UNSW AUSTRALIA

Credential-based Trust Management in Self Sovereign Identity

Never Stand Still | Faculty of Engineering | School of Computer Science and Engineering

Rahma Mukta

Supervisor: Dr. Hye-young Paik, Dr. Qinghua Lu, Prof. Salil S. Kanhere

Current Credential Sharing

- **Self sovereign Identity (SSI) promises much freedom and autonomy for individuals with their identity and the ability to manage identity related claims by themselves**
- **Existing SSI solutions grants a level of trust to well-known institutions (e.g., government offices, university) only [1-2]**
- **Trust issue arises when individual wants to on-board as issuer to generate their own identity related credential (e.g., provide delegation when patient is suffering from schizophrenia)**

Possible Solution

- **Onboarding of individuals as “personal issuer” to manage their own credentials**
- **Building trust in the issuer authorization process**
- **Passing flow of trust from well-known institutions to “personal issuers”, to whom trust is needed**

Aims

- **Design a verifiable and multi-level issuer trust hierarchies in SSI**
- **Design a protocol for “personal issuer” on-boarding designed on multi-level trust hierarchies**
- **Ensure individual autonomy on his/her credential**

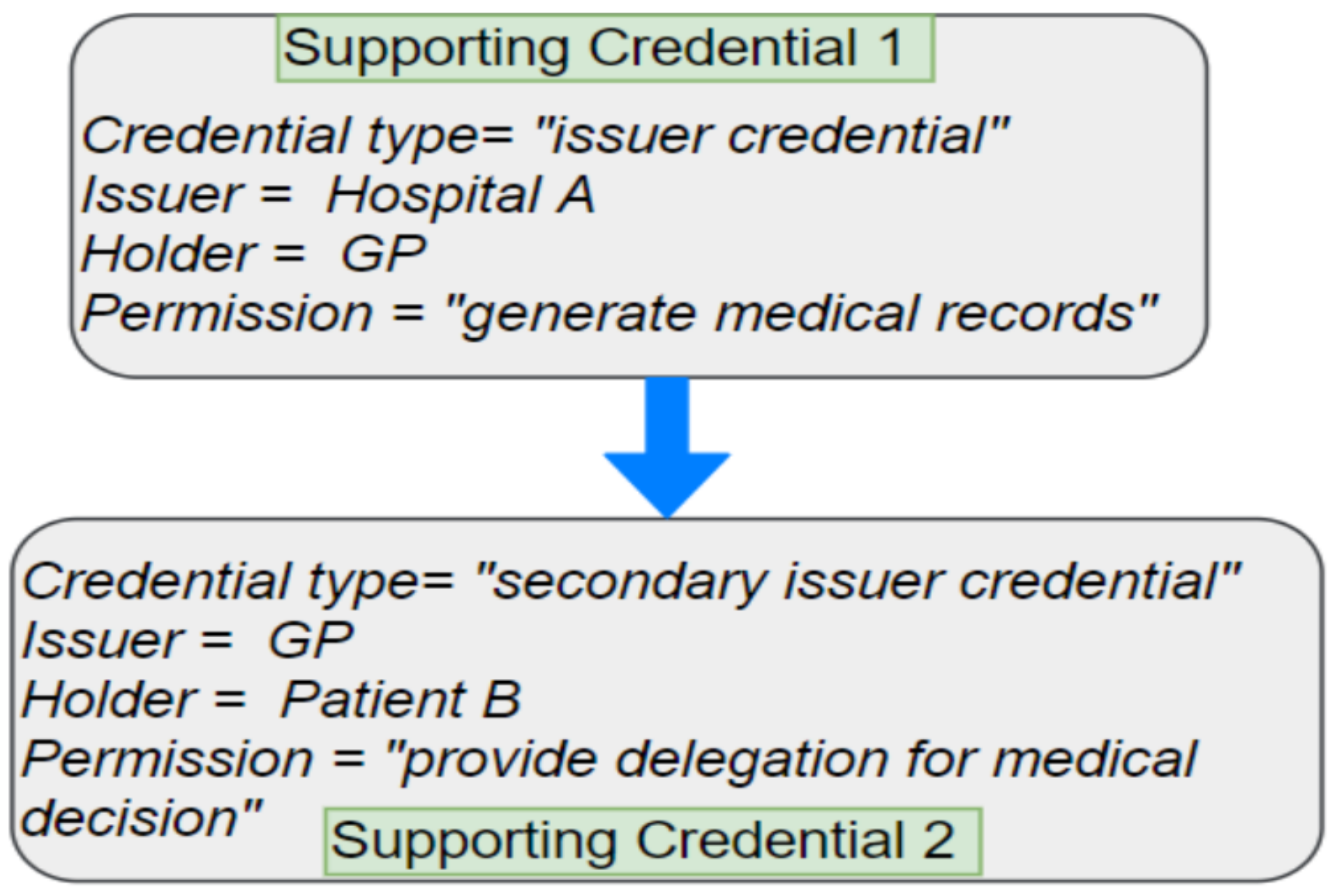

Supporting Credential 1
Credential type= "issuer credential"
Issuer = Hospital A
Holder = GP
Permission = "generate medical records"
Credential type= "secondary issuer credential"
Issuer = GP
Holder = Patient B
Permission = "provide delegation for medical decision"
Supporting Credential 2

Figure 1: Credential chain to pass the trust from well-known issuer to “personal issuer”

Approach

- **`Web of Trust' is a cryptography concept that establishes an authentic binding between a public key and its owner's attributes. Some other people assert the owner's attribute by signing it with their private key. We propose the concept of ``supporting credentials'' to introduce this “Web of Trust” principle in our framework for generating multi-level issuer trust hierarchies.**
- **A ``supporting credential'' is a verifiable credential that specifies the issuer's trust on the supporting credential holder. With this trust, the holder is on-boarded as a credential issuer.**
- **Blockchains create a secure and transparent environment for credential sharing. This enables secure authentication of credential and issuer authorization in terms of supporting credentials.**
- **Each certificate issuer and holder is uniquely represented by a blockchain account, and their issuer-holder relationship is represented by a decentralized identifier (DID), registered using respective blockchain account. DIDs are stored separately on two smart contracts, “Issuer Registry” to hold issuer DIDs and “DID Registry” to hold holder DIDs.**
- **Supporting credential recipient needs to prove their ownership to SSI platform to be onboarded as issuer. Also, “personal issuer” needs to share their supporting credential with self-signed credentials to prove their authorization as issuer.**
- **All credentials are verifiable in terms of issuer signature by the verifier.**

System Architecture

Specific contributions compared to related works are highlighted by grey background color in the figure.

External Governance Layer

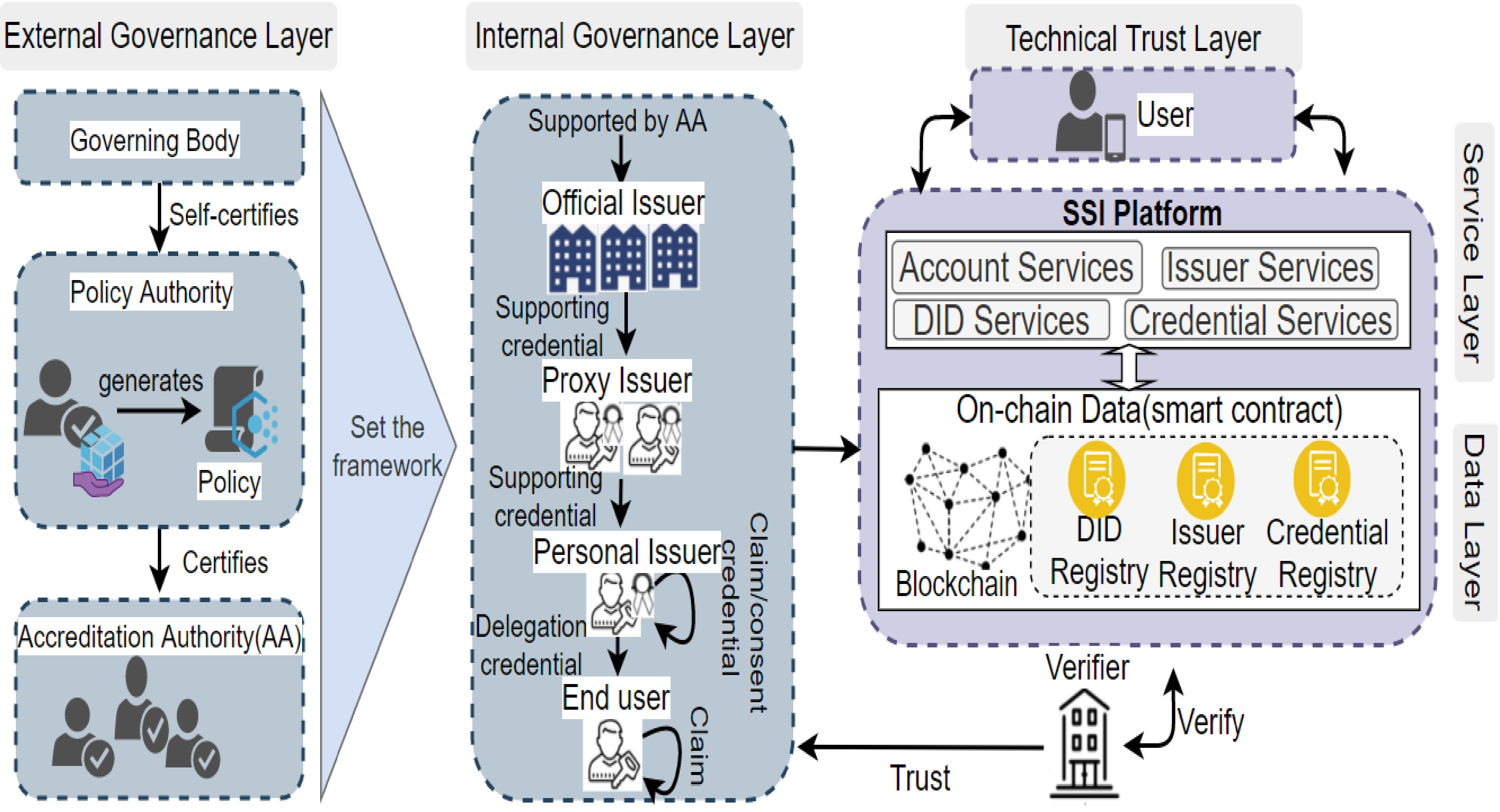
- *Trusted authority chain to define a framework (including credential schema and rules for credential issuance) to be used for “personal issuer” onboarding*

Internal Governance Layer

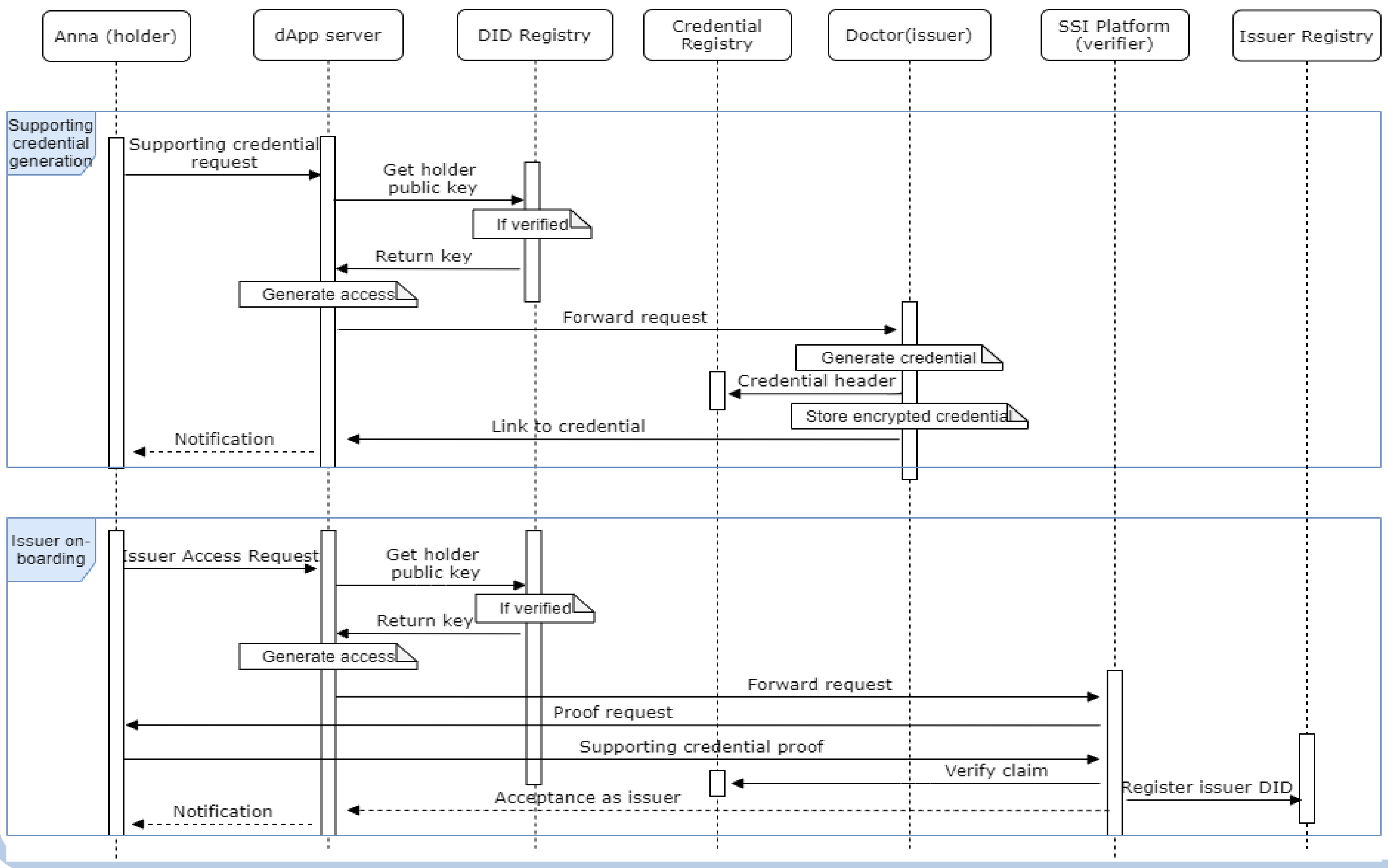
- *Multi-level trust hierarchies to pass the trust from “official issuer” (well-known institution) to “personal issuer”, finally to the submitting holder (i.e., end user)*
- *Official issuers (e.g., hospital) shows their trust to proxy issuer (e.g., doctor) by providing supporting credential*

Technical Trust Layer

- *This is the SSI platform for credential issuance and verification*
- *Credential verification includes signature verification and supporting credential verification using on-chain data*



System Implementation



System Setup

- **To ensure pure peer to peer communication, we introduced DApp server to connect client side with blockchain through smart contract**
- **Service layer of SSI platform resides on the same device as a blockchain node and the components of the off-chain data layer.**
- **Interaction among the participants is occurred through DApp server, but the server does not store any information**

Implementation Scenario

- **The figure represents the implementation scenario of “personal issuer” (Anna) onboarding, where SSI platform is in the verifier role for issuer authorization**
- **The first phase begins when Anna sends a request for a supporting credential to the DApp server**
- **Issuer(doctor) verifies holder's information and generates the requested supporting credential with storing the credential hashes on-chain**
- **During second phase, to be on-boarded as issuer Anna sends an access request to SSI platform with the above supporting credential received from doctor**
- **SSI platform verifies the authenticity and integrity of credential from blockchain and registers Anna's DID on-chain as a registered issuer**

Conclusion

- **This ongoing research work motivated the need to address the trust issue during “personal issuer” on-boarding in SSI ecosystem**
- **Blockchain-based verifiable credentials can be used to establish “web of trust” among the participants**
- **SSI platform ensures authorized issuer onboarding and also, any verifier can verify the issuer’s eligibility to issue a credential**

Future Work

- **Evaluate real time performance of the proposed protocol**
- **Expand the work to consider revoked credential while verification**
- **System stores all DIDs on-chain for data privacy. That may rise scalability issue. Further steps may consider how to balance between privacy and scalability**

References

- **Mukta, J. Martens, H. Paik, Q. Lu, and S. S. Kanhere. Blockchain-based verifiable credential sharing with selective disclosure. In IEEE TrustCom, pages 959–966, 2020.**
- **Soltani, U. Trang Nguyen, and A. An. A new approach to client onboarding using self-sovereign identity and distributed ledger. In IEEE iThings and IEEE GreenCom and IEEE CPSCom and IEEE SmartData, pages 1129–1136, 2018**