Proposed ***Sovereign Identity Framework for Blockchain-based Land Registry***

The land registry framework is designed to provide a secure and trustworthy way of managing land registration data. The framework is built on a decentralized and secure architecture, using blockchain technology to ensure data integrity and immutability. It includes several key components that work together to enable secure, private, and trustworthy real estate transactions.

The concept of self-sovereign identity (SSI) is based on the principle of identity established by [1], and has since been expanded upon by several authors. Christopher Allen's article highlights the ten essential principles for SSI [2], while [3] offer similar but slightly different classifications of SSI principles. However, no single classification is complete, and some principles may not fit neatly into any one group. This study introduces the principle of "Inclusion" and removes the principle of "Existence" to better suit the needs of developing countries. The "usability" principle is also added to the assessment model, recognizing the importance of customer service in creating effective digital identity systems. The proposed taxonomy compares SSI solutions based on compliance with the principles outlined by [4], [5]

1. User Control and Consent: Self-sovereign identity puts users in control of their own identity information. This means that individuals should have the right to determine what personal data is collected, how it is used, and who has access to it. Users should also have the ability to revoke consent and delete their data at any time.
2. Privacy and Protection: Self-sovereign identity requires that personal data be protected and kept private. This includes using encryption and other security measures to prevent unauthorized access, and ensuring that personal data is not shared with third parties without explicit consent.
3. Persistence: Self-sovereign identity requires that identity information be persistent, meaning that it can be used across different applications and contexts. This requires the use of standardized formats and protocols for identity information, such as decentralized identifiers (DIDs) and verifiable credentials.
4. Transparency: Self-sovereign identity requires that identity systems be transparent and open. This means that the rules and processes governing identity systems should be clearly defined and visible to all stakeholders, and that there should be a clear audit trail for all identity transactions.
5. Portability: Self-sovereign identity requires that individuals have the ability to easily move their identity information from one system to another. This means that identity systems should be designed to allow for easy transfer of personal data, and that users should have the ability to take their identity information with them as they move between different systems and applications.
6. Interoperability: Self-sovereign identity requires that identity systems be interoperable, meaning that they can work together seamlessly. This requires the use of open standards and protocols for identity information, as well as the ability to transfer and use identity information across different systems and applications.
7. Human Integration: Self-sovereign identity requires that identity systems be designed with human needs in mind. This means that identity systems should be user-friendly and accessible, and that they should be designed to accommodate a wide range of human needs and abilities.
8. Inclusion: Self-sovereign identity requires that identity systems be inclusive and accessible to all. This means that identity systems should be designed to accommodate a wide range of cultural, linguistic, and social contexts, and that they should be accessible to individuals regardless of their socioeconomic status, location, or other factors.

Together, these principles form the foundation of the self-sovereign identity model, which aims to put individuals in control of their own identity information while also promoting security, privacy, and interoperability.

Table 1 provides a brief and succinct summary of the SSI principles and the corresponding SSI components that can be employed to ensure compliance with these principles. Furthermore, the succeeding paragraphs offer more detailed elucidation on each SSI component utilized in creating a land registry framework that complies to the SSI principles.

Table 1. Overview of SSI principles and required SSI components for its compliance

SSI Principle	*SSI Components*
Control & Consent	• asymmetric cryptography authentication protocol • DPKI (DID holder) • verifiable credential • asymmetric cryptography authentication protocol
Privacy & Protection	• ZK capable verifiable credentials • pairwise-pseudonymous DIDs • Verifiable presentations • DKMS endpoints
Persistence	• Time revocation • Revocation list • Proof of non-revocation • DKMS key recovery
Portability	• Open standard DID • Interoperability Standards • Data Formats (e.g. JSON-LD)
Transparency	• open protocols and open standards • Verifiable Credentials • Distributed Ledger Technologies (DLTs)
Interoperability	• JSON-LD • universal resolver • DID Auth protocol
Human Integration	• DID naming system • Digital credential wallet
Inclusion	• DID documents • verifiable presentation • Multiple identifiers • Anonymous credentials

1. Proposed SSI framework

A. SSI-based land registry Framework

The land registry process can be difficult to manage and can involve multiple departments and entities. To overcome these difficulties and increase inter-department cooperation, an architectural design based on the description of Self-Sovereign Identity (SSI) was developed. SSI-based land registration systems make inter-departmental communication feasible and provide significant data protection for owner and property data. The SSI based land registry framework is shown in figure 1

The proposed SSI-based land register architecture involves three main players: the owner/seller (holder), the buyer (verifier), and an issuer (government entity such as the Land Registry, Bank, Surveyor, and Revenue Department). The Owner/Seller is the core subject of a property transaction in the land registration system. Through the use of user agents, both buyers and sellers can manage their digital identity by generating and saving domain names (DIDs) and cryptographic keys in their digital wallet. They can also save passwords and credentials and configure permissions. A wide range of gadgets, such as cell phones and laptops, can be used to connect with the agents. The owner/seller keeps full control over all of their data, including any land-related documents represented by verified credentials (VCs).

Overall, the proposed SSI-based land registration system provides a secure and efficient way to manage land registry processes and facilitate inter-departmental cooperation. It offers a high level of data protection for owner and property data, which is crucial in maintaining the integrity and transparency of the land registry process. By incorporating user

agents and institutional agents, the proposed system ensures that all stakeholders can manage their digital identities and maintain control over their data.

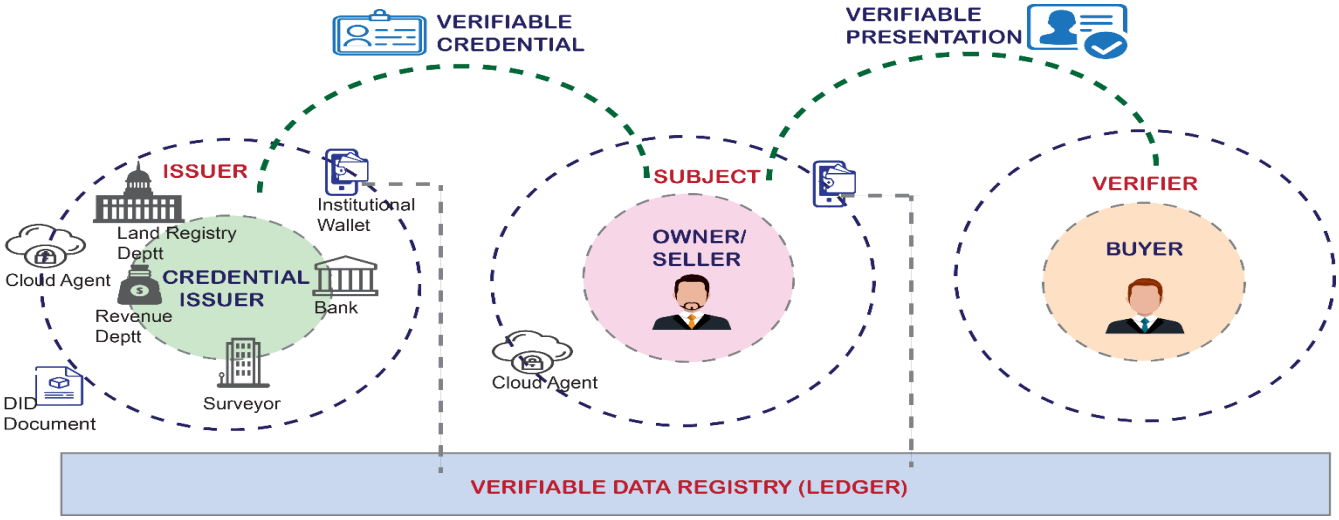

Figure 1. SSI based Land registry framework

B. SSI roles: (Issuer, verifier, and holder) and complies with SSI property

A VC is a set of cryptographically signed and hence verified by another party (verifier). Depending on the situation, they may use a different type of verifier. The SSI roles are shown in figure 2. The next sections introduce and clarify the various responsibilities of individuals when interacting with VCs [17].

(1) Issuer

The function of issuer is performed by a trusted party whose identity and public key are publicly known. It is up to the verifier to determine whether or not an issuer is credible.in the case of land registry, Issuers may include a public entity. for example, A land registry certificate(VC) could be used to verify the identity of the identity holder. Finally, the issuer signs the VC with a digital signature. The digital documents are provided to the buyer, who keeps them in their digital wallets [17]

(2) Holder

Only the holder has the authority to make claims on behalf of acquired VCs on the holder's behalf. A VC might be a person, a company, or mobile device.. Apart from these interfacing parties, there is another player in the game, namely that of the certificate's subject . the attributes of the subject is attested to the certificates.In SSI, the holders are referred to as the VC subject. Furthermore, the holder of these VC should not be permanently associated to them.

(3) Verifier

The holder must provide the verifier with information about their own identity or other relevant attributes. It obtains this information using Verifiable Presentation (VP), which depend on one or more previously stated statements and backed up by evidence of their correctness. Verifiers employ proof requests to determine which data has to be proven. For each claim that needs to be validated, a proof request outlines the requirements that must be fulfilled before the claim can be verified.

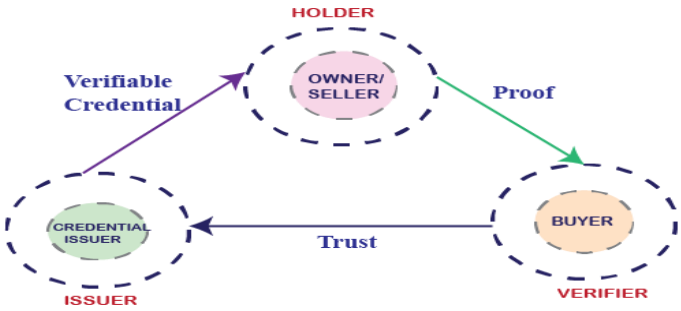

Figure 2. Roles of SSI system

C. Process Flow of Land registration system using SSI

In the context of a self-sovereign identity-based land registry framework, we have identified a generalized process flow that can be applied to a land registry framework while ensuring compliance with the principles of self-sovereign identity.

The SSI process flow in the land registry framework consists of several crucial steps, including DID generation, acquisition of verifiable credentials from identity issuers, storage of VCs, and interaction with verifiers through verifiable presentations. The identified properties are connected to specific steps in the process flow, as presented in Figure 3.The creation of secure DIDs is a crucial step in the process as it enables verifiable decentralized identity, providing verifiability and authenticity while empowering entities with existence and representation. After DID creation, the identity holder can either request to access the land registry service or request an assertion from identity issuers [16].

When acquiring a service, proof requests are needed to proceed with identification and verification. The identity holder can submit a verifiable presentation that enhances *privacy* and allows for *minimal disclosure* of identity data required for the interaction. This facilitates *ownership and control*, *privacy*, *minimal disclosure*, *and consent* while ensuring *verifiability and authenticity*[16].

If the identity holder does not have all the required credentials, they must obtain appropriate assertions (VCs) from trustworthy issuers, which are then stored in the user's digital wallet, along with identifiers. The user can present these credentials as needed while maintaining *ownership and control* of the identity and associated data.The SSI process also ensures portability and interoperability, enabling the transfer of identity data between wallets or devices and the ability to access services from different wallets or devices.

To ensure compliance with the principles of self-sovereign identity, the land registry framework must also ensure security and protection, usability, and a good user experience throughout the entire SSI process. Additionally, transparency, standardization, persistence, compatibility with legacy systems, and cost are general properties that should be considered in the development of the framework.

In summary, a self-sovereign identity-based land registry framework must follow a specific process flow that complies with the principles of SSI while also ensuring security, usability, and a good user experience. The framework must also consider general properties such as transparency, standardization, persistence, compatibility with legacy systems, and cost.

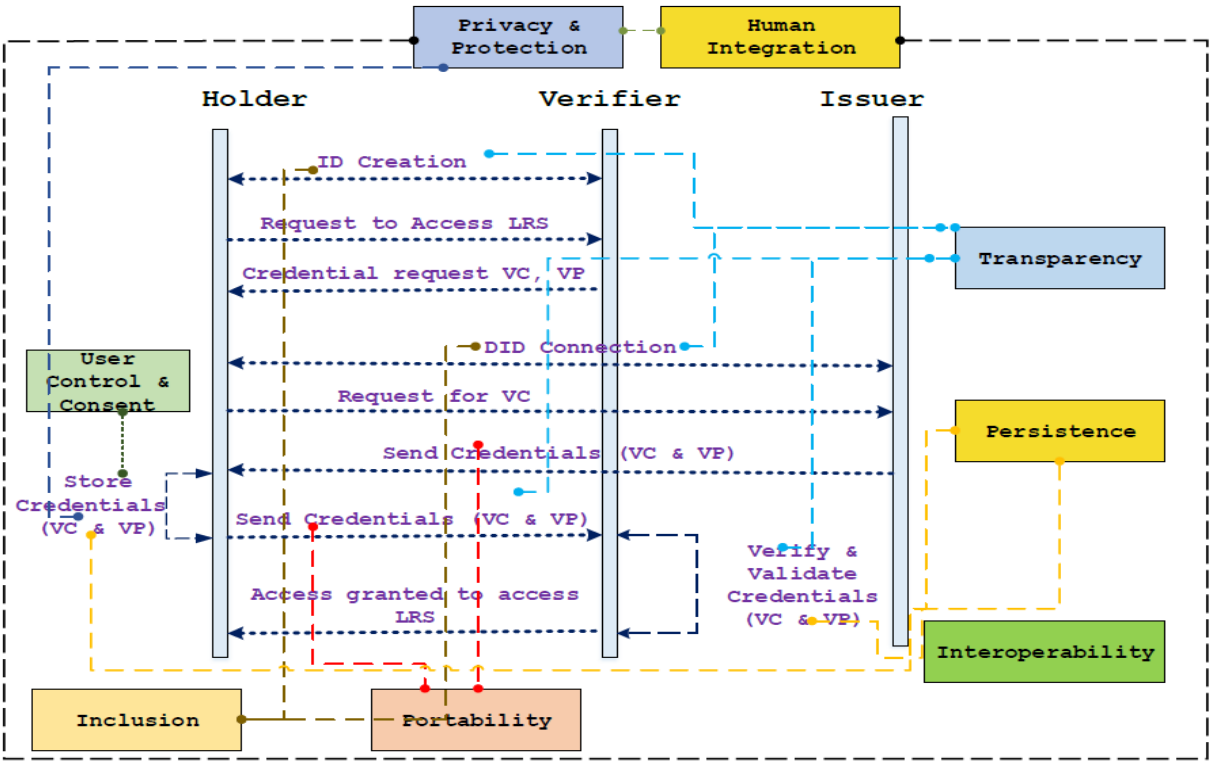

Figure 3 Process Flow of Land registration system using SSI