Where did it come from and where is it going?" *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 10–13, 2019, ISSN: 2471-2825. DOI: 10.1109/MCOMSTD.2019.9031542.

[3] P. C. Bartolomeu, E. Vieira, S. M. Hosseini, and J. Ferreira, "Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot," in *Proceedings, 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, Piscataway, NJ: IEEE, 2019, pp. 1173–1180, ISBN: 978-1-7281-0303-7. DOI: 10.1109/ETFA.2019.8869262.

[4] K. C. Toth and A. Anderson-Priddy, "Self-sovereign digital identity: A paradigm shift for identity," *IEEE Security & Privacy*, vol. 17, no. 3, pp. 17–27, 2019, ISSN: 1540-7993. DOI: 10.1109/MSEC.2018.2888782.

[5] B. Cyphers and G. Gebhart, *Behind the one-way mirror: A deep dive into the technology of corporate surveillance*, Electronic Frontier Foundation, Ed., 2019. [Online]. Available: https://www.eff.org/wp/behind-the-one-way-mirror.

[6] A. Mühle and A. Grüner, "A survey on essential components of a self-sovereign identity," 2018. [Online]. Available: https://www.researchgate.net/publication/326459642_A_Survey_on_Essential_Components_of_a_Self-Sovereign_Identity.

[7] R. Soltani, U. Trang Nguyen, and A. An, "A new approach to client onboarding using self-sovereign identity and distributed ledger," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, IEEE, 7/30/2018 - 8/3/2018, pp. 1129–1136, ISBN: 978-1-5386-7975-3. DOI: 10.1109/Cybermatics{\textunderscore}2018.2018.00205.

[8] D. W. Chadwick, R. Laborde, A. Oglaza, R. Venant, S. Wazan, and M. Nijjar, "Improved identity management with verifiable credentials and fido," *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 14–20, 2019, ISSN: 2471-2825. DOI: 10.1109/MCOMSTD.001.1900020.

[9] K. Wittek, L. Lazzati, D. Bothe, A.-J. Sinnaeve, and N. Pohlmann, "An ssi based system for incentivized and self-determined customer-to-business data sharing in a local economy context," in *2020 IEEE European Technology and Engineering Management Summit (E-TEMS)*, IEEE, 2020, pp. 1–5, ISBN: 978-1-7281-0903-9. DOI: 10.1109/E-TEMS46250.2020.9111805.

[10] A. Stasis, N. Triantafyllou, P. Georgakopoulos, R. L. Armitt, and P. Kavassalis, "Designing an academic electronic identity management system for student mobility using eidas eid and self-sovereign identity technologies," in *26th Annual EUNIS Congress*, 2020.

[11] R. Karatas and I. Sertkaya, "Self sovereign identity based e-petition scheme," *International Journal of Information Security Science*, vol. 9, no. 4, pp. 213–229, 2020.

[12] R. B. Gans, J. Ubacht, and M. Janssen, "Self-sovereign identities for fighting the impact of covid-19 pandemic," *Digital Government: Research and Practice*, vol. 2, no. 2, pp. 1–4, 2021, ISSN: 2691-199X. DOI: 10.1145/3429629.

[13] D. Beverungen, O. Müller, M. Matzner, J. Mendling, and J. Vom Brocke, "Conceptualizing smart service systems," *Electronic Markets*, vol. 29, no. 1, pp. 7–18, 2019, ISSN: 1019-6781. DOI: 10.1007/s12525-017-0270-5.

[14] L. Gonçalves, L. Patrício, J. Grenha Teixeira, and N. V. Wünderlich, "Understanding the customer experience with smart services," *Journal of Service Management*, vol. 31, no. 4, pp. 723–744, 2020, ISSN: 1757-5818. DOI: 10.1108/JOSM-11-2019-0349.

[15] C. Porter, "Design shortcomings in e-service enrolment processes," *International Journal of E-Services and Mobile Applications*, vol. 10, no. 3, pp. 1–18, 2018, ISSN: 1941-627X. DOI: 10.4018/IJESMA.2018070101.

[16] N. Masuch, E. Eryilmaz, T. Küster, U. Pletat, J. Fähndrich, T. Theodoropoulos, M. Koukovini, N. S. Hadjidimitriou, and N. Dellas, "Decentralized service platform for interoperable electro-mobility services throughout europe," in *Towards User-Centric Transport in Europe 2: Enablers of Inclusive, Seamless and Sustainable Mobility*, B. Müller and G. Meyer, Eds., Cham: Springer International Publishing, 2020, pp. 184–199, ISBN: 978-3-030-38028-1. DOI: 10.1007/978-3-030-38028-1{\textunderscore}13.

[17] B. Kirpes, P. Danner, R. Basmadjian, H. d. Meer, and C. Becker, "E-mobility systems architecture: A model-based framework for managing complexity and interoperability," *Energy Informatics*, vol. 2, no. 1, p. 28, 2019. DOI: 10.1186/s42162-019-0072-4.

[18] D. van Bokkem, R. Hageman, G. Koning, L. Nguyen, and N. Zarin, "Self-sovereign identity solutions: The necessity of blockchain technology," *arXiv e-prints*, arXiv:1904.12816, 2019. [Online]. Available: https://arxiv.org/pdf/1904.12816v1.pdf.

[19] M. Sporny, D. Longley, and D. Chadwick, *Verifiable credentials data model 1.0: Expressing verifiable information on the web*, 2020. [Online]. Available: https://www.w3.org/TR/vc-data-model/.

[20] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, M. Sabadello, and J. Holt, *Decentralized identifiers (dids) v1.0: Core architecture, data model, and representations*, 2020. [Online]. Available: https://www.w3.org/TR/did-core/.

[21] EVRoaming Foundation, *Ocpi 2.2: Open charge point interface*, 12.06.2020. [Online]. Available: https://evroaming.org/app/uploads/2020/06/OCPI-2.2-d2.pdf.

[22] J. Ratej, B. Mehle, and M. Kocbek, "Global service provider for electric vehicle roaming," in *2013 World Electric Vehicle Symposium and Exhibition (EVS27)*, Nov. 2013, pp. 1–11. DOI: 10.1109/EVS.2013.6914941.

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

[24] J. Anke, J. Pöppelbuß, and R. Alt, "It takes more than two to tango: Inter-organizational collaboration in smart service systems engineering," *Schmalenbach Business Review*, vol. 72, no. 4, pp. 599–634, 2020. DOI: 10.1007/s41464-020-00101-2.