PhD Open Days

SSIBAC: Self-Sovereign Identity Based Access Control

PhD Program in Information Systems and Computer Engineering

Rafael Belchior (rafael.belchior@tecnico.ulisboa.pt)

Introduction

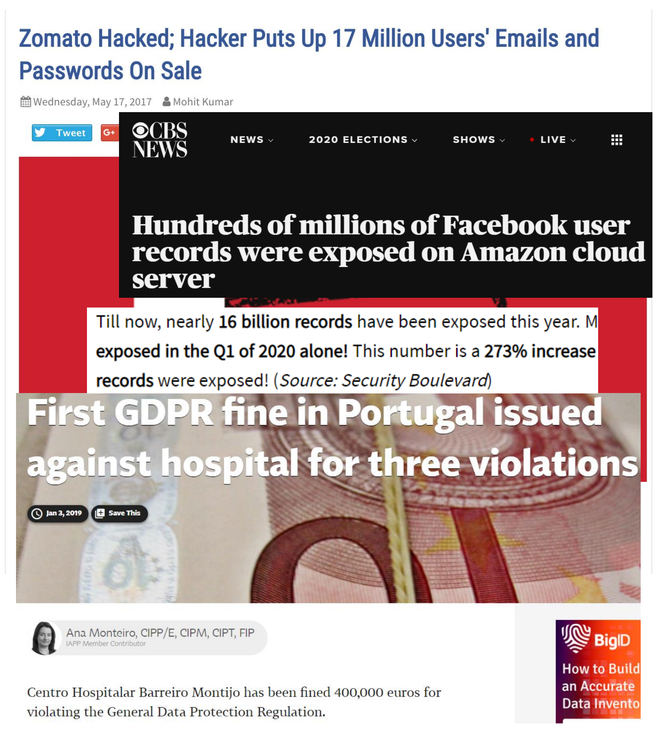
Self-sovereign identity (SSI) [1] is a new identity management approach that ensures users have full control of their personal data.

Despite regulatory efforts, such as the General Data Protection Regulation (GDPR), data breaches still occur, causing great damage.

By using techniques such as zero knowledge proofs (ZKPs), SSI allows satisfying predicates based on user data without revealing that data. This provides privacy for access control processes, where a user needs to satisfy a certain predicate to access resources [2].

We propose an access control system that follows the SSI paradigm**, Self-Sovereign Identity Based Access Control (SSIBAC)** [3].

Motivation

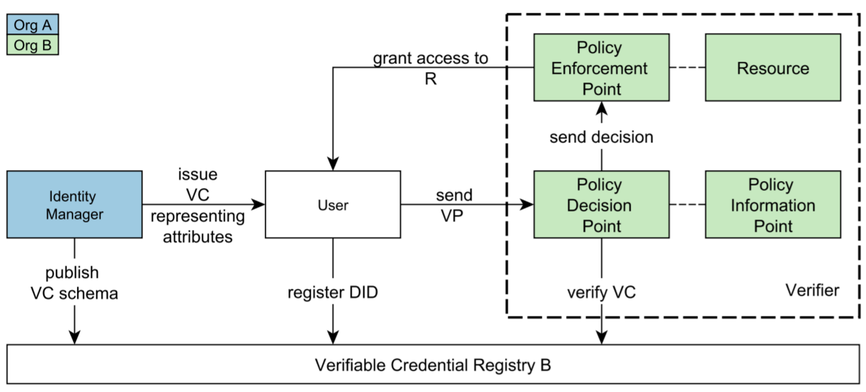


SSI Concepts

A **Decentralized Identifier (DID)** represents an identity and allows trustable interactions, rooted on a verifiable registry (e.g., a blockchain), and public-key cryptography [4].

A **Verifiable credential (VC)** provides a standard way to digitally express credentials (or claims) in a way that is cryptographically secure, privacy-respecting, and machine-verifiable [2]. This happens via **verifiable presentations (VP)**, which contains metadata and proofs for a subset of the contained claims.

Access control models (ACM) provide selective access to a set of resources, under a specific set of conditions. Common ACMs include AttributeBased Access Control (ABAC)

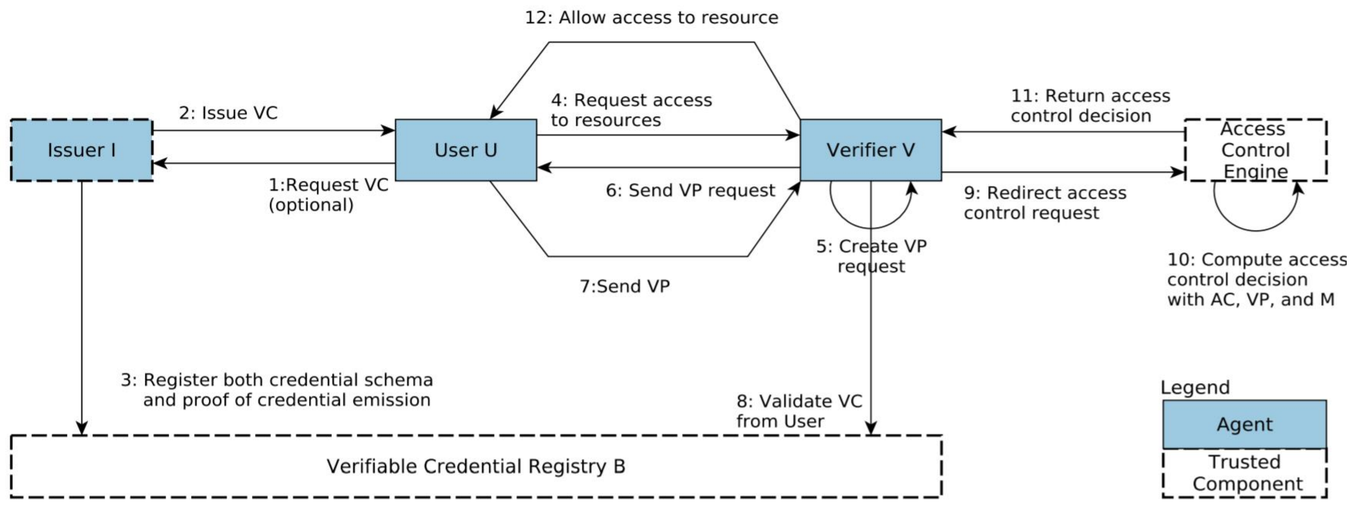


SSIBAC components.

SSIBAC

SSIBAC maps VCs to access control policies, requesting a verifiable presentation to satisfy such policy. SSIBAC can be instantiated on conventional ACMs.

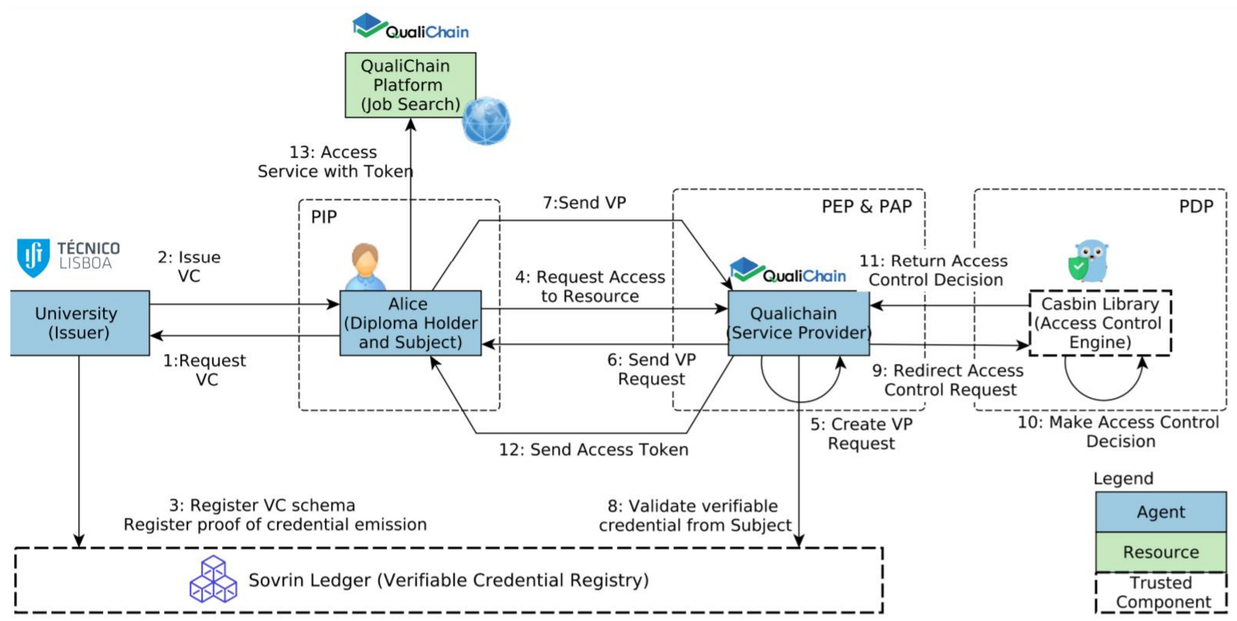
SSIBAC Access Control Flow



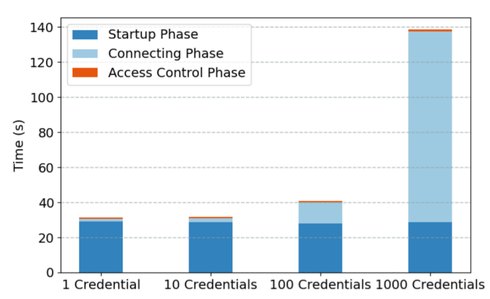
A **user** is issued **VCs**(1,2), which are rooted in a **blockchain** (3). The user then requests access a **resource** (4). The verifier calculates the necessary **access control policy** and requires a **VP**. It is sent to the user (5, 6). After the response is sent (7) and validated (8), the verifier gives as input the result of the validation process to an **access control engine** (9, 10), which decides if user can access the resource (11,12).

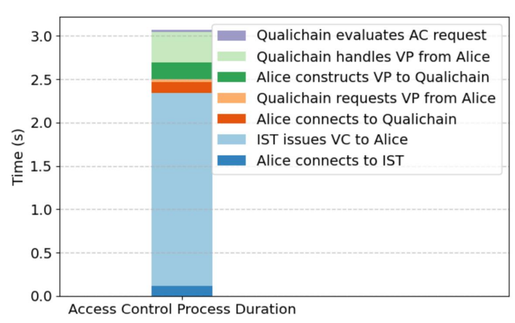
Evaluation: SSIBAC on Qualichain

SSIBAC can be useful for access control in QualiChain. We focus on granting a diploma holder access to a service provided by QualiChain. Alice has a VC from IST certifying she is a student. With this VC, Alice requires access to the Qualichain platform.



SSI-based ACM applied to the QualiChain scenario





References

[1] - Allen, C. (2016). The path to self-sovereign identityLife with Alacrity. Peck, M.. Blockchains: How They Work and Why They Will Change the World.

[2] -Sporny, M., Longley, D., & Chadwick, D.. (2020). Verifiable Credentials Data Model 1.0.

[3] - Belchior, R., Putz, B., Pernul, G., Correia, M., Vasconcelos, A., & Guerreiro, S. (2020). SSIBAC : Self-Sovereign Identity Based Access Control. In The 3rd International Workshop on Blockchain Systems and Applications. IEEE.

[4] - Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., Sabadello, M., & Holt, J.. (2020). Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations - W3C Working Draft 23 July 2020.

[5] - Qualichain. (2020). Qualichain. https://qualichain-project.eu/.

TÉCNICO LISBOA

Supervisor: André Vasconcelos, Miguel Correia

PhD Program in Information Systems and Computer Engineering

phdopendays.tecnico.ulisboa.pt