A Self-Sovereign Identity Framework for Patient-Centric Access Management

Purpose

Efficient and secure access and sharing of electronic patient data between patients and medical professionals amplify the quality of healthcare. Currently, there are various cited issues with the current models of data access management and sharing of Electronic Health Records (EHR). The following are some of the highlighted issues:

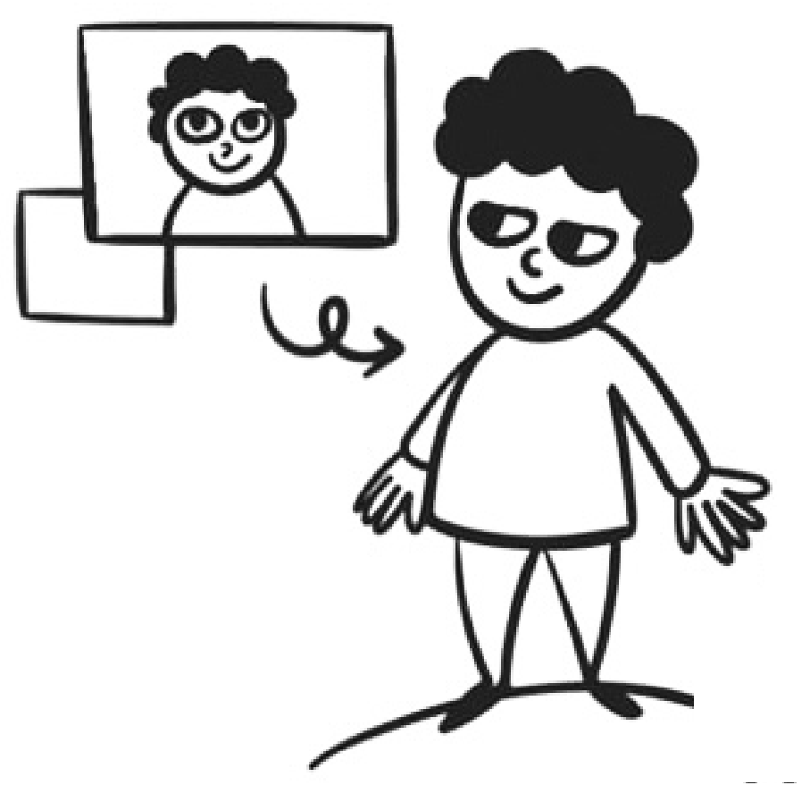
1. **Fragmented data held in different care providers.**
2. **Slow access and sharing**
3. **Interoperability**
4. **Patient sovereignty and control of data.**

We explored the use of self-sovereign identity to address these challenges and build a prototype with the aim to achieve a secure, privacy-preserving, and patient-centric access management and sharing of medical data.

Self-Sovereign Identity (SSI) is a concept that offers a digital identity that is owned by an individual or organization without the need for intermediaries. Instead of using traditional centralized intermediaries and third-parties, the identity is authorized via an autonomous distributed system. The advantage over traditional identities being full user control and autonomy. The identity is created, controlled, and used by the identity's owner.

Self-Created

Self-Controlled

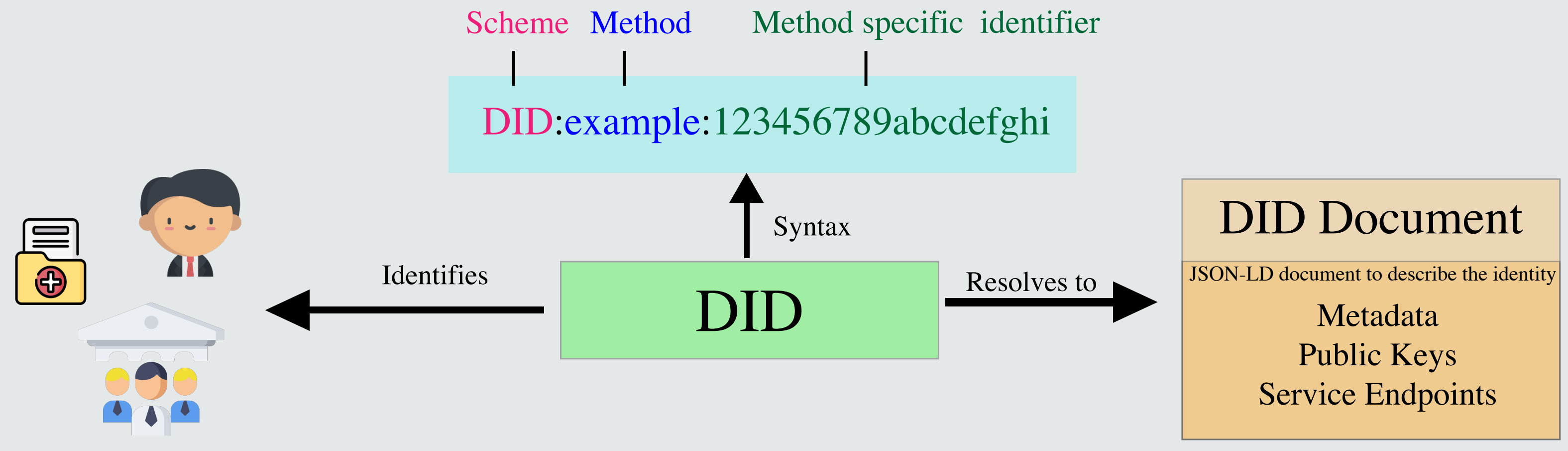


Control of use and sharing

SSI Components

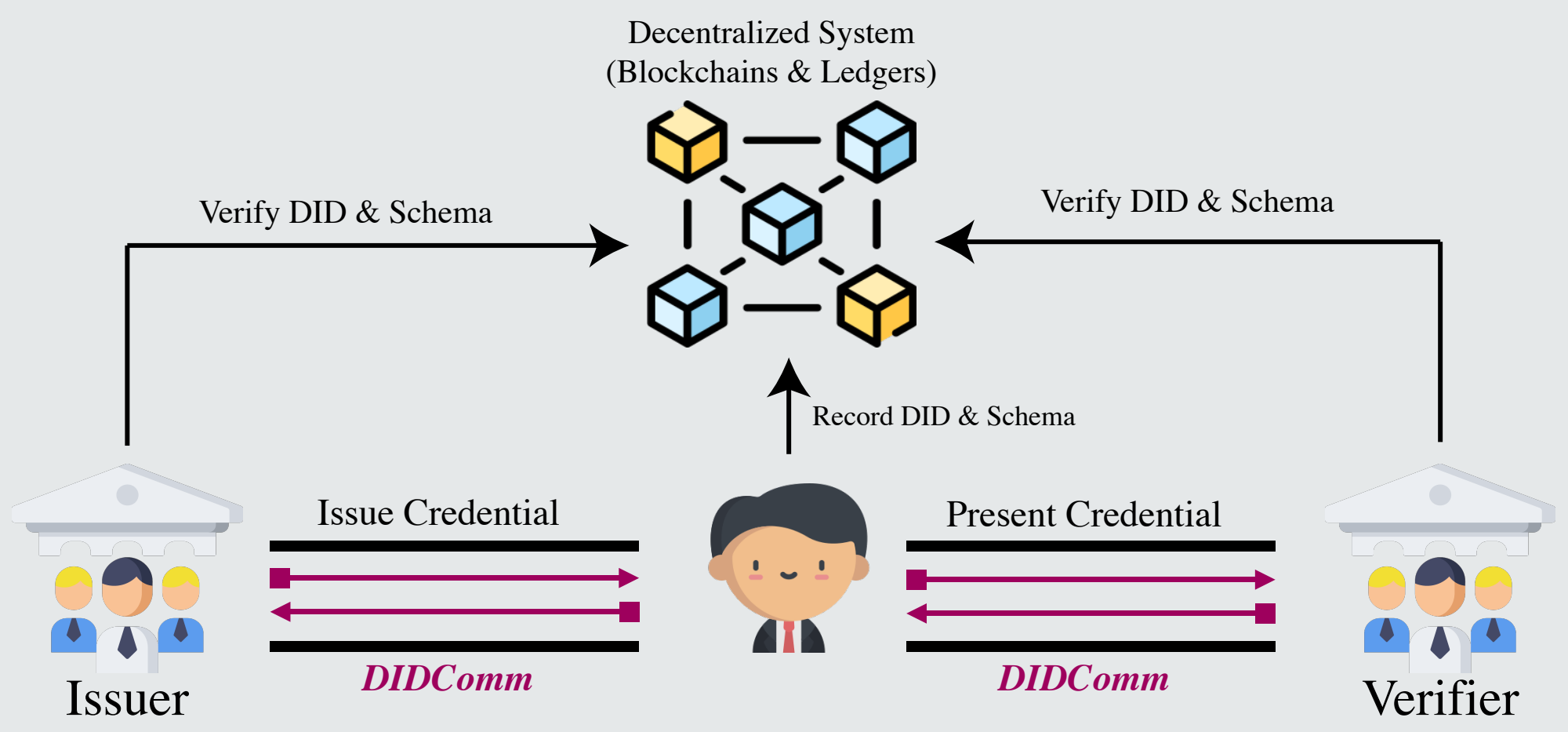
Decentralized Identifiers (DID)

A self-controlled digital fingerprint assigned to users, entities, or things. DIDs are globally unique, resolvable with high availability, and cryptographically verifiable. The DID document contains public keys and other cryptographic items including the specific DID scheme to allow secure verification.


Scheme
Method
Method specific identifier
DID:example:123456789abcdefghi
Syntax
Identifies
DID
Resolves to
DID Document
JSON-LD document to describe the identity
Metadata
Public Keys
Service Endpoints

Verifiable Credentials (VCs)

A set of cryptographic claims and metadata that provide a digital equivalent to the physical credentials we use on daily basis to verify who we say we are such as a driving license. VCs define a number of verifiable and tamper-proof claims issued by a trusted entity to the holder of the identity. These claims can be cryptographically verified by any other entities.



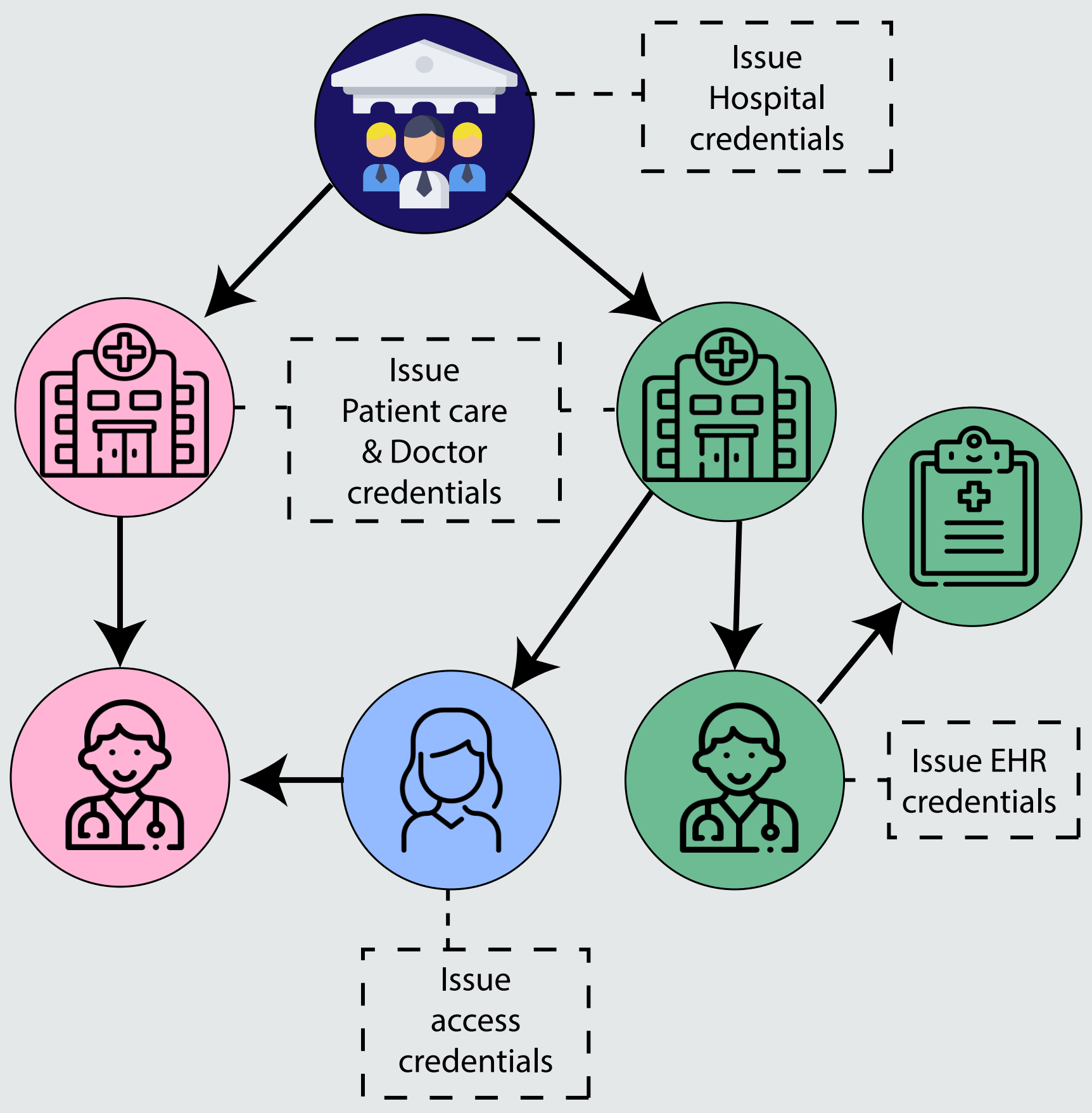
DID Communication (DIDComm)

An encrypted and asynchronous communication protocol that uses information within the DID Document, particularly the parties' public key and their endpoint to send information with verifiable authenticity.

Approach

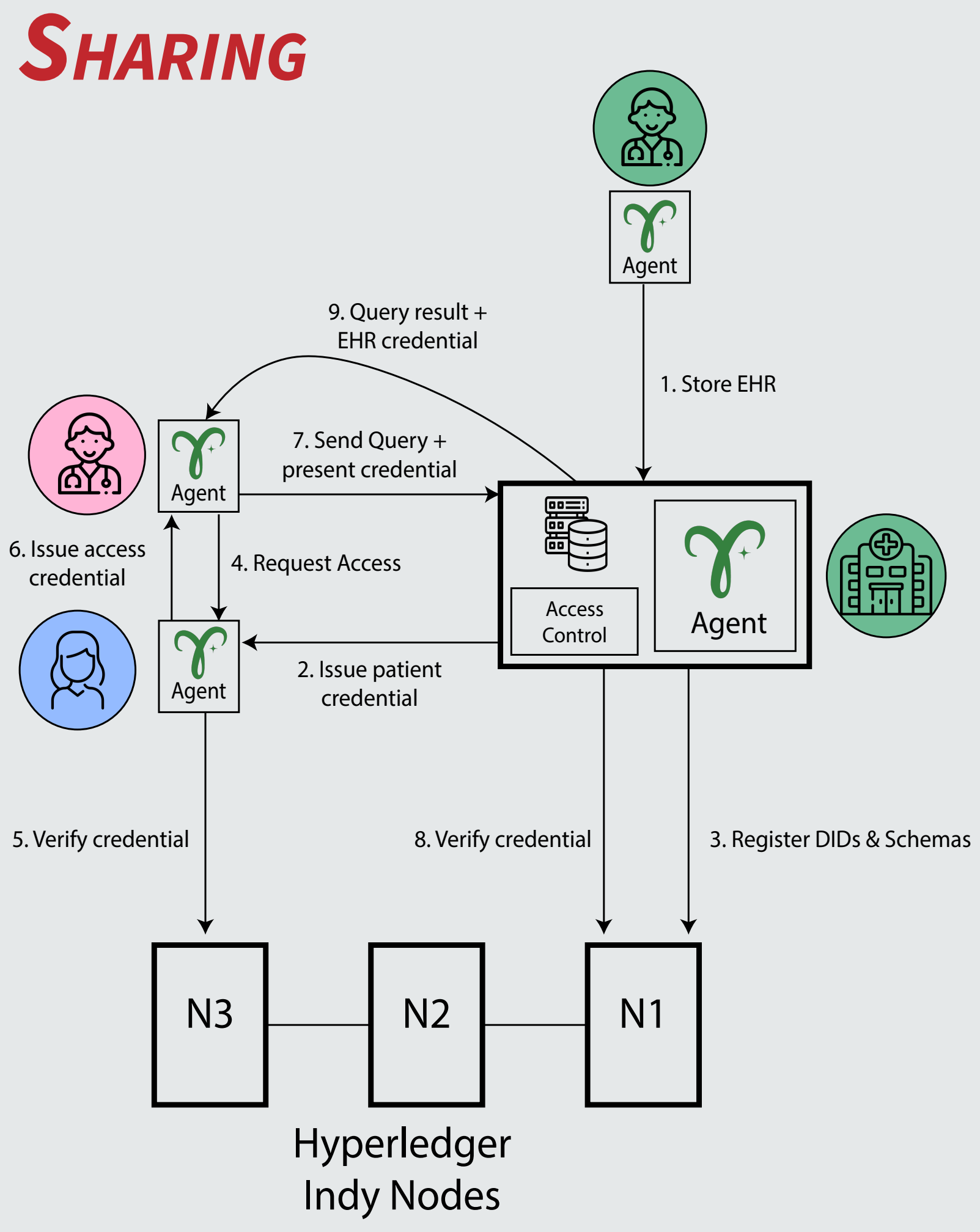
Identities and Credentials

We leverage DIDs and VCs to create digital identities for each user role: a regulator (government entity), hospitals, doctors, and patients (data owners). Hospitals are issued with credentials by a government authority allowing them to store patient data. In addition, doctors get a credential definition given by the hospital allowing the doctor to create an EHR. These data records are also given credentials by the doctor to verify their authenticity. Access credentials are issued by the patient to other doctors in order to access that EHR data.


Issue Hospital credentials
Issue Patient care & Doctor credentials
Issue EHR credentials
Issue access credentials

Establishing Trusted Access and Sharing

In our work, DIDs and VCs are created and managed by Hyperledger Aries Cloud Agents. Doctors can add a new record associated with a particular patient, and the patient can authorize access and sharing of EHR. We used Hyperledger Indy blockchain as a decentralized data registry for registering and verifying DIDs and schemas. The access control policy implements an off-chain access interface to the hospital's database, and allows access based on the presented credentials.


Agent
1. Store EHR
9. Query result + EHR credential
Agent
7. Send Query + present credential
6. Issue access credential
4. Request Access
Access Control
Agent
Agent
2. Issue patient credential
5. Verify credential
8. Verify credential
3. Register DIDs & Schemas
N3
N2
N1
Hyperledger Indy Nodes

References

[1] Reed, D., Sporny, M., Longely, D., Allen, C., Sabadello, M., Grant, R.: Decentralized identifiers (DIDs) v1.0. https://w3c.github.io/did-core/

[2] Sporny, M., Longely, D., Chadwick, D.: Verifiable credentials data model 1.0. Technical report W3C, November 2019. https://w3c.github.io/vc-data-model/

[3] Hyperledger: Hyperledger aries cloud agent - python (2019). https://github.com/hyperledger/aries-cloudagent-python

[4] Davie M, Gisolfi D, Hardman D, Jordan J, O'Donnell D, Reed D. The trust over ip stack. IEEE Communications Standards Magazine. 2019 Dec;3(4):46-51.

[5] Kish LJ, Topol EJ. Unpatients—why patients should own their medical data. Nature biotechnology. 2015 Sep;33(9):921-4.

Mohammed Alghazwi
Fatih Turkmen
Dimka Karastoyanova

Information Systems Group
Bernoulli Institute

university of groningen

faculty of science and engineering