IEEE TrustCom/BlockchainSys 2020, the 3rd International Workshop on Blockchain Systems and Applications.

SSIBAC: Self-Sovereign Identity Based Access Control

Rafael Belchior

Benedikt Putz, Guenther Pernul,

Miguel Correia, André Vasconcelos,

Sérgio Guerreiro

TÉCNICO LISBOA

Universität Regensburg

inesc id lisboa 20 YEARS

DEFINING TECHNOLOGY

IEEE

QualiChain

Outline

- Introduction to SSIBAC
- Background on Access Control, DIDs and VCs, and
- SSIBAC Model
- SSIBAC + ABAC
- Use Case: Qualichain
- Evaluation
- Conclusions

inesc id lisboa 20 YEARS
DEFINING TECHNOLOGY

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

-Data breaches are usual, and its severity increasing

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

https://resilientedigital.com/wp-content/uploads/2020/01/Qu%C3%A9-es-la-Auto-Identidad-Soberana-SSI-%E2%80%93-Self-Sovereign-Identity.jpg

SSI: Self Sovereign Identity

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

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

SSI: Self Sovereign Identity

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

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

-A verifiable credential (VC) provides a standard way to digitally express credentials in a way that is cryptographically secure, privacy-respecting, and machine-verifiable

SSI: Self Sovereign Identity

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

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

-A verifiable credential (VC) provides a standard way to digitally express credentials in a way that is cryptographically secure, privacy-respecting, and machine-verifiable

-This happens via verifiable presentations (VP), which contains metadata and proofs for a subset of the contained claims. Can use Zero Knowledge Proofs.

SSI: Self Sovereign Identity

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

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

-A verifiable credential (VC) provides a standard way to digitally express credentials in a way that is cryptographically secure, privacy-respecting, and machine-verifiable

-This happens via verifiable presentations (VP), which contains metadata and proofs for a subset of the contained claims. Can use Zero Knowledge Proofs.

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

-SSI allows services to store less data about users

Access Control

Introduction

Background

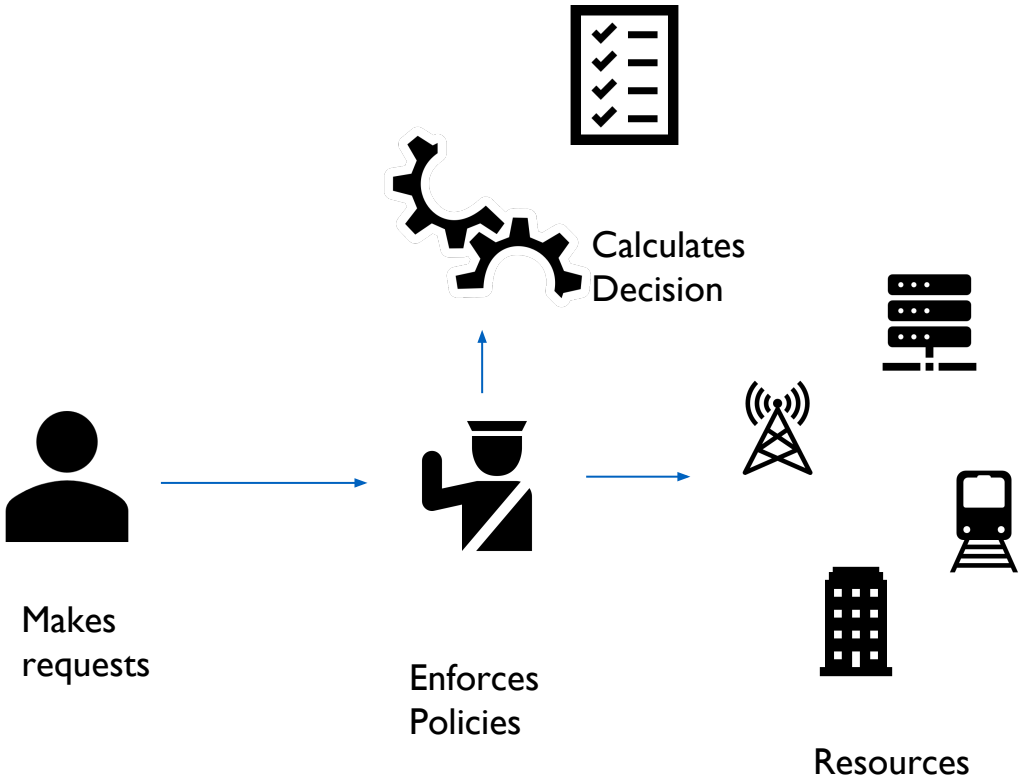
SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions



Access Control

Introduction

Background

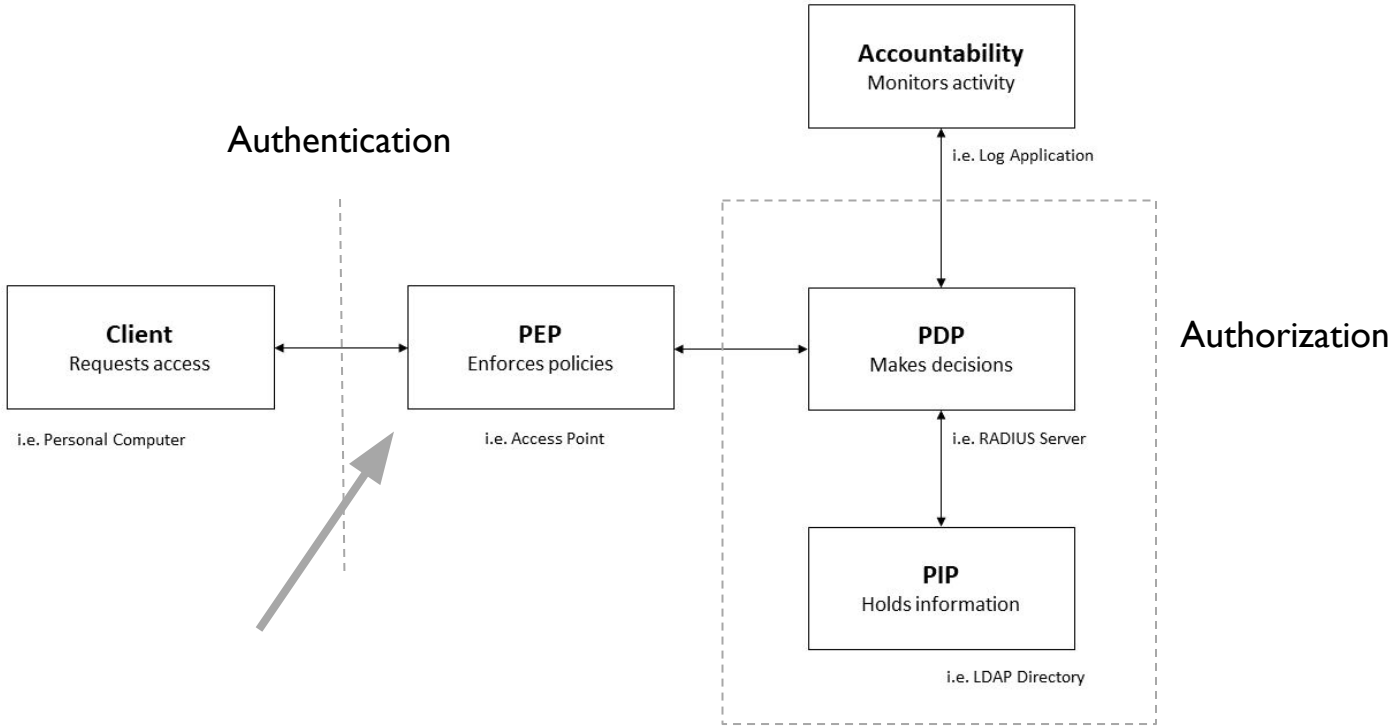
SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions



Access Control

Introduction

Background

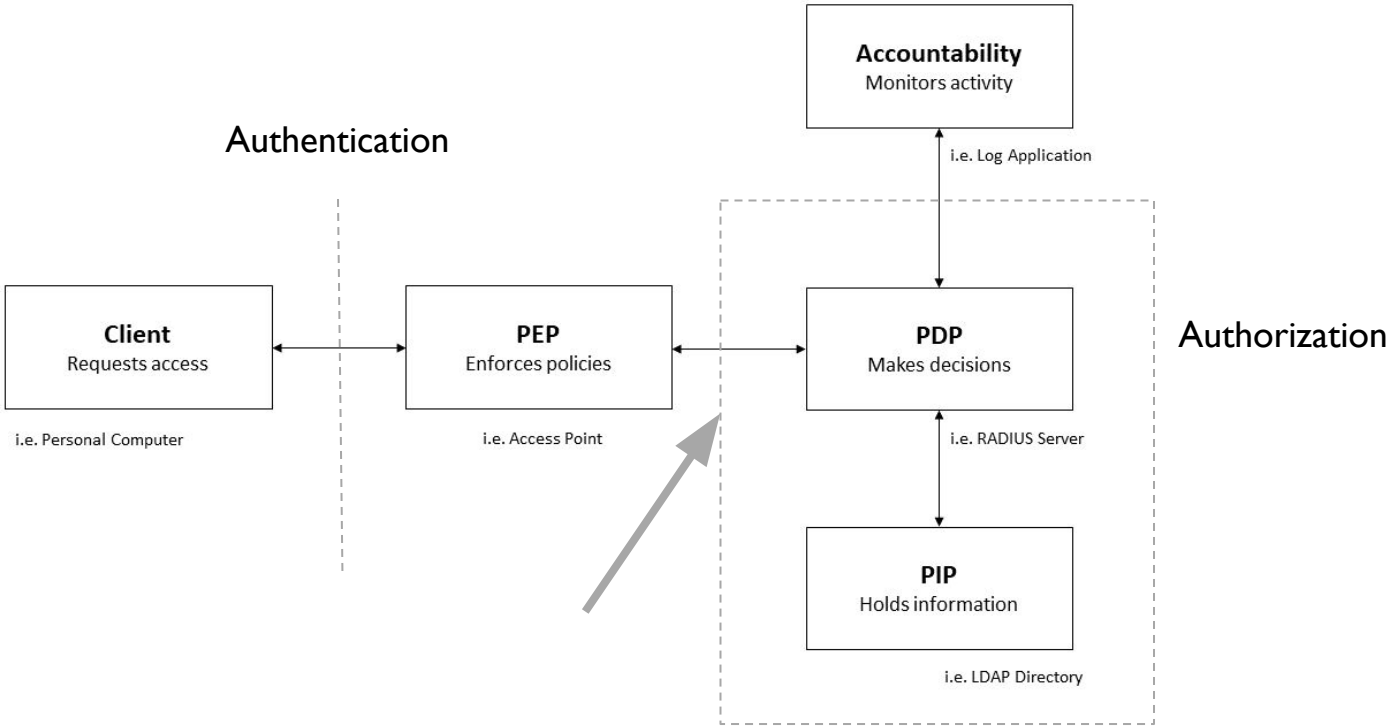
SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions



Access Control

Introduction

Background

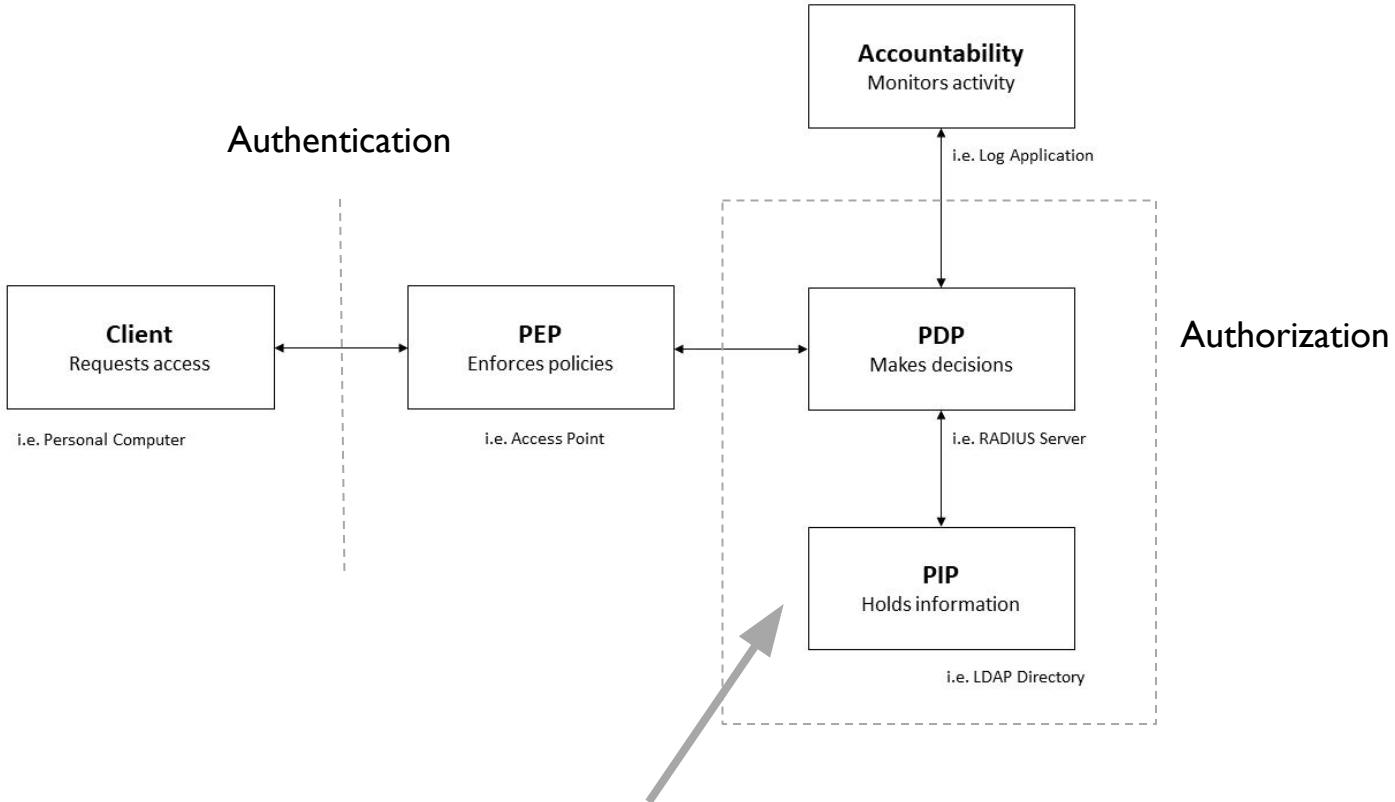
SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions



Access Control

Introduction

Background

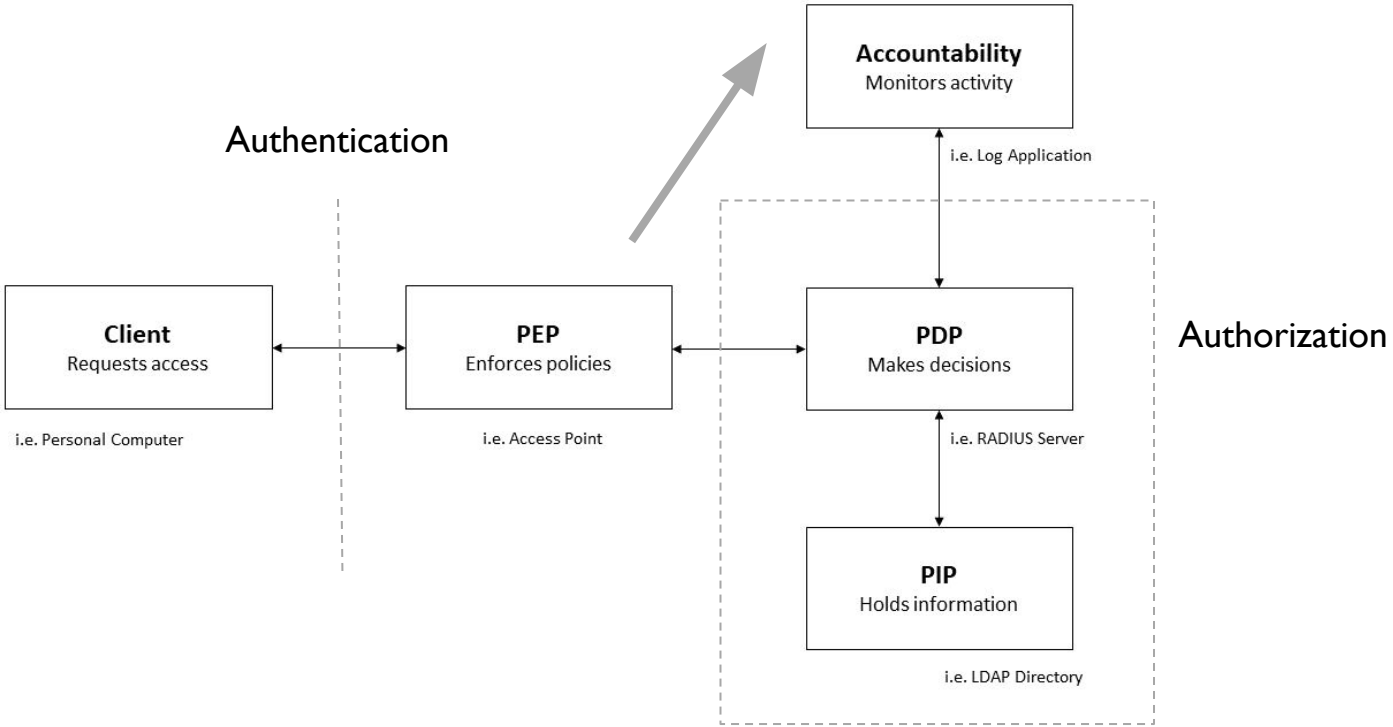
SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions



SSIBAC: Self Sovereign Identity Based Access Control

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

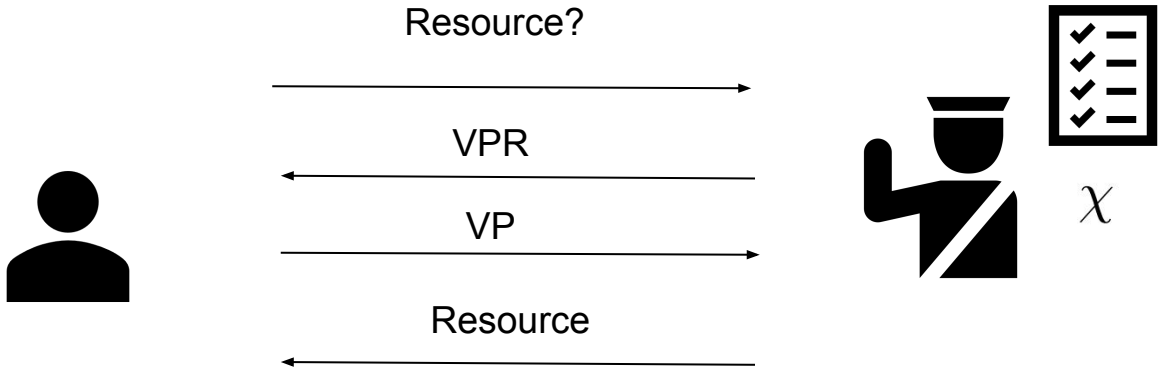
Use Case: Qualichain

Evaluation

Conclusions

SSIBAC maps:

- VCs to attributes/roles/etc... on access control policies
- access control requests to verifiable presentation requests
- verifiable presentations to access control policies
- access control policies evaluated using conventional ACMs



SSIBAC: Self Sovereign Identity Based Access Control

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

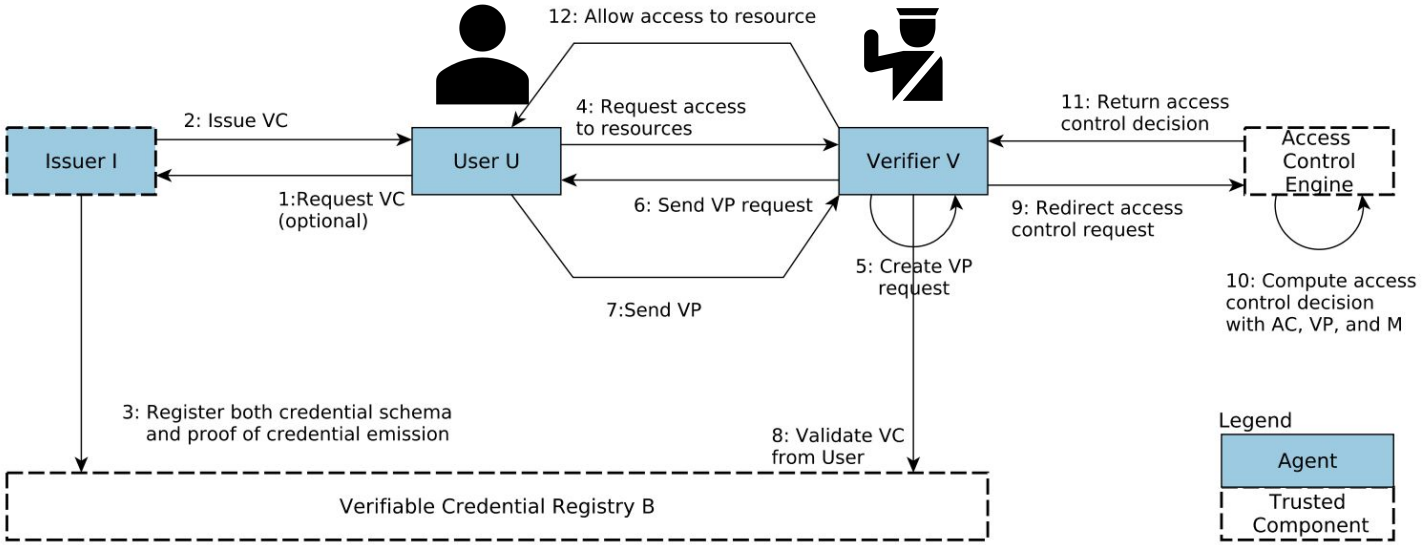


Fig. 1: Access control flow enforced by the SSIBAC model

SSIBAC: Self Sovereign Identity Based Access Control

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

SSIBAC components

- a set of users $\mathcal{U} = \{u_1, u_2, ...\}$. Each $user_i$ is identified by a DID and holds a public/private key pair (K_p^i, K_s^i) associated to that DID and a set of VCs $\mathcal{L}_i = \{l_1^i, l_2^i, ...\}$;
- a set of resources $\mathcal{R} = \{r_1, r_2, ...\}$;
- a set of issuers $\mathcal{I} = \{i_1, i_2, ...\}$ that issue VCs for users;
- a set of verifiers $\mathcal{V} = \{v_1, v_2, ...\}$ who request VPs and mediate the access control flow. Typically, they are also resource providers;
- a set of permission validators $\mathcal{P} = \{p_1, p_2, ...\}$;

Attribute, Role, etc

SSIBAC: Self Sovereign Identity Based Access Control

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

- a set of injective functions $\psi = \{\psi_1, \psi_2, ...\}$, such that $\psi_i : \mathcal{L}_i \rightarrow \mathcal{P}_k$, i.e., function ψ_i maps the VCs from $user_i$ to permission validator P_k;
- an injective function $\chi : \mathcal{AC} \rightarrow \mathcal{VP}_R$, mapping access control policies to VPRs.

χ () = VPR

SSIBAC + ABAC

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

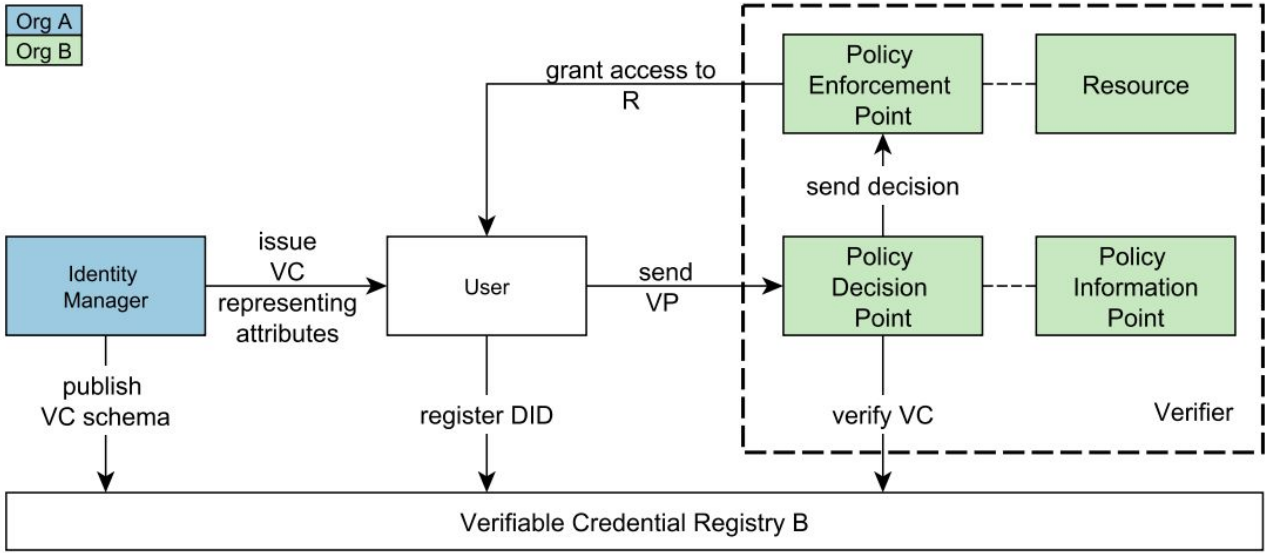


Fig. 2: SSIBAC in a multi-organizational setting, in light of the XACML standard perspective

Qualichain

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

The QualiChain project aims to propose a blockchain based approach for disrupting the archiving, management, and verification of educational and employment qualifications

Qualichain

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

Stakeholders:

- **certification seekers**, e.g., graduated students. Correspond to users (or subjects)
- **certification providers**, e.g., higher education institutes; correspond to issuers
- **certification validators**, e.g., potential employer, correspond to verifiers

Universities issue verifiable credentials for students for using the QualiChain platform.

It is desirable to use SSI-based access control in this scenario so that QualiChain does not need to store any personal data; authorization is conducted in a p2p way, using DIDs and VCs:

Qualichain

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

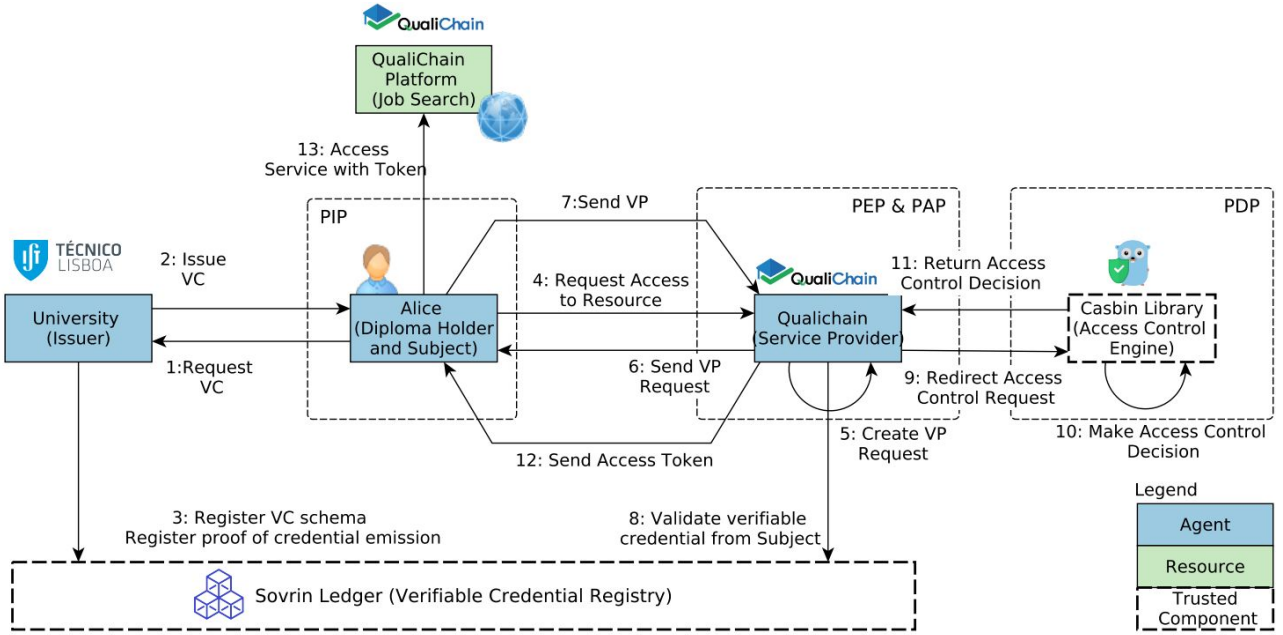


Fig. 3: SSI-based ACM applied to the QualiChain scenario

Implementation

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

HYPERLEDGER INDY

GreenLight Dev Ledger Contributed by the Province of British Columbia - vonx.io

HYPERLEDGER ARIES

Evaluation

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

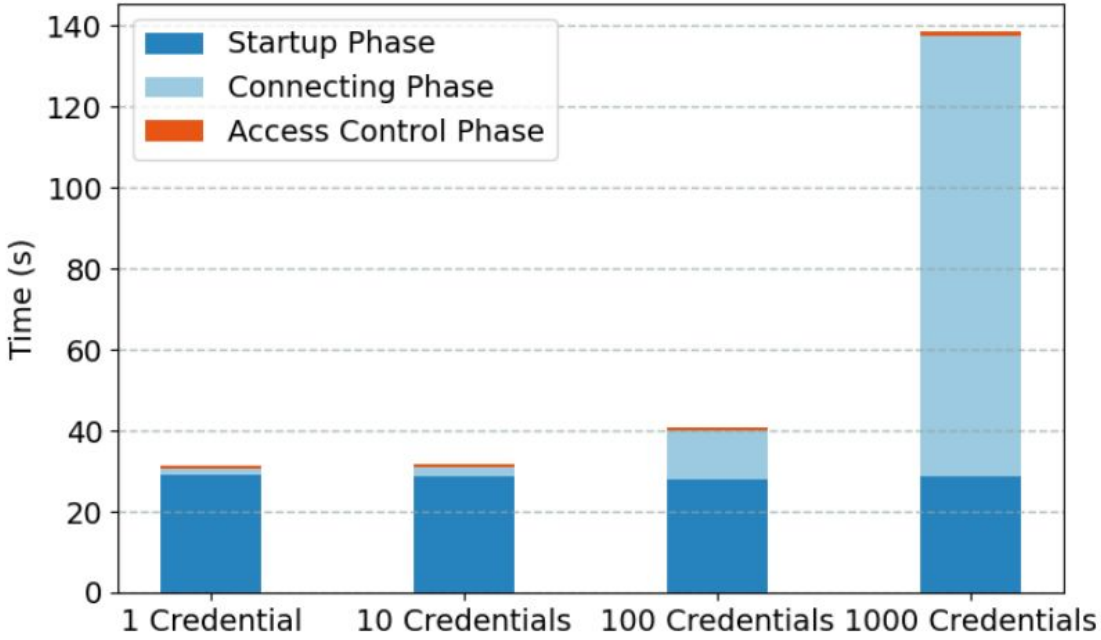


Fig. 4: Latency depending on the number of emitted credentials

Evaluation

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

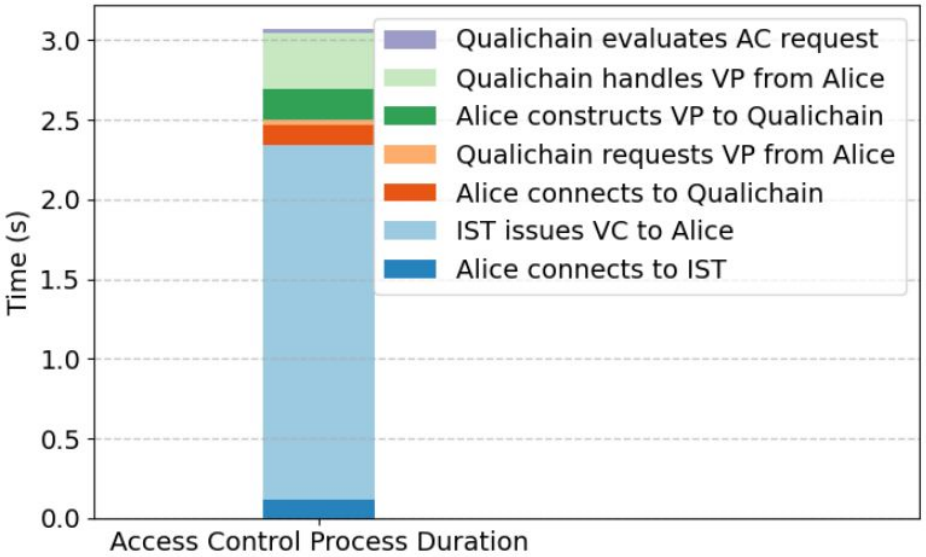


Fig. 5: Duration of the various steps in the *Connecting* and *access control* phases (startup phase omitted), with 10 issued credentials

Evaluation

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

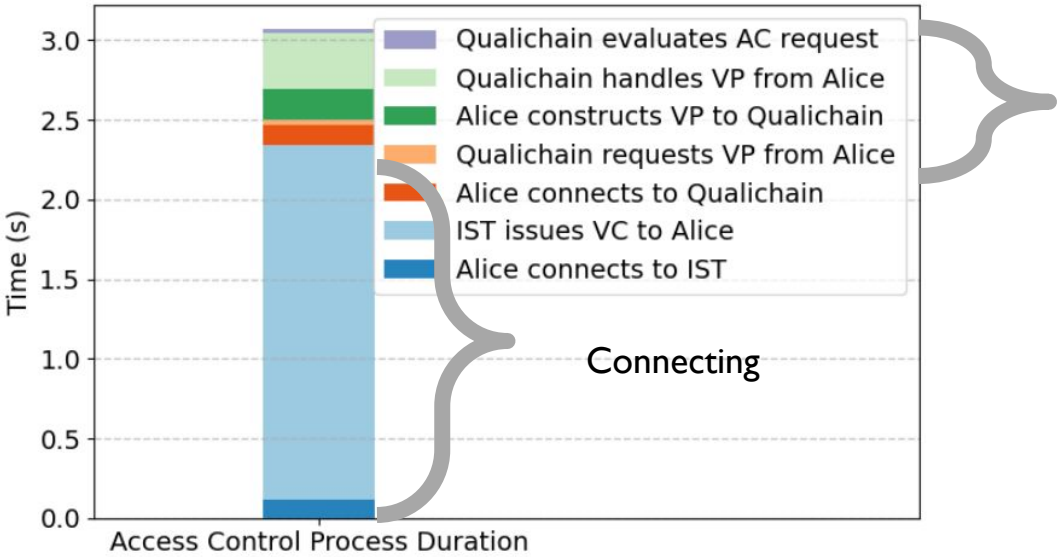


Fig. 5: Duration of the various steps in the *Connecting* and *access control* phases (startup phase omitted), with 10 issued credentials

E2E access control request and response takes ~1s

Conclusions

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

- Self-Sovereign Identity Based Access Control (SSIBAC), the first approach to access control based on decentralized identity

Conclusions

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

- Self-Sovereign Identity Based Access Control (SSIBAC), the first approach to access control based on decentralized identity

- We explore this topic by instantiating our SSIBAC model with attribute-based access control, which is applied to a real-world case, the EU QualiChain project.

Conclusions

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

- Self-Sovereign Identity Based Access Control (SSIBAC), the first approach to access control based on decentralized identity
- We explore this topic by instantiating our SSIBAC model with attribute-based access control, which is applied to a real-world case, the EU QualiChain project.
- Our experimental evaluation shows that each access control request can be served in around 0.9 seconds.

Conclusions

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

- Self-Sovereign Identity Based Access Control (SSIBAC), the first approach to access control based on decentralized identity
- We explore this topic by instantiating our SSIBAC model with attribute-based access control, which is applied to a real-world case, the EU QualiChain project.
- Our experimental evaluation shows that each access control request can be served in around 0.9 seconds.
- Although more timeconsuming than traditional centralized access control systems, access control based on self-sovereign identity can alleviate the data privacy problem

Future Work

Introduction

Background

SSIBAC Model

SSIBAC + ABAC

Use Case: Qualichain

Evaluation

Conclusions

- Explore cross-chain (and cross-blockchain) authorization, leveraging recent blockchain interoperability techniques.
  (see “A Survey on Blockchain Interoperability: Past, Present, and Future Trends)

- Verifiers are single points of failure.
  Solution: decentralizing the access control engine e.g. using blockchain based access control
  (see Distributed Attribute-Based Access Control System Using a Permissioned Blockchain)

TÉCNICO LISBOA

Thank you for your attention

SSIBAC PAPER

UR Universität Regensburg

inesc id lisboa 20 YEARS

IEEE

QualiChain