COMP39/9900 Computer Science/IT Capstone Project
School of Computer Science and Engineering, UNSW

Project Number: P18

Project Title: Verifiable Credentials: The Future of Digital Identity in Action

Project Clients: Evan Krul

Project Specializations: Software development; Web application development; Mobile application development; Security/Cyber Security; Human Computer Interaction (HCI).

Number of groups: 5

Background:

This project aims to implement a complete and extensible digital credential system.

Background

Digital identity no longer refers to usernames and passwords associated with some website. Our _traditional_ identities are being digitized at an unprecedented rate. Digital driver's licenses in NSW have already been available for a few years. This project addresses the challenges of digitizing these _traditional_ identity documents.

As a user, there are two factors to consider when moving to a digital identity. First, we must be issued a digital ID (e.g., through the Service NSW app). Second, we must be able to use our digital identity.

The use of an identity means being able to present it to some other party. For example, presenting a driver's licence to a bar to prove you are over 18, presenting the same driver's licence to a car rental agency, or providing documents when opening a bank account.

We use the following terms:

- Identity Owner: who the identity is for (e.g., You)

- Issuer: who issues the identity (e.g., NSW Government)

- Service Provider: the entity that needs to collect identity documents (e.g., bar, car rental agency)

The current approach to providing this functionality is centralized:

- The NSW Government stores a record of your license in their database

- You can log into the Service NSW app. The app will contact the government server and display your credentials.

- If you want to share a credential with some service provider, you 'request' that the servers of the NSW government will share your identity information with the service provider.

This centralized identity management system approach has some key fatal flaws. The

concentration of power that the NSW Government has acts as a single point of failure. For you to use your identity, the government servers have to be online and act on your behalf to share the identity.

Furthermore, the government is informed every time you use your identity. Do you want the government to know what your favourite bar is? Surely not.

The sharing of identity data with the service provider is also problematic. Oversharing of information leads to catastrophic data breaches (Medibank, Optus, etc.). A bar does not need my name and address to know I am over 18, yet the current digital identity implementations share this with them. Additionally, a bar also should not be able to track my visits by linking the presentations of my identity.

In response to these concerns, a new identity paradigm has emerged: Self-Sovereign Identity (SSI).

SSI aims to revolutionize identity management by empowering individuals to take control of their digital identity and not rely on a centralized authority \[1\].

The essence of SSI lies in the issuance and verification of user credentials. These credentials, issued by trusted entities, attest to the authenticity of a particular attribute of a user's identity. By holding the credentials, users eliminate reliance on third-party data custodians, reduce the potential for data breaches, and ensure they retain control over their identity.

Simply put, instead of storing our digital identity on the NSW Government servers, we store the credentials in a wallet on our devices. Now the process becomes:

- The NSW Government sends me a digital credential of your license

- The Driver's License credential is stored in a wallet app on your phone

- If you want to share a credential with some service provider, you choose to share the credential stored on your device with them.

You have sovereign control over the use of your identity. The credentials are signed by the issuer with a digital signature so that when a credential is presented to a service provider, it can be verified (hence the name Verifiable Credentials). For more details, see Sections 1 and 2.1 of this paper: <https://arxiv.org/pdf/2404.06729>.

We can also expand verifiable credentials (Selective disclosure Section 3.2.1, Unlinkability Section 3.2.2 in <https://arxiv.org/pdf/2404.06729>).

Requirements and Scope:

The Project

This project aims to develop a comprehensive end-to-end SSI implementation to serve as a basis for future implementations and evaluations.

There is no solid, open-source, extensible, and up-to-date implementation of a complete SSI identity system. Having this in place would allow the demonstration and communication of SSI. Implementation of the extensions (i.e., Selective Disclosure) would highlight the privacy benefits of SSI. The outcome of this project would be to provide a functional baseline implementation of a complex and interconnected multi-party system. The project promises a wide range of technical challenges, from protocol design and implementation to library creation and UI/UX considerations in the wallet application.

Good software engineering principles are key, as this project must be easily extensible to aid in the evaluation of further research in SSI.

The general goals of this project are as follows:

1. Implement the complete lifecycle of credentials:
    1. An agent library/application for issues to issue credentials
    2. An agent and wallet (app or website) for identity owners to store and use their credentials
    3. An agent library for service providers to collect credentials
2. Support of Selective Disclosure when presenting credentials
3. Support of Unlinkability when presenting credentials
4. Sample implementations to demonstrate and evaluate, e.g., A car rental collecting a driver's license and a bar verifying age from the same verifiable credential.
5. Possible support of _Identity Escrow_
    1. More on this if you take the project, but it would require a fourth library/agent implementation

The project's scope is adaptable to the student's progress and challenges encountered during the project.

The end goal is a demo application that demonstrates the life-cycle of SSI credentials and supports selective disclosure, unlinkability, and potentially identity escrow.

[1] C. Allen, “The Path to Self-Sovereign Identity.” Accessed: May 02, 2023. [Online]. Available: <https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/>

- The agents must be extensible, being able to support any format of credential + signature scheme

- Align as much as possible to existing standards being developed (<https://arxiv.org/pdf/2404.06729> Table 2).

This includes:

- Credential Format
- Verification Mechanisms
- Protocols between parties
- etc.

- Clear documentation and clean code

Required Knowledge and skills:

- Software Engineering (extensible design is a must)

- Library design/implementation

- Protocol design/implementation

- Either app or web development

- Optionally: Docker

Expected outcomes/deliverables:

- Agent/Library for Issuers
- Agent/Library for Service Providers
- Agent/Library + Wallet for Identity Owners
- Full integration of the agents + wallet
- Demo application showing the lifecycle of a credential
- Optionally: Agent/Library + protocols for Identity Escrow.

Supervision:

Evan Krul

Additional resources: