Analysis and Enhancement of Self-sovereign Identity System Properties Compiling Standards and Regulations

Charnon Pattiyanon and Toshiaki Aoki
Graduate School of Advanced Science and Technology,
Japan Advanced Institute of Science and Technology, Ishikawa, Japan

Keywords: Self-sovereign Identity, Software Security, Legal and Regulatory Issues, Comparative Analysis.

Abstract: A self-sovereign identity (SSI) system represents a paradigm shift in identity management by leveraging the decentralization inherent in blockchain technology. The fundamental characteristics of the SSI system are constrained by a set of guiding principles and system properties. While knowledgeable scholars and practitioners have proposed such principles and properties, they have not yet been standardized. The SSI community has agreed upon and adheres to the existing proposals when implementing the SSI system. Additionally, the SSI system is used to manage personally identifiable information (PII), and compliance with certain standards and regulations is required. We discovered that while the current proposals do correspond to some extent to those documents, they cannot be characterized as explicitly compliant. We evaluate several well-known standards and regulations as credible sources in this work and compare them to the definitions in current proposals in order to identify inconsistencies. Then, we propose a list of SSI system properties that could be used to improve the security and privacy of the SSI system by addressing the inconsistencies discovered. We assess its applicability in real-world scenarios and its appropriateness from an expert's perspective. The proposed properties yield meaningful results that may resolve the inconsistencies.

1 INTRODUCTION

A self-sovereign identity (SSI) system is a type of service that utilizes blockchain technology to empower users with complete control over their personally identifiable information (PII), which is securely stored on a user-owned storage device. The fundamental concept is defined by users' ability to disclose as little PII as necessary for service authentication and authorization (Allen, 2016).

Due to the SSI system's cutting-edge and sophisticated nature, deployment requires some effort to familiarize oneself with its functions and constraints. Allen (2016) presented ten principles that succinctly encapsulate the SSI system's constraints, regardless of the technology or method of implementation. Allen's principles were regularly cited in the majority of writings devoted to the SSI system. A *principle* is a collection of succinct statements indicating which expectations are critical and unique to the SSI system. For instance, the existence principle (Allen, 2016) states that:

> "Users must have an independent existence. Any self-sovereign identity is ultimately based on the ineffable 'I' that's at the heart of identity. It can never exist wholly in digital form. This must be the kernel of self that is upheld and supported. A self-sovereign identity simply makes public and accessible some limited aspects of the 'I' that already exists."

Principles serve as a starting point for discussions and help to shorten the SSI system's learning curve. Allen did, however, acknowledge that the principles are still subject to refinement.

Naik and Jenkins (2020) was an attempt to refine Allen's principles for compliance with the European's general data protection regulation (GDPR), with the goal of preserving privacy in the SSI system. They presented a set of 20 governing principles as an extension of Allen's. Regrettably, their work did not adequately identify links to the GDPR's compliance explicitly. Another attempt was published by Ferdous et al. (2019). They aimed to do a thorough analysis of the SSI system and extracted 17 system properties based on multiple sources, e.g., Allen's article and Sovrin[1]'s white paper (Tobin and Reed, 2017). A

[1] An industry level solution to the SSI system.

Pattiyanon, C. and Aoki, T.
Analysis and Enhancement of Self-sovereign Identity System Properties Compiling Standards and Regulations.
DOI: 10.5220/0010877300003120
In *Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022)*, pages 133-144
ISBN: 978-989-758-553-1; ISSN: 2184-4356

property is identical to a principle, except that the system and its components are the subjects. In Ferdous et al. (2019) proposal, they used fundamental notions and make no reference to standards or regulations.

Existing research identifies gaps that motivate us to enhance the security and privacy of the SSI system through compliance with well-established standards and regulations. A *standard* is a published document that was developed collaboratively by members of a community with the intent of assessing, controlling, and measuring a target (i.e., an organization, factory, system, or software). Through a series of principles, policies, practices, and measures, the standard established a benchmark for the target. On the other hand, a *regulation* is a legal document created by national governments. Quantifiable controls, endorsed tasks, or mandatory principles for assessing or evaluating the target were specified in the regulation. Regulations are stringent, and violations will result in severe legal consequences. For conciseness, we will refer to standards and regulations as credible sources.

The remainder of this paper is organized as follows: Section 2 discusses a motivating problem; Section 3 discusses current property proposals and the controls imposed by credible sources; and Section 4 discusses our analysis method and results. Section 5 contains an evaluation of the enhanced properties; Section 6 contains a discussion; and Sections 7 and 8 contain a comparison of related works and a conclusion to this work.

2 MOTIVATION

As mentioned in Section 1, three recent proposals for principles and properties have been made. Their proposal, on the other hand, is neither clearly consistent with credible sources nor does it include a reference to credible sources. As such, we will illustrate a legal and regulatory compliance issue that highlights the need for property enhancement.

Assume we have a properly implemented SSI system capable of validating and issuing claims in accordance with the fundamental notion. A user may submit a claim, which is a brief statement attesting to the accuracy of their personal information, and request validation from the relevant issuer. Following the claim's validation, the issuer creates a verifiable version of it using a cryptographic schema published on the blockchain and returns it to the user. We depict the aforementioned scenario using a sequence diagram, as illustrated in Fig. 1. As developers, we may intend to implement this scenario to possess the *consent* property (Ferdous et al., 2019), that defined as:

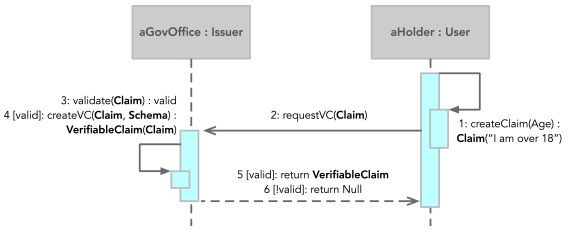

Figure 1: An illustration of the claim validation and issuance scenario as a sequence diagram.

> "Users must agree to the use of their identity. Any identity system is built around sharing that identity and its claims, and an interoperable system increases the amount of sharing that occurs. However, sharing of data must only occur with the consent of the user."

Since the user consents to the claim being read, the issuer has the right to read it. Once. we would want to evaluate this system against the GDPR (2016)'s Article 5.1.(b) purpose limitation, stated as follows:

> "Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;..."

According to the GDPR article's definition, the consent property lacked safeguards against subsequent processes that were incompatible with the original purpose. For example, a dishonest issuer may retain the claim after it has been validated. The claim is retained in excess of the specified purpose.

A common solution or workaround for this issue is for developers to verify the system's compliance with any credible source they choose. Then, they must increase their effort by modifying the implemented system in order to complete all endorsed tasks. This method is complex and time-consuming, depending on the number of credible sources compiled.

The aforementioned issue with a common solution presents us with two research questions:

1. Could the SSI system properties be easily reconciled with well-known credible sources?
2. Are the properties still valid for the SSI system's fundamental notion after the SSI system's properties have been enhanced by the addition of endorsed tasks from credible sources?

To address those research questions, we present a revised list of SSI system properties in this work, which has been enhanced to ensure consistency with well-known credible sources. We begin by identifying inconsistencies between the tasks endorsed by credible sources and the proposed properties. Then we determine which tasks are pertinent to the SSI system and

should be included on the list. The following are the work's major contributions:

- We find inconsistencies between current property proposals and the selected well-known, credible sources. It is advantageous for system implementors to be aware of these inconsistencies and to have a starting point for addressing them throughout their property implementation.
- We enhance the SSI system properties to be in consistent with credible sources. These enhanced properties will guarantee implementors of the SSI system that their implementation adheres to the credible sources from the ground up and they can focus their efforts only on property verification.

3 PRELIMINARIES

3.1 Self-sovereign Identity System and Its Property Proposals

This section will provide an overview of the SSI system, its terminology, and its proposed properties. To aid in comprehension of the SSI system, the following terms are frequently used throughout articles (Allen, 2016; Ferdous et al., 2019; Tobin and Reed, 2017; Stokkink et al., 2020; Lee et al., 2020):

A **holder** is an individual who owns their identity or a system user who has complete control over their PII. They have the option of disclosing their PII for the purpose of service authentication.

An **issuer** is an individual, an organization, or a system that is responsible for validating the correctness of users' claim.

A **verifier** is an individual, an organization, or a system that provides users a service and requires credentials for service authentication and authorization.

An **identity attribute** is a key-value pair that is used to store PIIs. Attributes should be stored locally in a user-owned device.

A **decentralized identifier** is a unique identifier that uses public-private key infrastructure as a key exchange mechanism using the blockchain.

A **claim** is a collection of succinct statements attesting to the user's PII. At times, it may make use of a privacy-preserving mechanism, such as zero-knowledge proofs.

A **claim schema** is a cryptographic schema (which contains keys or hash strings) used to define a verification scheme. It will serve as an input for the creation of **verifiable claims** and will be publicly available on the blockchain for anyone wishing to verify the claim.

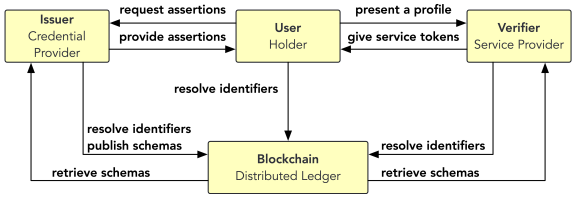

Figure 2: An overview of the SSI system model.

Utilizing those terms, it can form a model of the SSI system, which adheres to the requirement for verifiable credential data model (W3C, 2019). We illustrate an overview of the SSI system model in Fig. 2.

Indeed, the technical specification for the SSI system has further information, but for the sake of this work, we will utilize only this abstraction to construct the analysis criteria.

The SSI system is implemented differently depending on the technology used. To ensure that the implementation captures the essence of the SSI system, however, principles and properties act as constraints on the implementation. To establish a clear distinction between principles and properties, the following definition of a principle is used.

Definition 1 (Principle) *A principle is represented as an ordered set* $PR = \{e_i | e_i : S \times A \times O, i \in \mathbb{N}\}$*, where* e_i *is the i-th constraint that is utilized to determine if a principle has been realized; S denotes a set of constrained subjects, e.g., a system component, an infrastructure, or policies; A is a set of constrained activities; O denotes a set of relevant information objects.*

We discovered that principles in two current proposals (Allen, 2016; Naik and Jenkins, 2020) provide with a list of constraints, such as "user must agree to the use of their identity". These constraints serve as a check list for ensuring the principle is followed. Each constraint has three pieces of important information: constrained subjects, activities, and related information objects. This information was used to define the principle. On the other hand, a property is a subset of principles that are applicable to just system components, such as the one that was proposed by Ferdous et al. (2019). We define a system property as below.

Definition 2 (Property) *A property is represented as an ordered set* $P = \{e_i | e_i : S_c \times A \times O, i \in \mathbb{N}\}$ *where* $P \subseteq PR, S_c \subseteq S$ *is a subset of constrained subjects that scoped only system components.*

We will base on these definition in our consistency analysis and enhancement.

3.2 Standards and Regulations

Given our goal of establishing standards and regulations as credible sources, we should make a clear dis-

tinction between how they will be compiled and how they will be used.

Both standards and regulations share a common characteristic in that they define controls that are used to determine or assess whether a target complies with a specified standard or does not violate a regulation. A control is a collection of tasks that have been endorsed and serve as a checklist for assessing its compliance. This means that if the target system performs the endorsed tasks, it will be in compliance with the applicable standard or regulation. For instance, the ISO/IEC 29100:2011 control entitled "openness, transparency, and notice" has an endorsed task stated as follows:

> "PII collector should identify the purposes for which personal information is collected, used, retained, and disclosed."

Control may be referred to in a variety of ways in credible sources, including as obligations or principles. As a result of their simplicity, we will refer to all terms as controls and define them as follows.

Definition 3 (Control) *A control is represented as an ordered set* $C = \{t_j | t_j : CT \times CF \times CI, j \in \mathbb{N}\}$ *where* t_j *is the j-th endorsed task; CT is a set of controlled targets; CF is a set of corresponding functions or processes that are controlled; and CI is a set of information objects that subject to be controlled.*

For instance, the "openness, transparency, and notice" control consisted of 'PII collector' as a control target, 'identify purposes to collect' and 'identify purposes to use' are examples of corresponding functions, and 'personal information' is the controlled information object. As it is obviously shown that the definition of principle (Def. 1), property (Def. 2), and control (Def. 3) are similar in structure, we will be able to analyze for inconsistencies and enhance the existing system properties based on these definitions.

4 CONSISTENCY ANALYSIS AND PROPERTY ENHANCEMENT

This section will describe our methodology for identifying inconsistencies between existing property proposals and credible sources. While we demonstrate an inconsistent case in Section 2, it also shows that the properties are not completely inconsistent and somewhat align with credible sources' controls. This section expands on this key concept in order to improve existing proposals and provide more secure and privacy-preserving properties.

Our methodology is qualitative and comparative in nature and is comprised of four steps, as depicted in

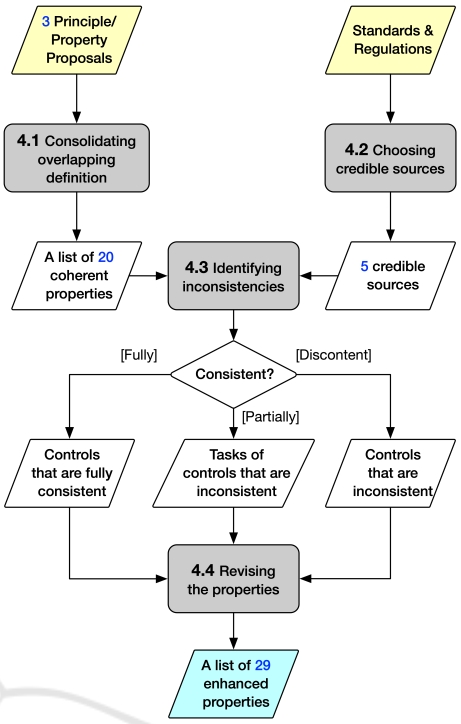

Figure 3: An overview of the research methodology.

Fig.3. To begin, we discovered that the principles and properties of existing proposals are identical or share a portion of their definition. We compare and consolidate the overlapping definitions in step 4.1 to arrive at a single coherent definition. We identified twenty properties that could be consolidated as a result of the three proposals. Then, in step 4.2, we conduct a survey of standards and regulations in order to identify a set of credible sources capable of enhancing the properties through the establishment of selection criteria. Five credible sources met our criteria. In step 4.3, we compare property definitions to control from credible sources to identify inconsistencies. This step documents three instances of consistency: Fully implies that all tasks endorsed by credible sources are consistent with some properties; Partially implies that only a subset of tasks is consistent; and Discontent indicates that the control is dissatisfied with some property. In step 4.4, the three groups of results will be used to enhance the existing properties.

4.1 Consolidating Overlapping

As discussed in Section 3.1, three recent proposals for the SSI system's principles and properties were made (Allen, 2016; Ferdous et al., 2019; Naik and Jenkins, 2020). Certain principles and properties were discovered to be identical, while others shared only a portion of their definition. It will be exhaust-

ing if we continue to improve each proposal individually. Consolidating the overlapping definitions into a single coherent definition will make this paper more concise and understandable.

Because Ferdous et al. (2019) and Naik and Jenkins (2020) were based on Allen (2016)'s article, those works incorporate fundamental principles. As can be seen, each of Allen's ten principles was incorporated into the others. As a result, there is no reason to include Allen's principles in order to increase effort. We will consider only those two proposals (X for Ferdous et al. (2019), Y for Naik and Jenkins (2020)) in this step. We compare two distinct properties $(P^x, P^y | P^x \in X,\ P^y \in Y)$ by validating each pair of constraints $(e^x_m, e^y_n | e^x_m \in P^x, e^y_n \in P^y)$ against the following conditions:

1. P^x and P^y share the same title.
2. P^x and P^y share the same high-level purposes.
3. (e^x_m, e^y_n) such that $(S^x_{c,m} \subseteq S^y_{c,n}) \wedge (A^x_m \subseteq A^y_n), \exists m, n.$

When at least one of the conditions is met, the pair of properties is said to be overlapped. Then, two overlapping properties' definitions will be consolidated into a single property. Table 1 contains an exhaustive list of twenty coherent definitions derived from the two proposals. We use alphabetical superscriptions to indicate the source of the constraint. Table 1 will suffice and will be used as an input for Section 4.3's consistency identification.

4.2 Choosing Credible Sources

To accomplish our goal of enhancing the SSI system's security and privacy preservation through enhancement of its properties, we need a collection of credible sources that is sufficient and appropriate for that purpose. Hundreds of standards and regulations, on the other hand, are enforced in numerous segments of the IT industry. Some are directed at the organization, its human resources, or its paperwork, while others are directed at the operation of the system. This work focuses exclusively on the second category. Documents pertaining to an organization, human resources, and paperwork are not within our purview.

This step is for determining which standards and regulations are appropriate for enhancing the properties of the SSI system. We outline the following criteria for choosing credible sources:

1. The source must be, at least, targeted toward a software product and its features.
2. The source must provide a set of controls that can evaluate the software product's features.
3. The source must be universally applicable regardless of any specific domain.

The first criterion is to attempt to eliminate sources

Table 1: A complete list of coherent definitions - See a complete comparison table in Appendix A. of (Pattiyanon and Aoki, 2021).

Coherent Definition
P1. Existence: (1) SSIs must represent real-world user's characteristic[a,b] (2) utilizing selective information that is necessary for use in the digital domain[b].
P2. Sovereignty: (1) An identity owner must have full control of their identity to decide when they wish to release identity data and to which entity for whatever purpose[a,b]. (2) Other person, organization, or government should not own or control their identity in any way[b].
P3. Access Control: (1) An identity owner should have unrestricted access and control over all access to their identity[a,b].
P4. Transparency: (2) All systems, protocols, and algorithms employed in an identity infrastructure should be free, open-source, as independent as possible of any particular architecture or proprietorship[b], and (1) transparent for every involved entity[a].
P5. Persistence: (1) SSIs must be persistent as long as required by their owner[a,b]. (2) However, it must be revoked or abandoned by its owner at any time[b].
P6. Portability: (1) SSIs and related data can be transferred from a medium or platform to another when the previous one disappears due to any reason[a,b].
P7. Interoperability: (1) All involved systems must be capable of communicating with each other at any scale to maximize level of interoperability[a,b].
P8. Consent: (1) Every single piece of identity data must be released to a third party only after the corresponding user has consented to do so[a].
P9. Minimization: (2) When releasing SSIs to a third party, an identity owner should be requested to selectively provide or disclose[a] (1) the minimum information of identity maintaining as much anonymity as possible[a,b].
P10. Protection: (2) SSIs and their communication channels should be secured[b] and (1) well-protected with the latest cryptographic mechanism satisfying the CIA (Confidentiality, Integrity, and Authenticity) and non-repudiation properties[a].
P11. Autonomy: (1) SSIs must support full autonomy on the management and administration of identity[a].
P12. Single Source: (1) An identity owner should be the single source of truth regarding their identity[a] that (2) maintained on the owner-controlled storage[b].
P13. Availability: (1) All infrastructures and services of the SSI system must be readily available to all participants (including an identity owner) without any discrimination to access from different platforms[a,b].
P14. Sustainability: (2) An infrastructure and services of the SSI system should be environmentally, economically, technically, and socially sustainable[b] by (1) using open standards[a].
P15. Cost Free: (1) SSIs should be offered to everyone free of cost or negligible cost[a,b], (2) without incurring any hidden cost, licensing fees, or other financial charges for creating, managing, and adopting them[b].
P16. Flexibility: (1) An infrastructure and services should accommodate the changing demand by facilitating diverse, decomposable, and extensible at any scale[b].
P17. Safeguard: (1) The freedom and rights of every owners should be safeguarded in any conditions[b].
P18. Verifiability: (1) SSIs should be verifiable in the digital domain, similar to a physical credential representing the real-world identity[b].
P19. Recovery: (1) An infrastructure and services of the SSI system should be sufficiently resilient to successfully recover any SSI in the case of a key, wallet, or device lost[b].
P20. Accessibility: (1) An infrastructure and services of the SSI system should be user-friendly and accessible by as many people as possible[b].

Table 2: An evaluation result of ten well-known sources against the predefined criteria.

Source Name	#Page	#Control	Criteria		
			1.	2.	3.
Security Source					
ISO/IEC 15408:2009 (2009)	64	-	×		×
ISO/IEC 27001:2013 (2013b)	23	114		×	×
ISO/IEC 27002:2013 (2013a)	80	14	×	×	×
NIST SP800-12 (2017)	101	20		×	×
ASVS 4.0.2 (2020)	69	14	×	×	×
Privacy Source					
ISO/IEC 29100:2011 (2011)	21	11	×	×	×
GDPR (2016)	88	7	×	×	×
PDPA (2012)	44	9	×	×	×
HIPAA (1996)	169	5	×	×	
ISTPA RMRM (2009)	37	16			×

that are irrelevant to our work. The second criterion is used to eliminate sources that do not have evaluable controls or that have controls that only evaluate non-feature constraints. For example, several articles of the GDPR (2016) regulate the privacy policies of the target system, which are distinct from the system's features. The final criterion is chosen to eliminate domain-specific sources in order to increase the generality of the SSI system's properties, as the SSI system's nature is self-contained and applicable to any domain. If all of the criteria listed above are met, the source is considered credible.

We limited our survey to five well-known security sources and five well-known privacy sources in this work. Then, we compare each source to our predefined criteria and present the results in Table 2. It contains summary information about each source, such as the number of pages (#Page) and controls that follow Definition 3 (#Control). Following that, the remaining three columns indicate with a cross mark (×) which criterion a source adheres to. It also reports that two security sources and three privacy sources hold all criteria. We will take those sources as another input of consistency analysis. We explain each credible source in the following sub-section.

A) ISO/IEC 27002:2013. defines security control codes of practice, which supplement 114 security controls (divided into 14 control sets) from Annex A. of ISO/IEC 27001:2013b. However, those security controls are aligned with the endorsed tasks in Def. 3. Therefore, we utilize its 14 control sets as controls and arrange corresponding security controls as endorsed tasks. A control in this source will be identified by A.{Set No.}.({Control No.}), e.g., **A.9.(3)** means the third controls in Annex A.9.

B) ASVS 4.0.2 (2020). is a standard that defines hundreds of security verification requirements for applications. This source provides 14 controls along with objectives, high-level requirements, and detailed requirements. The detailed requirements is too specific for the development, e.g., "Passwords are one way hashed with a salt". It is in a different abstraction with the system properties. As a result, we summarize the endorsed tasks from the high-level requirements only. A control in this source will be identified by V{Control No.}.({Requirement No.}), e.g., **V1.(1)** means the first requirement of the first control.

C) ISO/IEC 29100:2011. is a standard that introduces a privacy framework for IT systems. This source provide seven privacy principles, which are expressed in concise, evaluable statements. We refer to those principles as controls and arrange those statements as endorsed tasks. A control in this source is identified by PR{Principle No.}.({Statement No.}), e.g., **PR2.(1)** means the first statements of the second privacy principle.

D) GDPR (2016). is a well-known data protection regulation for systems and organizations running their business in European countries. This source provides seven core principles in Chapter II Article 5.1 and 5.2, which we refer to it as controls. However, other articles were defined in different aspects, from an organization to a system aspect. We add up articles from Article 7 to 34, which the controlled targets (*CT*) and data (*CI*) could be implied to the system components. For example, Article 12.1 indicates that the data controller must provide information on data processing to the data subject, which relates to the Article 5.1.(a). A control in this source is identified by Art.{Article No.}.{Paragraph No.}.({Point}), e.g., **Art.5.1.(b)** means point B in the first paragraph of the article 5.

E) PDPA (2012). is a legislation for systems and organization running their business in Singapore. This source provides eleven controls in a form of obligations. We take those obligations as controls and arrange their definitions as endorsed tasks. A control in this source is identified by O{Obligation No.}.({Statement No.}), e.g., **O4.(1)** means the first statement of the fourth obligation.

However, not all endorsed tasks of every control are applicable for the SSI system. The task must either endorse system components and actors, or control on data objects that are comparable to which are in the SSI system. Therefore, at the end of this step, we will collect controls and determine which

Table 3: An example of a control with applicable endorsed tasks - See a complete list of controls in Appendix B of (Pattiyanon and Aoki, 2021).

PR10. Accountability: (1) PII collector should ensure the compliance with privacy and data protection requirements is able to demonstrate; (2) Responsibilities, internal and external auditing and controlling of all data processing should be specified;

Table 4: Pre-defined system components S_c that are comparable to controlled targets CT.

System Component S_c	**Controlled Target** CT
Identity Owner	Data Subject, Individuals
System	Application, System, Process, PII Collector, Data Controller, Collector
Protocol	
Algorithm	
Infrastructure	
Service	

endorsed tasks are applicable. Table 3 shows an example of a control with an applicable endorsed task highlighted.

4.3 Identifying Consistencies

We can determine which control's endorsed task is consistent with the existing properties because we received two comparable inputs from Sections 4.1 and 4.2 based on Definitions 2 and 3. Indeed, we contrast $e_i \in P$ with $t_j \in C$, assuming that the SSI system's property can achieve a higher level of security and privacy if it is more consistent with controls from credible sources. Inconsistencies discovered during the comparative analysis will be a valuable source of property enhancement in Section 4.4.

In this step, we compare $e_i = (sc, a, o)$ such that $(sc, a, o) \subseteq S_c \times A \times O$, and $e_i \in P$ with $t_j = (ct, cf, ci)$ such that $(ct, cf, ci) \subseteq CT \times CF \times CI$ and $t_j \in C$. A constraint e_i is comparable to an endorsed task t_j if at least two of the following conditions hold.

- $x \in sc, \exists x$ is comparable to $y \in ct, \exists y$ according to Table 4.
- $x \in d, \exists x$ is comparable to $y \in ci, \exists y$ according to Table 5.
- $x \in p, \exists x$ is explicitly equivalent to $y \in cf, \exists y$.

As stated in the preceding conditions, we conduct a domain analysis to discover a relationship between terms in standards and regulations and terms in the SSI system. Tables 4 and 5 were created to represent those relationships. Unfortunately, some pairs are incomparable and necessitate the services of a professional consultant. We use our domain knowledge to justify which pairs satisfy the criteria.

All pairs that demonstrate consistency will be collected and classified into three categories: FC is a collection of controls that satisfy all of their endorsed tasks ($\forall t$) by any property; IC is a collection of controls that satisfy some of their endorsed tasks ($\exists t$) by any property; and DC is a collection of controls that satisfy none of the endorsed tasks.

Table 5: Pre-defined pairs of data objects O that are comparable to corresponding information objects CI.

Data Object O	**Corresponding Information** CI
SSI, Personal Data, Partial Identity, Claim	Information
	Transaction
	Personally Identifiable Information (PII)
	Data
	Personal Data
Assertion, Profile	Credential

Table 6: Results from the consistency analysis.

Control C	**Class**	**Consistent Pair** (e, t)	**Missing Task** t
ISO/IEC 27002:2013a			
A.8	DC	-	(6),(7)
A.9	IC	(**P3.**(1), (4)), (**P3.**(1), (5)), (**P10.**(2), (6))	(3)
A.10	FC	(**P10.**(1), (2))	-
A.12	DC	-	(6)-(10)
A.13	DC	-	(1), (3)
A.14	IC	(**P10.**(2), (3))	(2)
A.17	FC	(**P13.**(1), (4))	-
A.18	FC	(**P10.**(1), (4))	-
OWASP ASVS 4.0.2 (2020)			
V2.	IC	(**P10.**(2), (4)), (**P19.**(1), (5)), (**P10.**(2), (7))	(1)-(3), (6),(8)
V3.	DC	-	(1)-(3)
V4.	IC	(**P3.**(1), (1))	(2)-(4)
V5.	DC	-	(1)-(3)
V6.	IC	(**P10.**(1), (1)), (**P10.**(2), (3))	(2)
V7.	DC	-	(1)-(4)
V8.	FC	(**P10.**(1), (1)), (**P10.**(1), (2)), (**P10.**(1), (3))	-
V9.	FC	(**P10.**(2), (1)), (**P10.**(1), (2)), (**P10.**(1), (3))	-
V10.	DC	-	(1)-(4)
V11.	DC	-	(1)-(3)
V12.	DC	-	(1),(2)
V13.	DC	-	(1)-(3)
V14.	DC	-	(1)-(3)
ISO/IEC 29100:2011			
PR1.	FC	(**P2.**(1), (1)), (**P8.**(1), (2))	-
PR2.	DC	-	(1),(2)
PR3.	IC	(**P5.**(1), (1))	(2)
PR4.	FC	(**P9.**(1), (1))	-
PR5.	FC	(**P2.**(1), (1)), (**P5.**(2), (2))	-
PR6.	DC	-	(1),(2)
PR7.	IC	(**P2.**(1), (2)), (**P4.**(1), (3))	(1),(4)
PR8.	FC	(**P2.**(1), (1)), (**P5.**(2), (2))	-
PR9.	IC	(**P10.**(1), (1)), (**P17.**(1), (1))	(2)
PR10.	DC	-	(1)
GDPR (2016)			
Art.5.1.(a)	IC	(**P8.**(1), (1))	(2)-(5)
Art.5.1.(b)	DC	-	(1),(2)
Art.5.1.(c)	FC	(**P9.**(1), (1))	-
Art.5.1.(d)	IC	(**P5.**(2), (2)), (**P5.**(2), (3))	(1),(4)
Art.5.1.(e)	FC	(**P5.**(1), (1))	-
Art.5.1.(f)	FC	(**P10.**(1), (1))	-
Art.5.2	DC	-	(1),(2)
PDPA (2012)			
O2.	DC	-	(1)
O3.	IC	(**P8.**(1), (1))	(2),(3)
O4.	IC	(**P5.**(1), (1))	(2)
O5.	DC	-	(1)
O6.	FC	(**P10.**(2), (1))	-
O7.	FC	(**P5.**(1), (1))	-
O8.	DC	-	(1)
O9.	IC	(**P3.**(1), (1))	(2)
O11.	FC	(**P6.**(1), (1))	-

The results of the consistency analysis between a list of properties' coherent definitions and credible sources' controls are shown in Table 6 . Each control is identified by its category, pairs that demonstrate its

consistency, and missing endorsed tasks that were not met by any property. Regrettably, the absence of endorsed tasks indicates inconsistencies that may contribute to improvement. In the following section, we will examine the feasibility of adding the missing endorsed tasks to the properties of the SSI system.

4.4 Revising the Properties

The inconsistencies discovered in the previous step provide insights into areas where current proposals for the properties of the SSI system fall short. In this step, we either add the missing endorsed tasks from Table 6 to existing properties or develop new properties to cover the gaps in compliance with credible sources. Our improvement is based on three criteria, which are listed below.

1. For a control C that is classified as IC:
   (a) We enhance a property EP that relates to a consistent pair (e,t) by adding missing endorsed task t if there are fit to the property context.
   (b) We introduce an additional property AP, which includes missing endorsed tasks $t \in C$ that are not fit to the related property context P that contains e from the consistent pair.
2. For a control C that is classified as DC, we introduce an additional property AP that includes missing endorsed tasks $t \in C$.
3. For all properties, including current, enhanced, and additional properties, we revise their elements to subject to the SSI system.

We obtain a list of the SSI system's properties using the preceding criteria, as shown in Tables 7 and 8. As can be seen from the list, we also specify three types of properties: **P**s are current properties that are only revised based on the third criteria; **EP**s are enhanced properties that include corresponding endorsed tasks from controls from credible sources; **AP**s are additional properties that are developed from discontent controls or endorsed tasks from controls that are not suitable for any property context.

The critical outcome of this paper will be a list of the SSI system's properties, which will aid in the analysis, design, and development of the SSI system implementation.

5 EVALUATION

This section will discuss how the proposed list of SSI system properties was evaluated. They are evaluated using two methods: use cases and a questionnaire for experts. The subsequent sub-sections will detail the evaluation procedure and results.

Table 7: A complete list of the enhanced SSI system properties with their definition.

Property Name P and Its Definition (Property Elements e)
P1. Existence: (1) An SSI system must allow its users to represent their real-world characteristics in the digital domain; (2) An SSI system requires to utilize selective information that is only necessary for use in the digital domain;
EP2. Sovereignty: (1) An SSI system must provide full control to an identity owner to decide when they wish to release identity data and to which entity for whatever purpose; (2) An SSI system must not allow other person, organization, or government to own or control user's identity in any way; (3) **PR.7.(4)** An SSI system should inform relevant stakeholders to understand possible risks and actions they can take to control their identity;
P3. Access Control*: (1) An SSI system must allow identity owners to have unrestricted access and control over all access to their identity;
EP4. Transparency: All systems, protocols, and algorithms in the SSI domain should be transparent for every involved entity; (2) All systems, protocols, and algorithms in the SSI domain should be free, open-source, and as independent as possible; (3) **PR7.(1)** An SSI system should provide notice about its policies and procedures to the identity owner;
EP5. Persistence: (1) An SSI system must persist SSIs as long as it is required by an owner; (2) An SSI system must revoke or abandon SSIs as requested by an owner at any time; (3) **PR3.(2)** An SSI system must observe the type and amount of SSI suitable for its purpose; (4) **Art.5.1.(d).(4)** An SSI system must communicate any rectification or erasure of SSIs to every participant;
P6. Portability: (1) An SSI system must allow SSIs and related data to transfer to another medium or platform when it disappears due to any reason;
P7. Interoperability: (1) All involved systems in the SSI domain must be capable of communicating with each other at any scale to maximize level of interoperability;
EP8. Consent: (1) An SSI system release SSIs to a third party after an owner has consented to do so; (2) **Art.5.1.(b).(2)** An SSI system should demonstrate the processing of SSIs regarding the owner consent; (3) **Art.5.1.(b).(3)** If the consent is given as a written declaration, an SSI system should represent the consent in an intelligible and easily accessible form, using clear and plain language; (4) **Art.5.1.(c) & O3.(2)** An SSI system must provide a right of an identity owner to withdraw their consent at any time with noticing of the likely consequences; (5) **Art.5.1.(d)** An SSI system must provide any information relating to the processing to the identity owner in a concise, transparent, intelligible and easily accessible form, using clear and plain language; (6) **O3.(3)** Once the consent is withdrawn, an SSI system must cease to collect, use or disclose the corresponding SSIs;
P9. Minimization: (1) When releasing SSIs to a third part, an SSI system must allow an identity owner to release the minimum information of identity maintaining as much anonymity as possible; (2) An SSI system must allow an identity owner to selectively provide or disclose them;
EP10. Protection: (1) An SSI system protects SSIs and their communication channels with the latest cryptographic mechanism satisfying the CIA (Confidentiality, Integrity, and Authenticity) and non-repudiation properties; (2) An SSI system must use a secure storage and communication channels for SSIs and related data; (3) **A.14.(2)** All services of an SSI system must be protected from public networks; (4) **V6.(2)** When an SSI system generates a randomized numerical data, a suitable random generator is used; (5) **PR9.(2)** An SSI system must identify and protect both physical and logical against privacy risks;
P11. Autonomy: (1) An SSI system must support full autonomy on the management and administration of identity;
P12. Single Source: (1) An SSI system accepts SSIs from an owner who is a single source; (2) An SSI system must maintain SSIs in the owner-controlled storage;
P13. Availability: (1) An infrastructure and services of an SSI system must be readily available to all participants (including an identity owner) without any discrimination to access from different platform;
P14. Sustainability: (1) An infrastructure and services of an SSI system should use open standards; (2) An infrastructure and services of an SSI system should be environmentally, economically, technically, and socially sustainable;
P15. Cost Free: (1) An SSI system should offer its services to anyone free of cost or negligible cost; (2) An SSI system should not incur any hidden cost, license fees, or other financial charges for creating, managing, and adopting SSIs;
P16. Flexibility: (1) An infrastructure and services of an SSI system should accommodate the changing demand by facilitating diverse, decomposable, and extensible at any scale;
P17. Safeguard*: (1) The freedom and rights of every owners should be safeguarded in any conditions;
P18. Verifiability: (1) An SSI system should allow the identity verification in the digital domain, similar to a physical credential representing the real-world identity;
P19. Recovery*: (1) An infrastructure and services of an SSI system should be resilient to successfully recover any SSI when a key, wallet, or device lost;
P20. Accessibility: (1) An infrastructure and services of an SSI system should be user-friendly and accessible by as many people as possible;
AP21. Information Handling: (1) **A.8.(6)** An SSI system should label user personal information based on privacy and sensitivity; (2) **A.8.(7)** An SSI system should handle user personal information properly according to its privacy and sensitivity; (3) **A.12.(6)** Information should be backed up regularly;
AP22. Authentication: (1) **A.9.(3)** An SSI system must implement a formal user registration and de-registration; (2) **V2.(8) & V4.(2) & V13.(1)** An SSI system must authenticate users with valid credentials to services before use; (3) **V2.(2) & V2.(6)** An SSI system must use strong authenticator with single or multi-factor one time verifier; (4) **V2.(1) & V2.(3)** An SSI system employs password security mechanisms and verifies valid lifecycle of password and credentials; (5) **V3.(1) & V3.(2) & V13.(1)** An SSI system employs session management mechanisms using session tokens that bind to the user authentication; (6) **V3.(3)** An SSI system must control session and enforce to terminate due to timeout;

Table 8: A complete list of the enhanced SSI system properties with their definition (Cont').

Property Name P and Its Definition (Property Elements e)
AP23. Accountability: (1) **A.12.(7) & A.12.(9) & Art.5.2.(2)** An SSI system should keep administrative, operative, and system event logs and review them regularly; (2) **A.12.8 & V7.(2)** An SSI system must protect log information against tampering or unauthorized access; (3) **V7.(1)** An SSI system does not log sensitive information unless required; (4) **V7.(3)** An SSI system does not store logs forever; (5) **PR10.(1) & Art.5.2.(1)** An SSI system should ensure the compliance with privacy and data protection requirements is able to demonstrate;
AP24. Communication Security: (1) **A.13.(1)** Networks in the SSI domain are managed and controlled; (2) **A.13.(3)** Groups of users, services, and systems are segregated; (3) **O8.(1)** An SSI system transfers SSIs to any system in another country if the country stated requirements prescribed to the comparable level of regulations;
AP25. Secure Configurability: (1) **A.12.(10)** The clocks of every component in the SSI domain are synchronized; (2) **V14.(1)** An SSI system has a secure, repeatable build environment; (3) **V14.(2)** An SSI system has hardened third-party library, dependency and configuration management; (4) **V14.(3)** An SSI system has a secure-by-default configuration;
AP26. Role Manageability: (1) **V4.(3)** An SSI system defines roles and privileges to every users; (2) **V4.(4)** An SSI system protect role and responsibility metadata from replay and tampering;
AP27. I/O and Error Handling: (1) **V5.(1) & V13.(2)-(3)** An SSI system should use input validation, output encoding architecture, and effective secure controls for system and web services; (2) **V5.(2)** An SSI system should validate, check length or range, sanitize or filter input data; (3) **V5.(3)** An SSI system encode or escape output data per the data context; (4) **V7.(4) & V10.(1)** An SSI system must handle malicious activities securely and properly; (5) **V10.(2)-(4)** An SSI system should protect application-based vulnerabilities including time-based attacks, phone home code, or unauthorized code; (6) **V11.(1)-(3)** An SSI system must verify that both normal and high value business flows are sequential, processed in order, and cannot be bypassed, as well as are protected against automated attacks; (7) **V12.(1)-(2)** An SSI system should handle and store untrusted files in a secure manner with limited permissions;
AP28. Purpose Limitation: (1) **PR2.(1) & Art.5.1.(b).(1)** An SSI system collects SSIs or personal data for specified, explicit and legitimate purposes; (2) **Art.5.1.(b).(2) & O2.(2)** An SSI system must not process SSIs beyond its purposes; (3) **PR2.(2) & O2.(1)** An SSI system must communicate the purposes of SSI processing to an owner;
AP29. Accuracy: (1) **PR6.(1)-(2) & Art.5.1.(d).(1) & O5.(1) & O9.(2)** An SSI system must check periodically that SSIs are accurate, complete, correct and up-to-date;

* Properties that are classified into IC, but they are not suitable for adding missing endorsed tasks t.

5.1 Use Cases

To generate use cases that incorporate the proposed list of SSI system properties, we must first identify a domain that will use the SSI system for user authentication. We assume that the use cases were created using the unified modeling language (UML) with the intent of attestation some properties. Authors with experience in both system design and the SSI system will create the system design.

Case 1: HR Application - Assume a business intends to construct a human resources (HR) application that would authenticate organizational software services and gather personnel background information. In the component of service authentication where the employee's name, postal address, and educational background are required, the HR application will implement the SSI idea. Assume that each employee is required to install the business's employee wallet application on their own mobile phone in order for the corporation to obtain their personal data. The wallet application requires a link to a service provided by the institution from which an employee graduated, which verifies the employee's claim of receiving a degree. The aforementioned use case is designed as

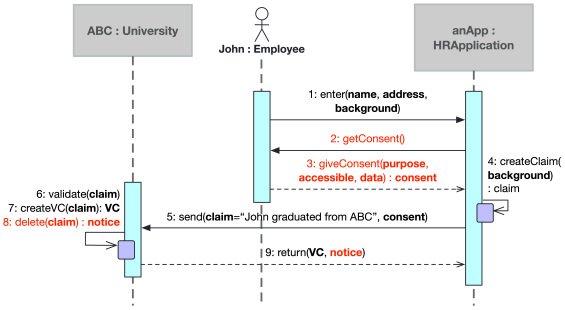

Figure 4: A use case for the HR application's service authentication scenario.

a sequence diagram in Fig. 4. Three properties are specified for the application: P3, EP5, and EP8. For instance, the EP5 Persistence property defines a constraint as follows:

> "A SSI system must communicate any rectification or erasure of SSIs to every participant."

Using this constraint, we may be concerned about a claim's rectification after it has been validated by the institution. As a result, we add two additional messages to the sequence diagram (i.e., messages 8 and 9), which satisfy this constraint.

Case 2: Traffic Police Application - Assume that a city's police department wishes to construct a traffic police application. This program is intended to enable a traffic police officer to conduct driver's license checks while on patrol. Drivers must carry a wallet application containing their personal information related to their driver's license. A police officer would do the checks by asking a driver to share their verifiable claim on their driver's license on the police application. The police application will validate it against a relevant blockchain schema. The above scenario is depicted in Fig. 5 as a sequence diagram. Assume that this application is developed with the goal of achieving two properties: AP28 and AP29. For example, the AP28 Purpose Limitation property defines a constraint as follows:

> "A SSI system must communicate the purposes of SSI processing to an owner."

This property may be held in this circumstance if the application is required to process a verified claim on the driver's license, which goes beyond the application's initial purposes. It necessitates informing the owner of the additional purposes, which results in the insertion of message 7.

These two use cases indicate how the proposed list of properties can be used to real-world applications in a variety of different disciplines.

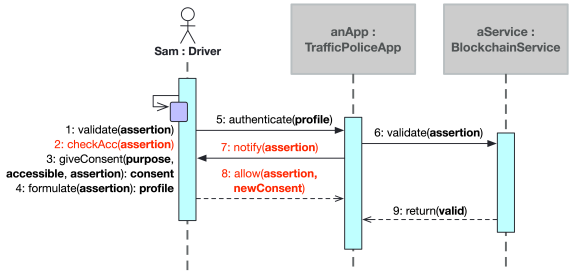

Figure 5: A use case for the traffic police application's license checking scenario.

Table 9: A summary of the questionnaire's responses - See the raw data attached in (Pattiyanon and Aoki, 2021).

Property Name	Agreed Responses (%)
EP2. Sovereignty	100.0%
EP4. Transparency	100.0%
EP5. Persistence	100.0%
EP8. Consent	100.0%
EP10. Protection	100.0%
AP21. Information Handling	100.0%
AP22. Authentication	100.0%
AP23. Accountability	85.71%
AP24. Communications Security	85.71%
AP25. Secure Configuration	100.0%
AP26. Role Management	100.0%
AP27. I/O and Error Handling	100.0%
AP28. Purpose Limitation	100.0%
AP29. Accuracy	100.0%

5.2 Expert Opinion

The preceding section discussed the applicability of the proposed set of properties in terms of their ease of adoption in specific use scenarios. Through an online questionnaire (Google Forms), we seek expert opinion on the proposed list of properties in this section. We created a questionnaire with two sections. The first section discusses the SSI system in general, its functions, and the proposed set of properties. The second section includes a set of fourteen questions that assess if the limits imposed by each added and upgraded property contradict with the SSI system's fundamental concept. If a conflict arises, we will seek justification from a relevant expert.

We contacted 21 participants with a minimum of one year of expertise in the identity management sector. We believe that the qualification will help demonstrate that professionals can grasp the notion of the SSI system even if they have no prior experience with it. We had eight responses, but one was from a developer with fewer than a year of experience. We omit that response from the conclusion in favor of a summary in Table 9.

The result that most of the properties are compatible with the notion of the SSI system. An expert, on the other hand, disputes two additional properties: AP23 and AP24. An expert argues that the AP23 Accountability property's definition should contain an audit log and that the AP24 Communication Security property's definition should reflect the consent obtained when data is communicated. Because audit logging is optional in the system aspect and consent is defined by another property (the EP8 Consent property), we infer that those inputs are suggestions.

6 DISCUSSION

The evaluation findings in two areas demonstrate significant benefits and limitations for SSI system implementers. These advantages and limitations are worth considering. This section discusses the findings in relation to the pre-defined research questions discussed in Section 2 as well as potential threats to validity.

> "RQ1. *Could the SSI system properties be easily reconciled with well-known credible sources?*"

We discovered that by examining and demonstrating the proposed list of properties in domain use cases (Section 5.1), the proposed properties could assist SSI system implementors by offering insight into what should be controlled. The sequence diagrams (Figs. 4 and 5) demonstrate that some functions may be lacking in the absence of the proposed properties. The new functionalities assist the SSI system in acquiring fundamental concepts and requirements while also ensuring compliance with credible sources. However, two limitations are evident in its applications: (1) The proposed properties do not entirely reconcile the SSI system's implementation with credible sources, as some endorsed tasks are not directed at the system (as we excluded in Section 4.2). It may need additional effort on the part of an organization to comply with them, but the effort will be significantly less than the effort required to implement without the proposed properties; and (2) the proposed properties' definition is subjective to implementors. Due to the fact that the proposed properties are specified in natural language, their application may result in human errors or misconceptions.

> "RQ2. *Are the properties still valid for the SSI system's fundamental notion after the properties have been enhanced by the addition of endorsed tasks from credible sources?*"

Due to the fact that the SSI system's fundamental notion are defined differently from those of credible sources, it is possible that the proposed properties with the addition of endorsed tasks will conflict with the fundamental notion. Plus the fact that our approach for analyzing consistency in Section 4 did not take the fundamental notion into consideration, we created our evaluation procedure to utilize expert

opinions to test the proposed properties against them. The first section of the questionnaire instructs experts to review fundamental notion that may bolster their confidence in the experts' comprehension. The result in Table 9 indicates that the majority of experts feel the proposed properties remain valid for the fundamental notion of the SSI system. However, the proposed properties were unable to demonstrate their validity against real-world SSI system solutions. This disadvantage is viewed as a limitation of this research.

6.1 Threat to Validity

As of our research design, we found two groups of threats to validity: internal and external threats. We will discuss on each group, respectively.

Internal Validity. This research identifies three internal threats to validity. First, this work relies on only five credible sources to bolster the SSI system's properties. It validates our work for certain sources but may invalidate it for others. This is, nevertheless, a starting point for individuals interested in improving the properties further. Additionally, credible sources are drawn from well-known and widely-applicable standards and regulations. At the very least, such sources were embraced globally. Second, as stated previously, this work does not include an assessment of its application to real-world SSI system solutions. The evaluation of use cases is entirely theoretical. However, we feel that the use cases we used are defined by the SSI system's fundamental notions. If real-world SSI system solutions are derived from those notions, the proposed properties cannot be used in any other way. Finally, the evaluation described in Section 5.2 was not undertaken with SSI system experts. We were unable to gather significant input for this work due to the scarcity of SSI system expertise. However, we invite professionals in the domain of identity management, which is closely tied to the SSI system. As a result, they can use their skills effectively to comprehending the SSI system after it is introduced.

External Validity. We discovered only a threat to validity externally. Apart from the use cases evaluated, real-world SSI system solutions may incorporate a variety of complex technologies. This may have an effect on the suitability of the proposed property definition, as it may be inapplicable to certain technologies. Regrettably, we were unable to verify that all implemented versions adhere to the proposed properties. However, as illustrated in Tables 7 and 8, the proposed properties are described at a high level of abstraction. It should be able to apply them without difficulty with the manual interpretation.

Table 10: A comparison of this work with other property proposals.

Related Work	#Property	Security?	Privacy?	Source
Allen (2016)	10	No	No	N/A
Ferdous et al. (2019)	17	No	No	Notions
Naik and Jenkins (2020)	20	No	Yes	GDPR
Our work	29	Yes	Yes	5 sources

7 RELATED WORK

The evaluation and discussion demonstrate the inherent advantages and disadvantages of the proposed properties. However, there are other proposals that seek to strengthen the SSI system's security and privacy as well. This section will compare the proposed properties to existing ones and discuss how the SSI system will be enhanced in related works.

To begin, we compare the proposed properties to those already proposed for the SSI system. Table 10 summarizes our comparison and emphasizes our strengths. Our work supports the ideas made by Allen (2016) and Ferdous et al. (2019), who made no reference to credible sources of property. Furthermore, whereas our work considers both the security and privacy aspects of the SSI system, Naik and Jenkins (2020)'s approach focused exclusively on the privacy issue and made a reference to the GDPR only.

On the other hand, various initiatives have been undertaken to enhance the SSI system's security and privacy. The majority of them, however, concentrated on enhancing certain technological features, such as the process for establishing zero-knowledge proofs (Lee et al., 2020) and the network communication protocol Stokkink et al. (2020). Additionally, the researchers tried to build trust in the SSI system by building a quantitative approach for assessing issuer reputation (Bhattacharya et al., 2020). Our work focuses on the overall enhancement of the SSI system, and it should be applicable in conjunction with other related work.

8 CONCLUSIONS

The terms "principle" and "property" refer to concise statements describing constraints based on the SSI system's fundamental concepts. While the current principles and properties proposed were not standardized, they were widely embraced and acknowledged in academic and industrial works on the SSI system. We determined that existing proposals vio-

lated well-established standards and regulations. We undertake a comparison analysis in this study to discover inconsistencies and then use them to suitably update the property definition. We propose an expanded list of 29 SSI system properties that includes the endorsed tasks that are missing from five credible sources. The proposed properties are demonstrated in two use cases and are concluded the definition agreed upon by identity management specialists.

This work is limited across some ways, including its relevance and suitability for real-world SSI system solutions, as well as the ambiguity of its definition. They may serve as a guide for our future work, which will concentrate on showing them in real-world circumstances using rigorous techniques such as model checking. With a formal model of the SSI system and formalized properties, it might be used successfully and profitably to real-world solutions.

REFERENCES

Allen, C. (2016). The Path to Self-Sovereign Identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

Bhattacharya, M. P., Zavarsky, P., and Butakov, S. (2020). Enhancing the Security and Privacy of Self-Sovereign Identities on Hyperledger Indy Blockchain. In *Int. Symp. on Netw. Comput. Commun.*, pages 1–7.

Centers for Medicare & Medicaid Services (1996). The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Ferdous, M. S., Chowdhury, F., and Alassafi, M. O. (2019). In Search of Self-Sovereign Identity Leveraging Blockchain Technology. *IEEE Access*, 7:103059–103079.

International Organization for Standardization (2009). Information technology - Security techniques - Evaluation Criteria for IT Security (ISO/IEC 15408:2009).

International Organization for Standardization (2011). Information technology - Security techniques - Privacy framework (ISO/IEC 29100:2011).

International Organization for Standardization (2013a). Information technology - Security techniques - Code of Practice For Information Security Controls (ISO/IEC 27002:2013).

International Organization for Standardization (2013b). Information technology - Security techniques - Information Security Management System - Requirements (ISO/IEC 27001:2013).

Lee, J., Hwang, J., Choi, J., Oh, H., and Kim, J. (2020). SIMS : Self-Sovereign Identity Management System with Preserving Privacy in Blockchain. *IACR Cryptol. ePrint Arch*. https://eprint.iacr.org/2019/1241.pdf.

Naik, N. and Jenkins, P. (2020). Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems. In *Proc. Int. Symp. on Sys. Eng.*, pages 1–6.

Nieles, M., Dempsey, K., and Pillitteri, V. Y. (2017). NIST Special Publication 800-12 Revision 1 - An introduction to information security. *NIST Special Publication*.

OWASP (2020). Application Security Verification Standard 4.0.2.

Pattiyanon, C. and Aoki, T. (2021). Analysis and Enhancement of Self-Sovereign Identity System Properties Compiling Standards and Regulations (Full Version). https://doi.org/10.5281/zenodo.5792398.

Stokkink, Q., Epema, D., and Pouwelse, J. (2020). A Truly Self-Sovereign Identity System. *arXiv*. https://arxiv.org/pdf/2007.00415.pdf.

The European Parliament and the Council of the European Union (2016). European General Data Protection Regulation (GDPR).

The International Security Trust and Privacy Alliance (ISTPA) (2009). Privacy Management Reference Model Version 2.0.

The Personal Data Protection Commission (2012). The Personal Data Protection Act 2012.

Tobin, A. and Reed, D. (2017). The Inevitable Rise of Self-Sovereign Identity: A white paper from the Sovrin Foundation [White Paper]. https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

W3C (2019). Verifiable Credential Data Model 1.0. https://www.w3.org/TR/vc-data-model/.