UNIVERSITÀ DI PISA

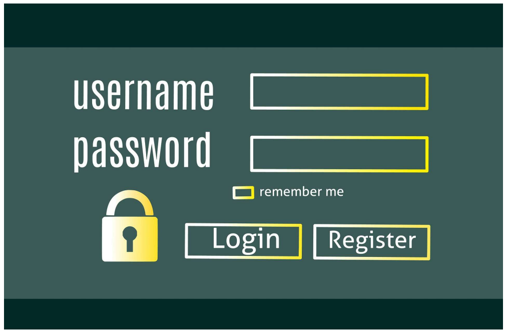
Trust Approaches in Self-Sovereign Identity

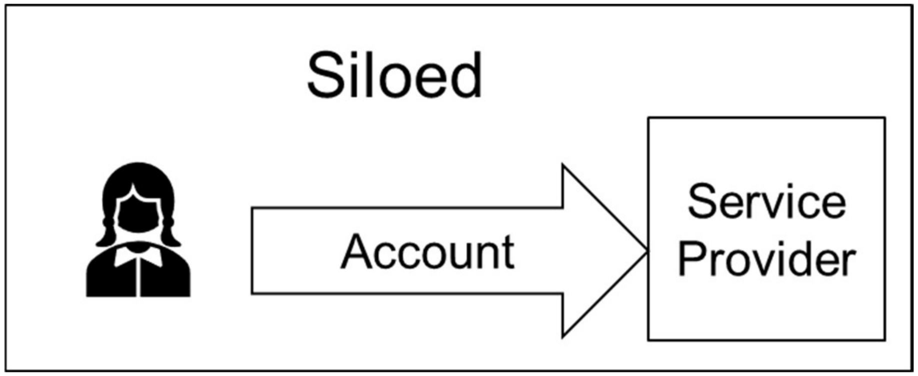
Speaker:
Calogero Turco
Mauriana Pesaresi's Seminar Series

Traditional Digital Identity

Account Based

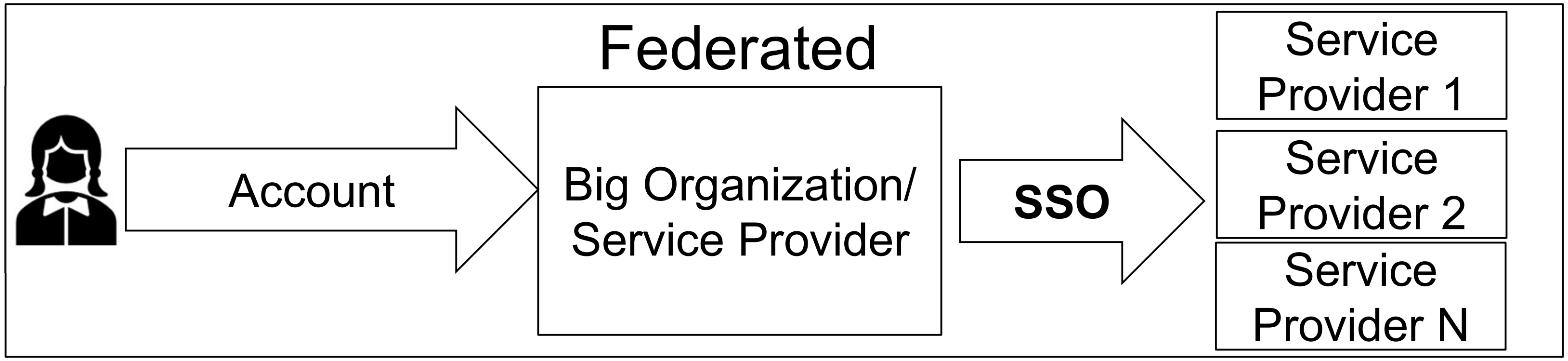
- Siloed Identity
- Federated Digital Identity
  - Single Sign-On (**SSO**)
    - Sign in as Google/Facebook




Siloed

Account

Service Provider


Federated

Account

Big Organization/ Service Provider

SSO

Service Provider 1

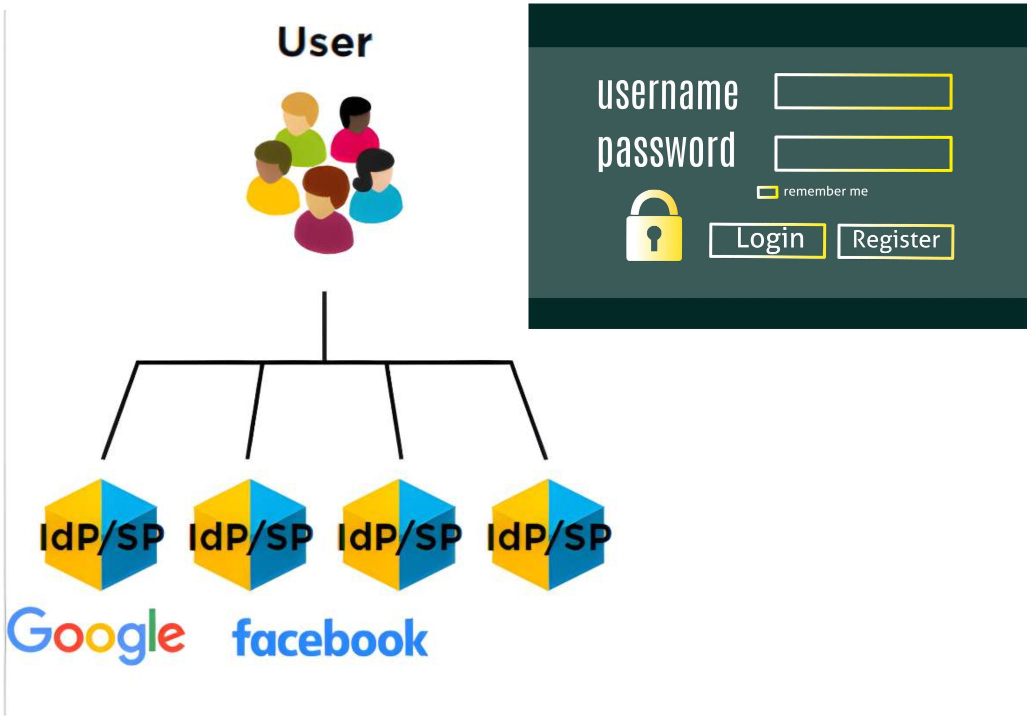
Service Provider 2

Service Provider N

Self Sovereign Identity(SSI)

Traditional Digital Identity

- Absence of control
- Security
- Censorship
- Personally Identifiable Information (PII)
- Designed for humans

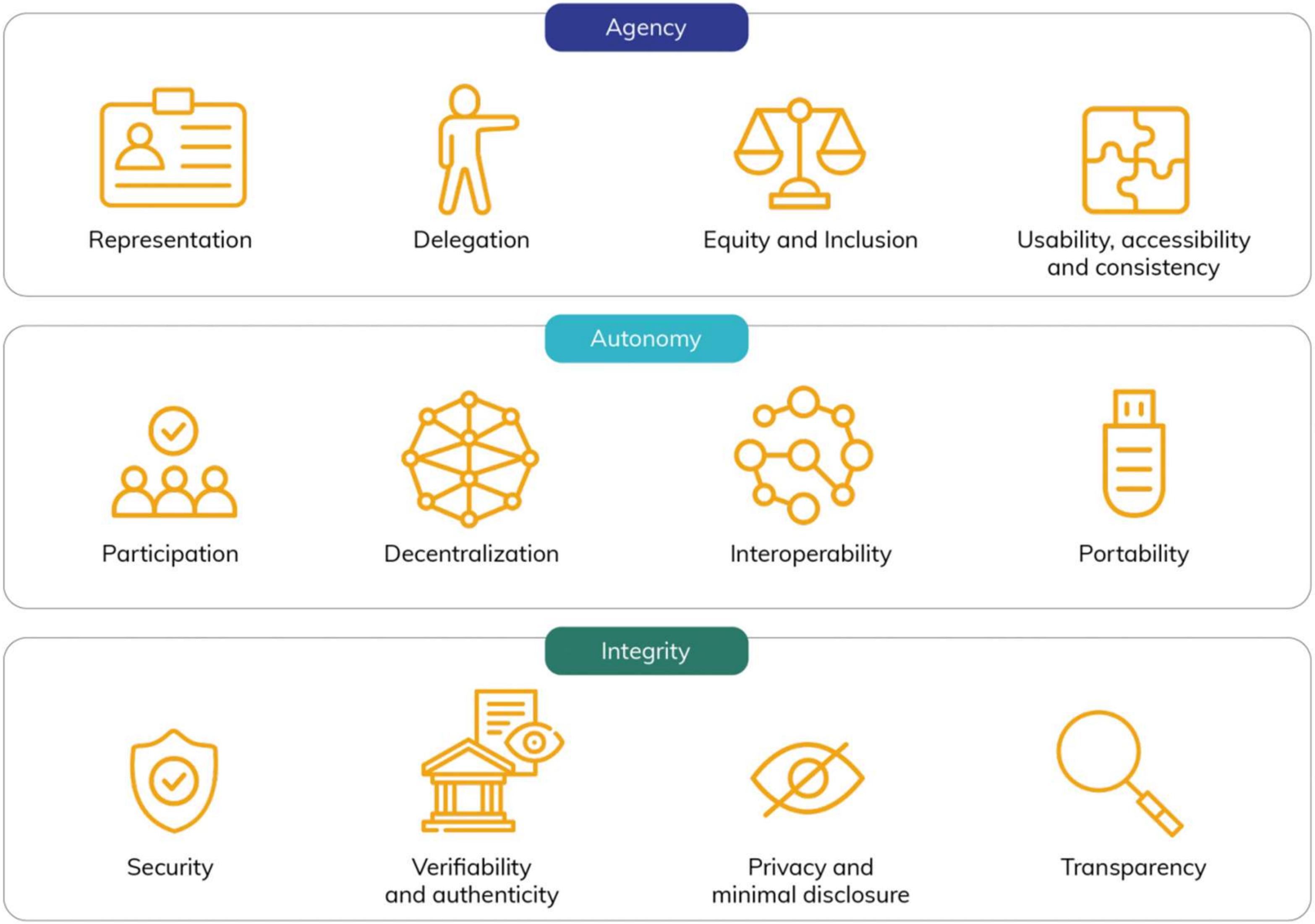


Self Sovereign Identity

By Hyperledger licensed by CC By 4.0

- From traditional to decentralized identity
- Portability and Sovereignity
- Verifiable Credentials

12 principles of SSI



Agency

- Representation
- Delegation
- Equity and Inclusion
- Usability, accessibility and consistency

Autonomy

- Participation
- Decentralization
- Interoperability
- Portability

Integrity

- Security
- Verifiability and authenticity
- Privacy and minimal disclosure
- Transparency

Verifiable Credentials

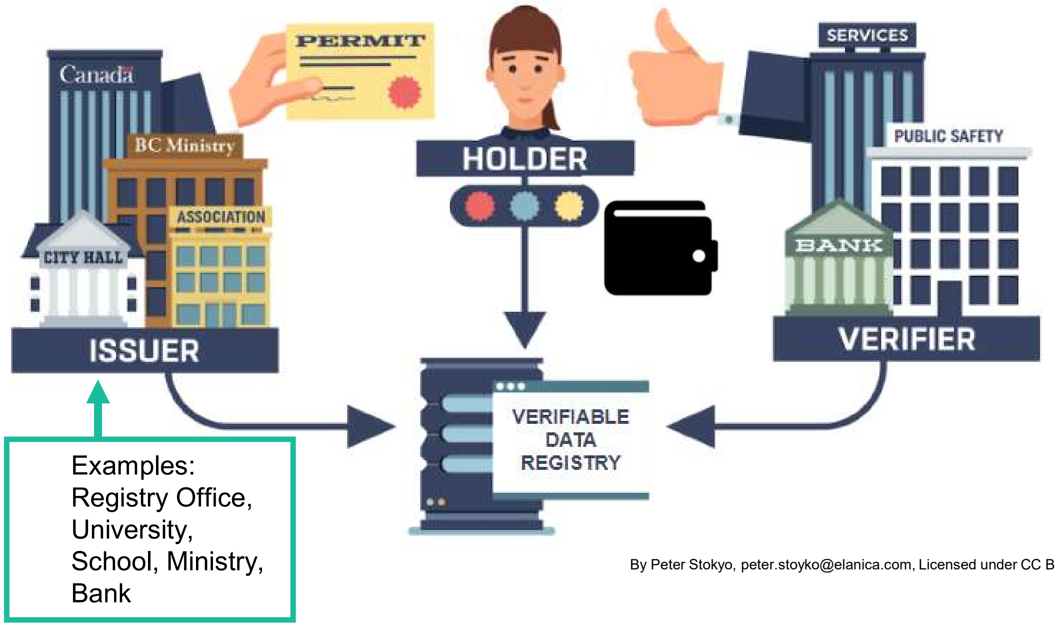
Privacy-Preserving Technology for Credentials

•Used for issuing, storing, and presenting:

- Education degrees
- Government-issued ID cards
- Shipping container manifests
- Certified product information
- Other machine-readable credentials

By Peter Stokyo, peter.stoyko@elanica.com, Licensed under CC By 4.0
https://www.lfdecentralizedtrust.org/blog/2021/04/21/why-distributed-ledger-technology-dlt-for-identity

SSI specifications

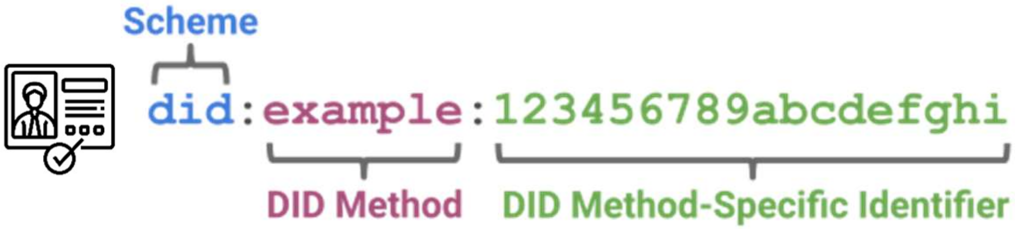


Examples:
Registry Office,
University,
School, Ministry,
Bank

By Peter Stokyo, peter.stoyko@elanica.com, Licensed under CC By 4.0

Verifiable Credentials Data Model by W3C:

- Wallet
- Verifiable Credential (**VC**)
- Verifiable Presentation (**VP**)


Scheme
did:example:123456789abcdefghi
DID Method
DID Method-Specific Identifier

From w3.org DID specification

Decentralized Identifiers:

- URI
- Human-readable
- Distributed Ledgers
  - (Blockchains :-))

SSI implementations

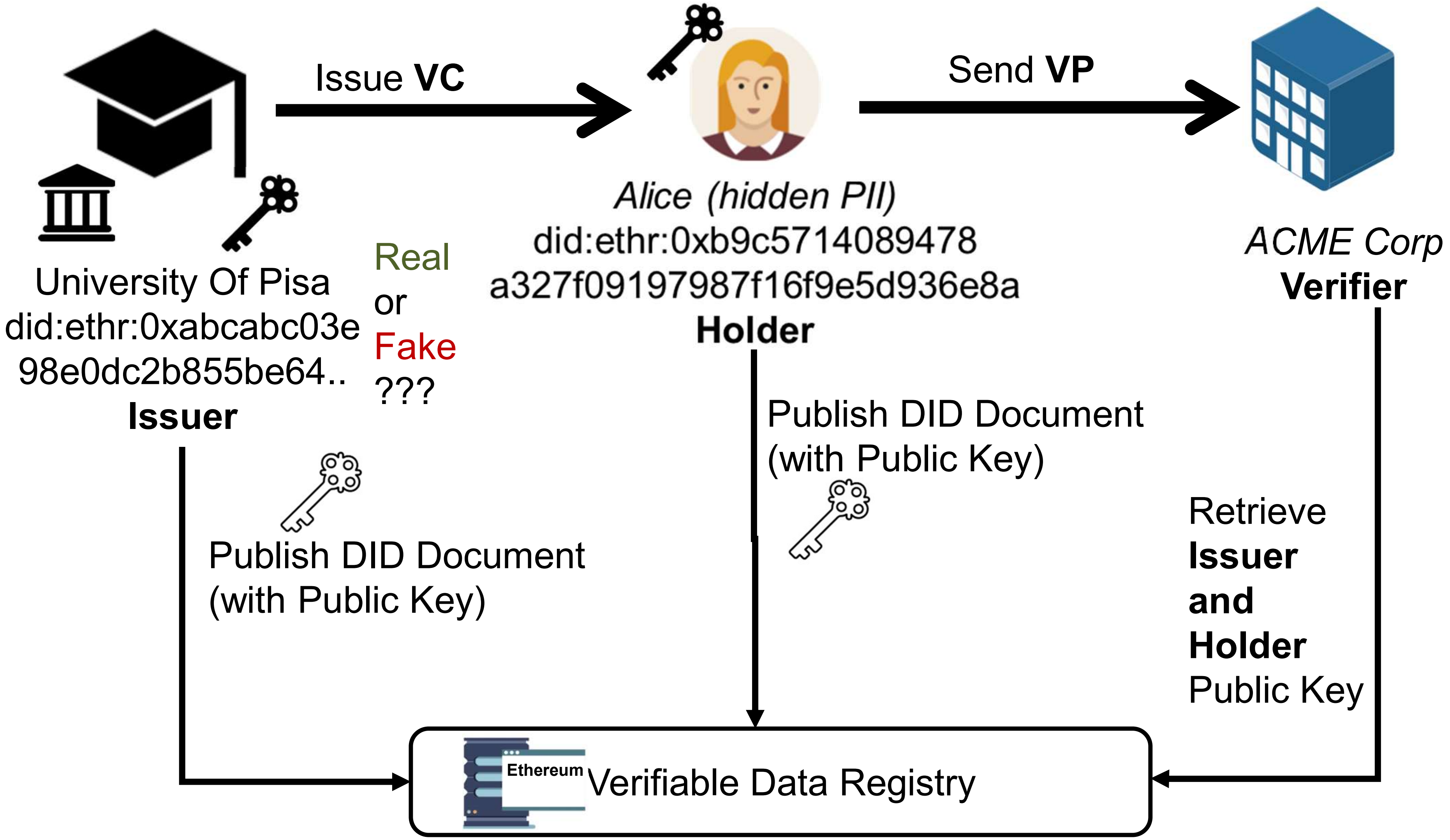
Two major implementations for Verifiable Credential Data Model workflow:

- Veramo
- Hyperledger Indy/Aries

DID methods: 205 listed at diddirectory.com

Use Cases and Trust Issues

Standard Workflow Use Case 1



University Of Pisa
did:ethr:0xabcabc03e
98e0dc2b855be64..
Issuer

Issue **VC**

Real
or
Fake
???

Alice (hidden PII)
did:ethr:0xb9c5714089478
a327f09197987f16f9e5d936e8a
Holder

Send **VP**

ACME Corp
Verifier

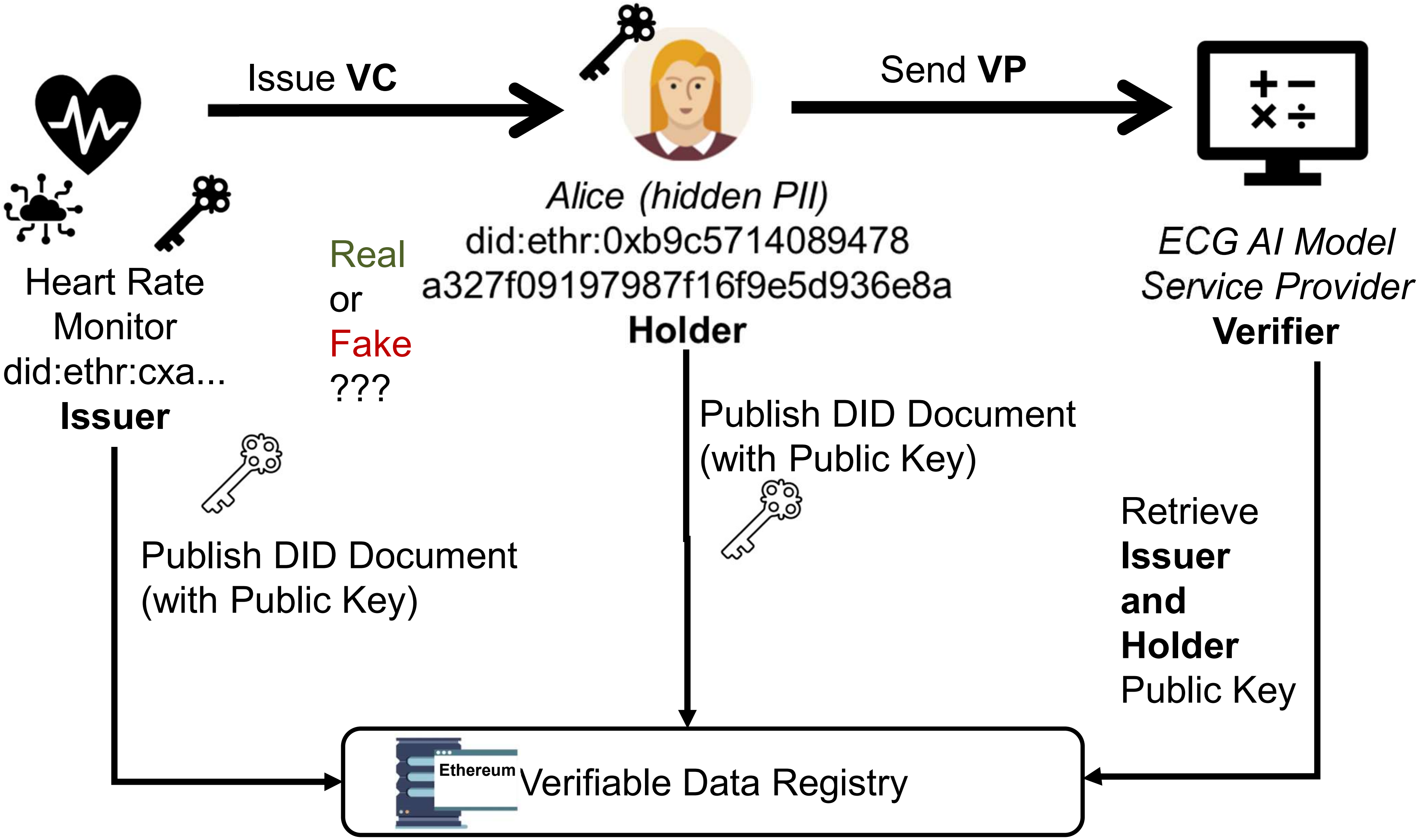
Publish DID Document
(with Public Key)

Publish DID Document
(with Public Key)

Retrieve
Issuer
and
Holder
Public Key

Ethereum
Verifiable Data Registry

Standard Workflow Use Case 2



Issue **VC**

Send **VP**

Heart Rate Monitor
did:ethr:cxa...
Issuer

Real
or
Fake
???

Alice (hidden PII)
did:ethr:0xb9c5714089478
a327f09197987f16f9e5d936e8a
Holder

ECG AI Model Service Provider
Verifier

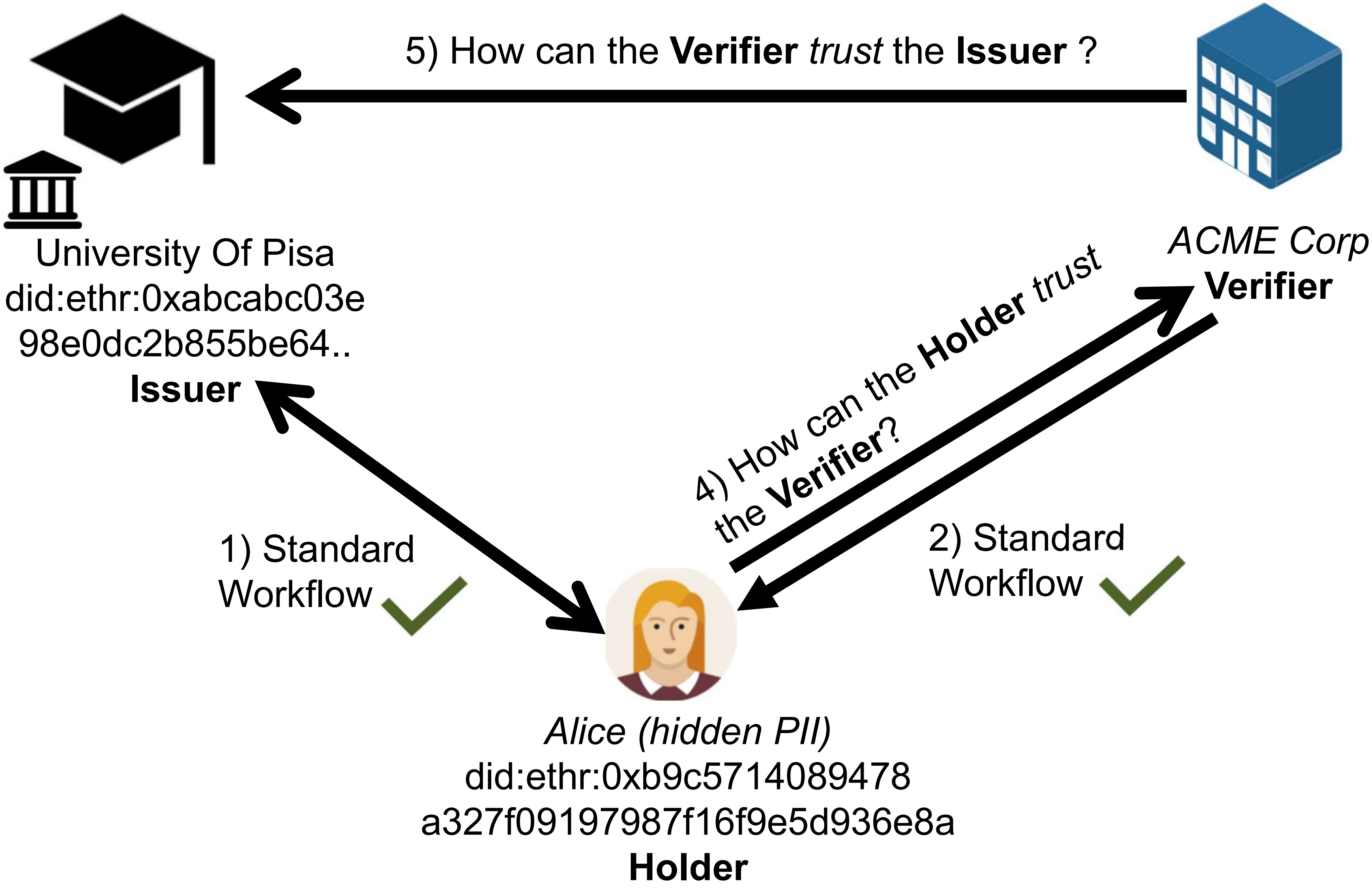
Publish DID Document
(with Public Key)

Publish DID Document
(with Public Key)

Retrieve
Issuer
and
Holder
Public Key

Verifiable Data Registry

What is ‘Trust’ in SSI?



5) How can the **Verifier** *trust* the **Issuer** ?

University Of Pisa
did:ethr:0xabcabc03e
98e0dc2b855be64..
Issuer

ACME Corp
Verifier

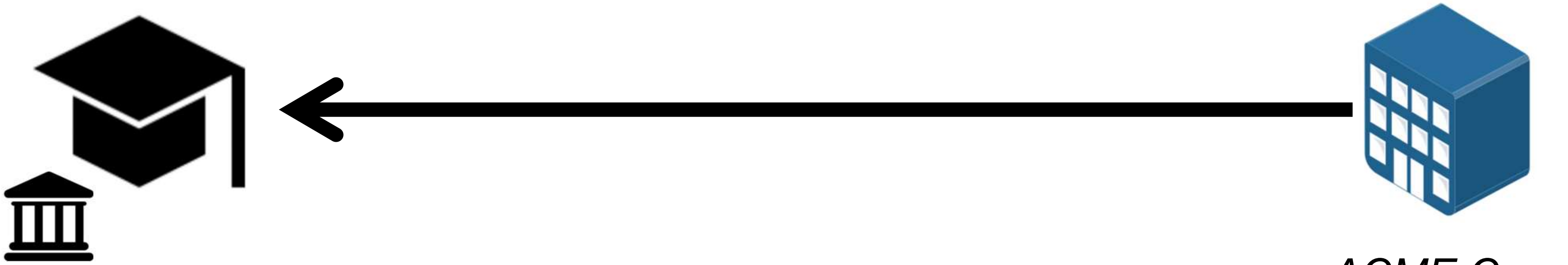
4) How can the **Holder** *trust* the **Verifier**?

1) Standard Workflow ✓

2) Standard Workflow ✓

Alice (hidden PII)
did:ethr:0xb9c5714089478
a327f09197987f16f9e5d936e8a
Holder

How can the Verifier Trust the Issuer ?



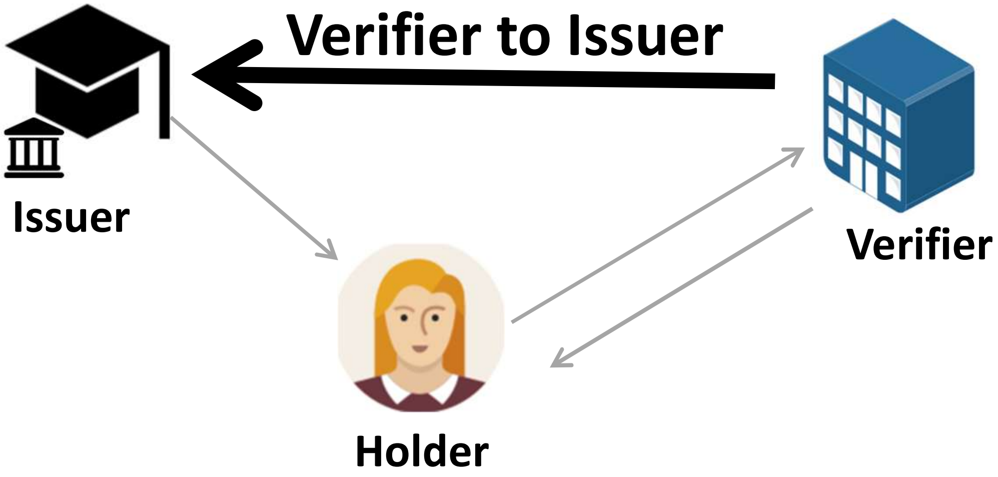
University Of Pisa
did:ethr:0xabcabc03e
98e0dc2b855be64..
Issuer

ACME Corp
Verifier

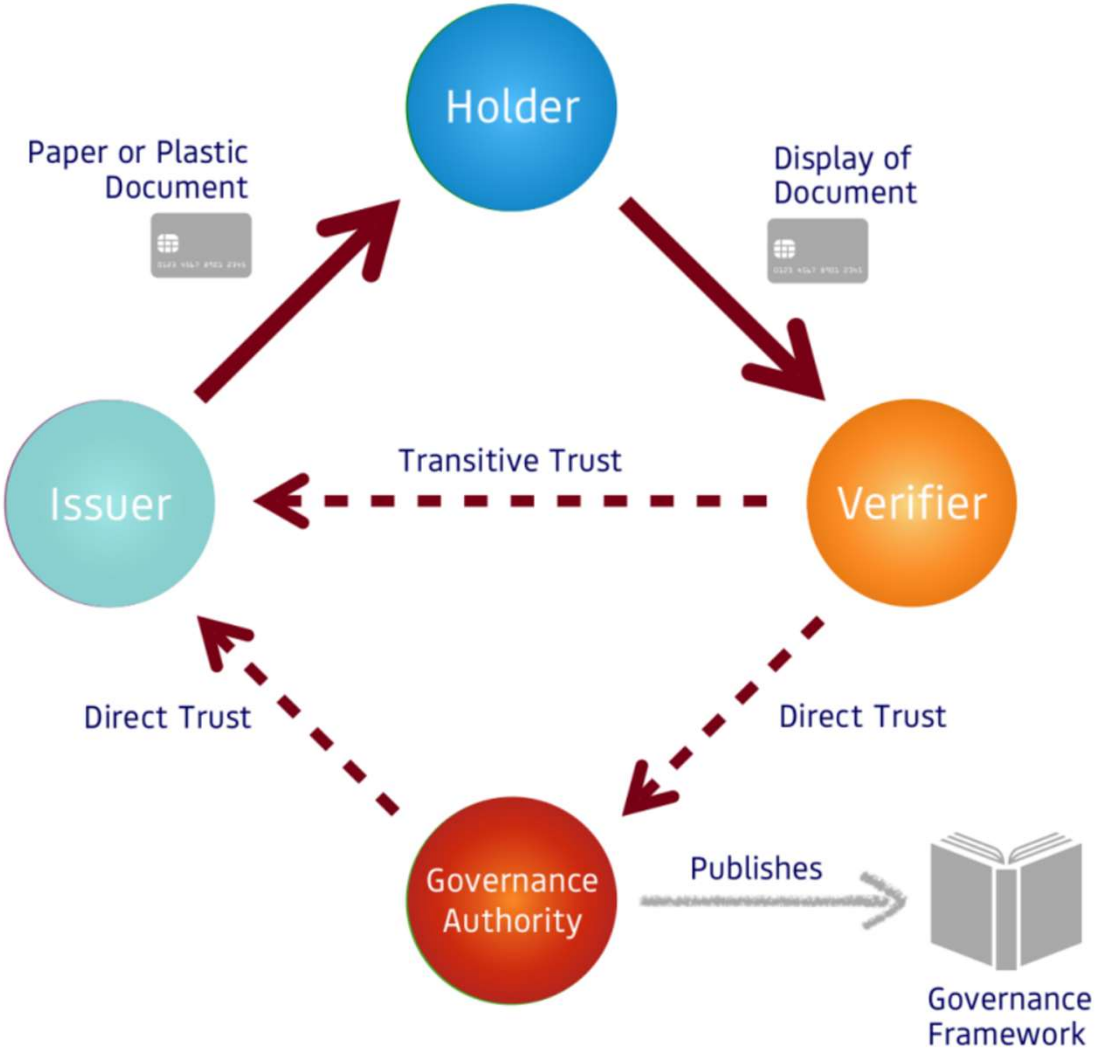
Solutions with different characteristics:

- Root Of Trust Solutions **RoT**
- Decentralized Solutions **DecS**
- Credential Based Solutions **CredBas**

Trust Issues and Measurement



Governance Framework Trust – Trust Diamond RoT

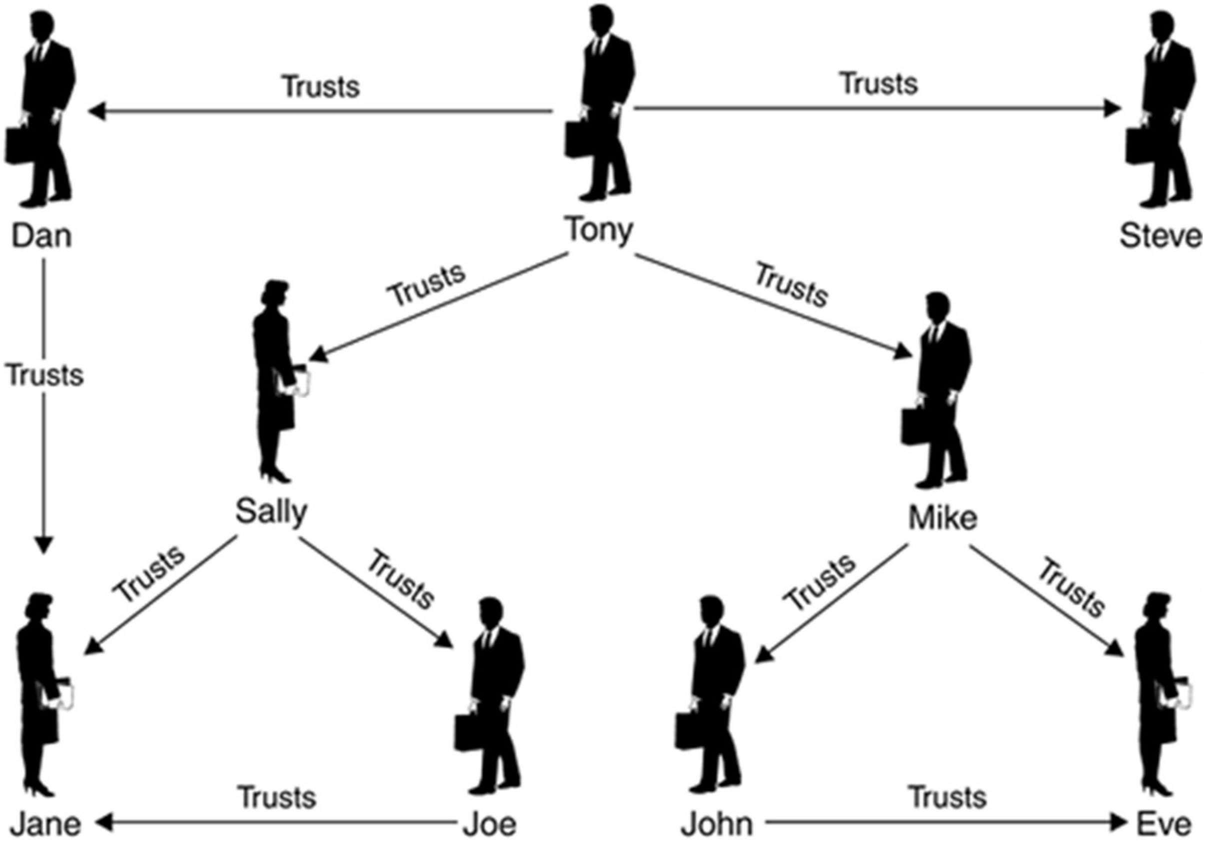


- Domain Specific
- Trust Registry
- Centralized according to Governance Framework

Social Networks and Web Of Trust **DecS**

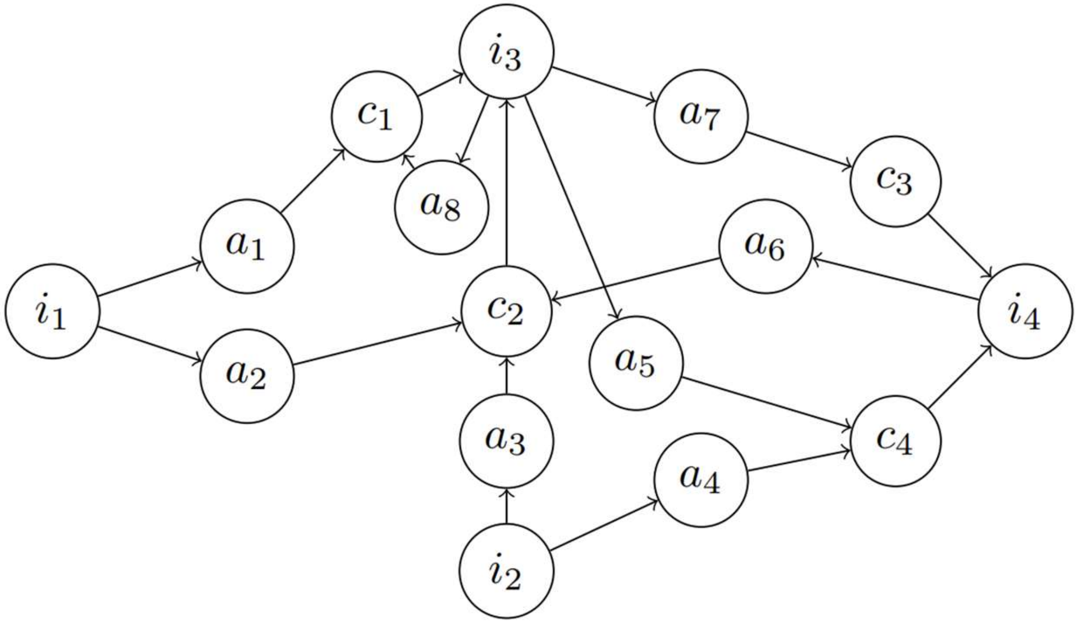
- No Governance Framework
- Based on Web Of Trust from Pretty Good Privacy (PGP)

Web of Trust Model

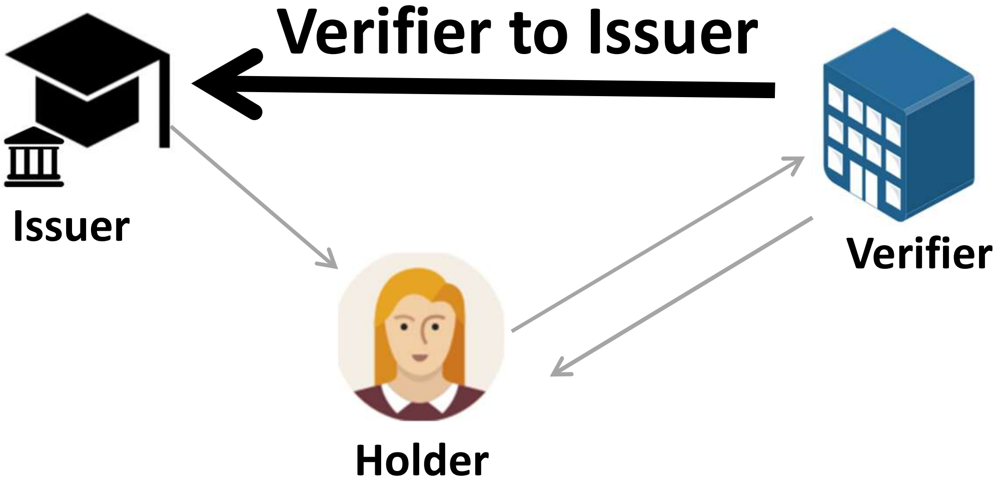


Credential-Based Quantifiable Trust **CredBas**

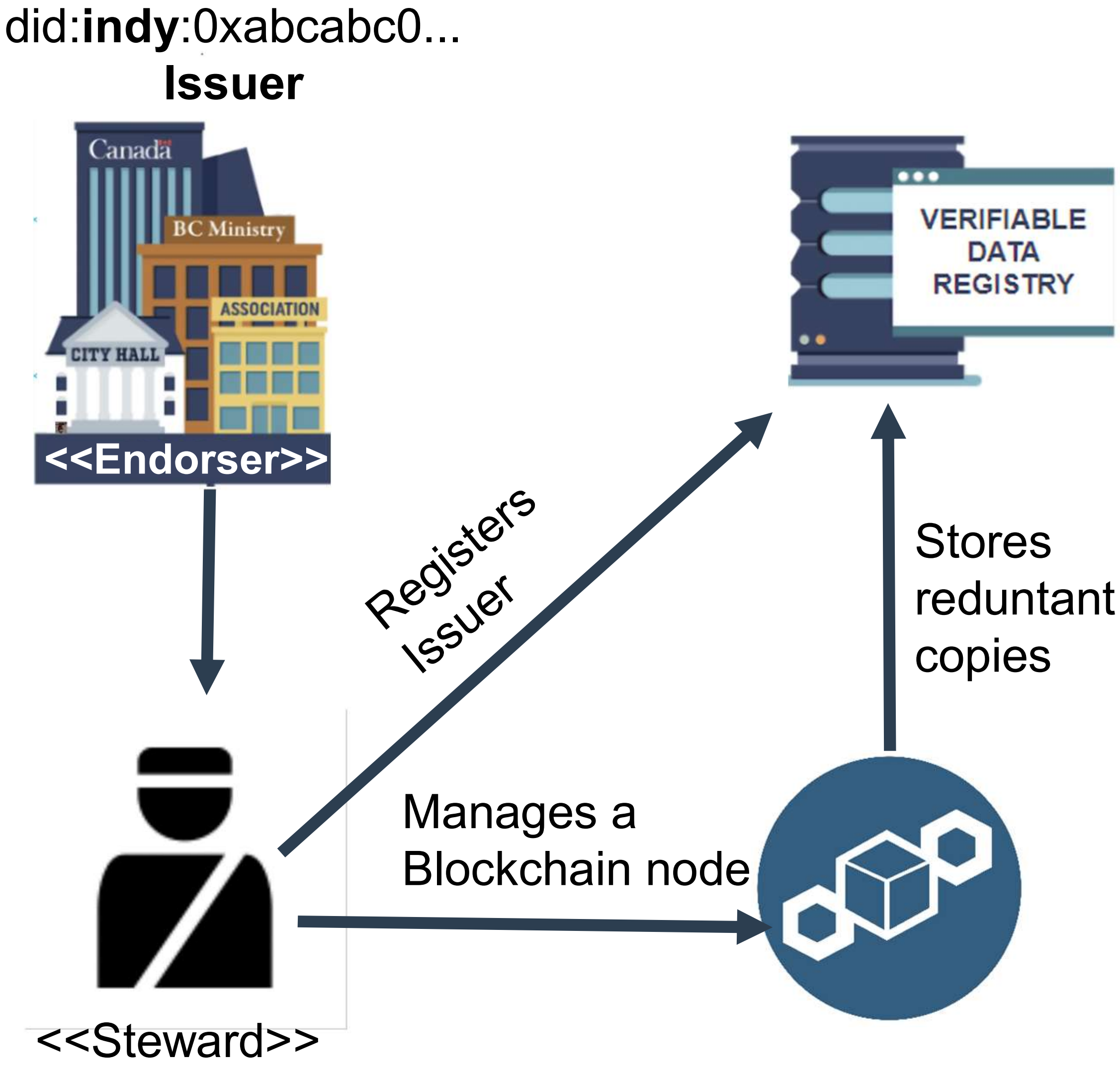
- a_i: attestations (proofs)
- c_j: claims (VCs)
- i_k: identity
- Each identity has an initial list of trusted identities with a score



Trust Frameworks



Centralized Governance **RoT**



did:**indy**:0xabcabc0...

Issuer

<<Endorser>>

Registers Issuer

Stores reduntant copies

Manages a Blockchain node

<<Steward>>

sovrin

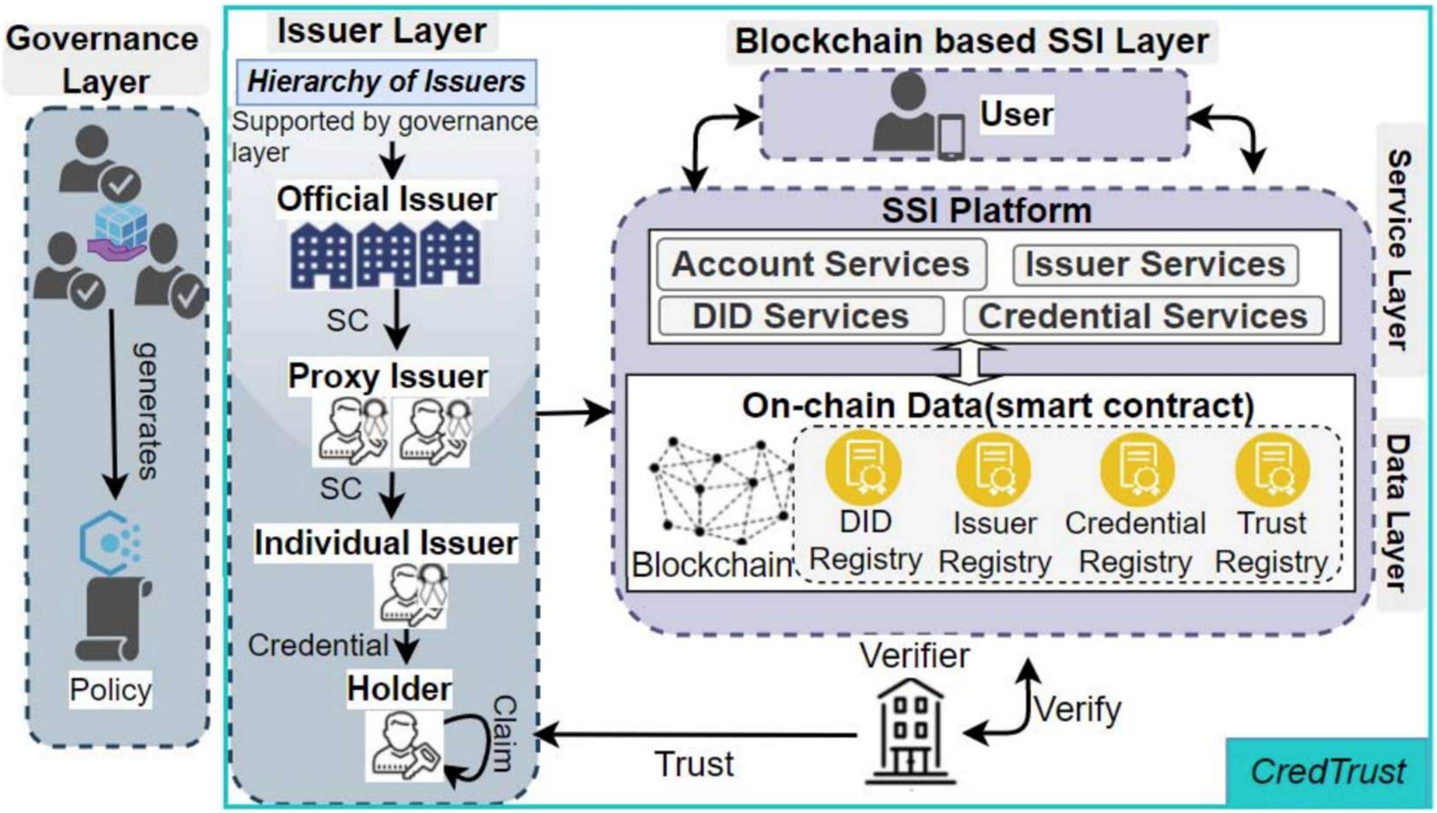
identity for all

- **Sovrin Governance Framework**, requires a Legal Entity Identifier
- Charges a Fee to register DID
- Blockchain is public **permissioned**
- Vendor Lock in

https://sovrin.org/mainnet-endorser-did-application-form/

Credential-based Trust Framework: CredTrust I

RoT + CredBas

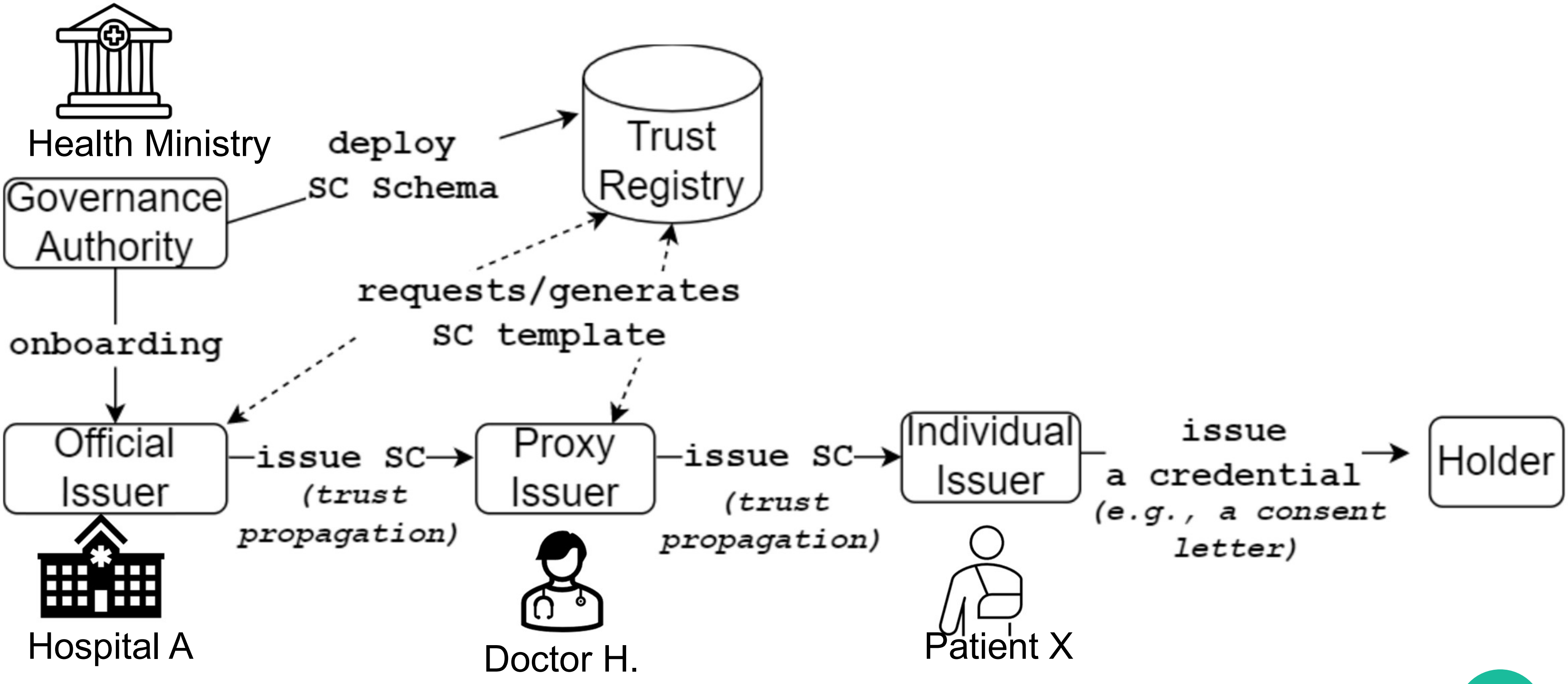


R. Mukta et al. "CredTrust: Credential Based Issuer Management for Trust in Self-Sovereign Identity."
doi: 10.1109/Blockchain55522.2022.00053

Credential-based Trust Framework: CredTrust II

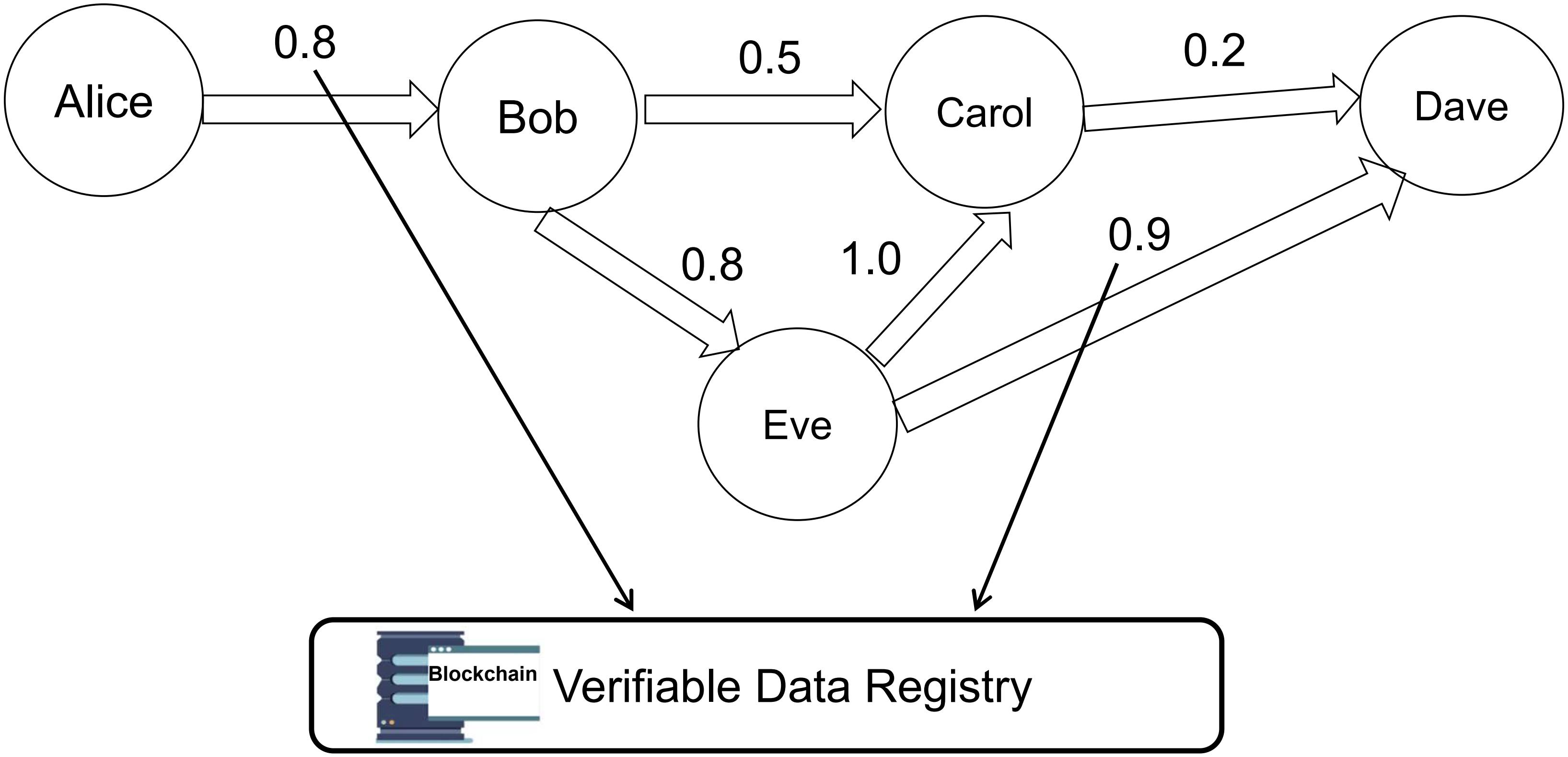
RoT + CredBas

Supporting Credential (SC): specifies the delegated capabilities to an Issuer

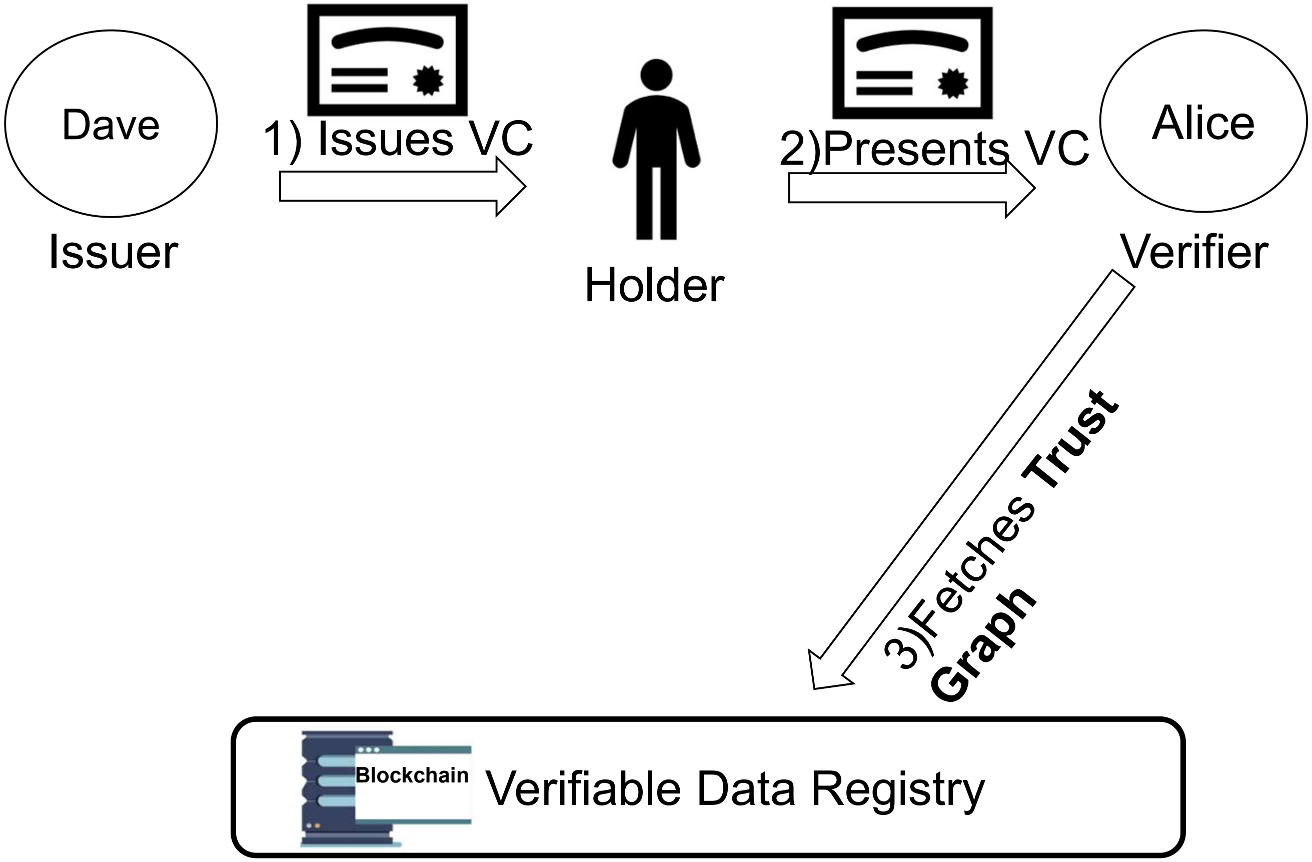


Trust Relationships on Blockchain I DecS

Trust Scores between entities published on Blockchain



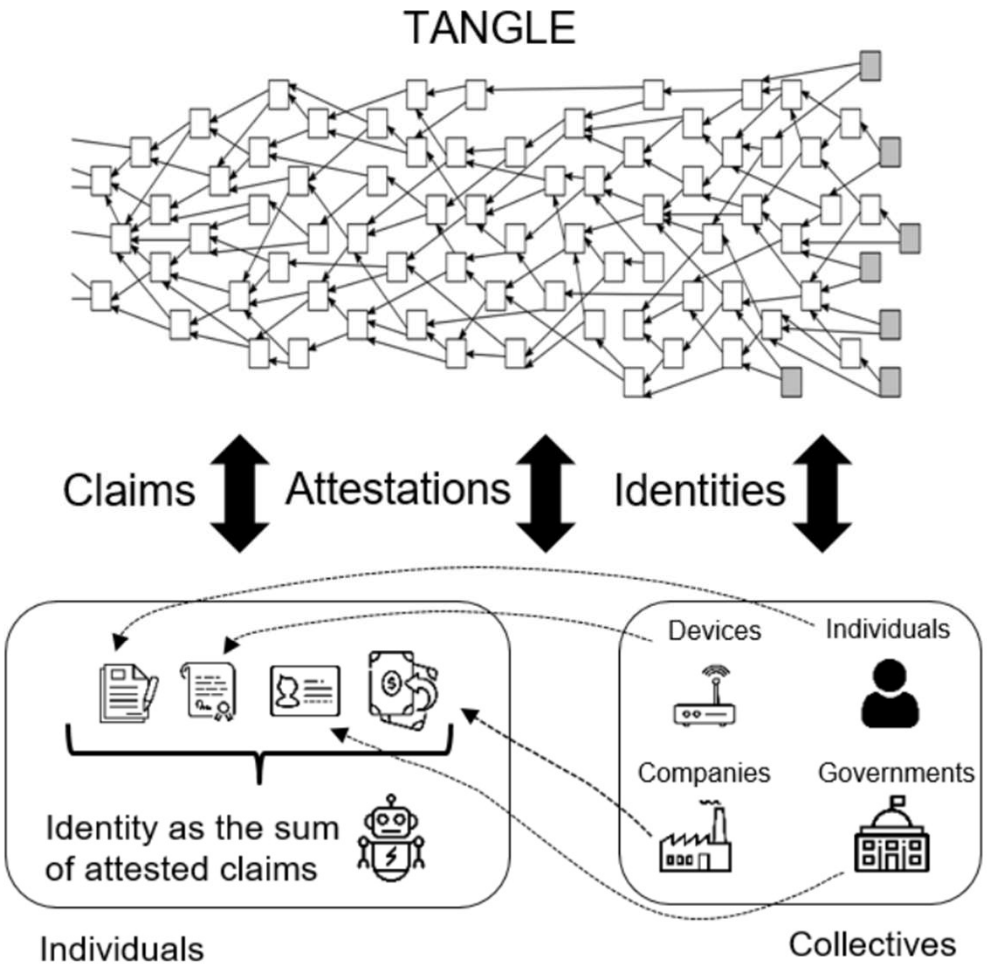
Trust Relationships on Blockchain II **DecS**

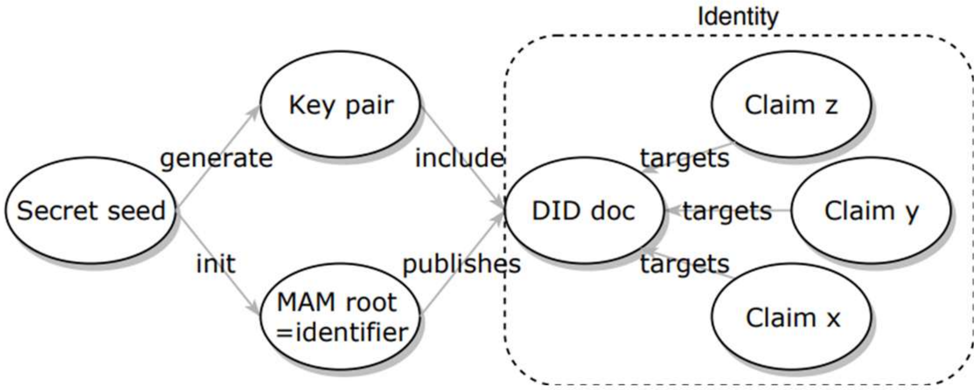


- Calculate VC Trust Score based on:
  - Edges weight
  - Vertex distance
- Fits well on Online Social Networks

A. De Salve et al."A Multi-Layer Trust Framework for Self-Sovereign Identity on Blockchain." *Online Social Networks and Media*, Volumes 37–38, 2023, Article 100265, ISSN 2468-6964. Available at: https://doi.org/10.1016/j.osnem.2023.100265

IoT and Web Of Trust **CredBas**





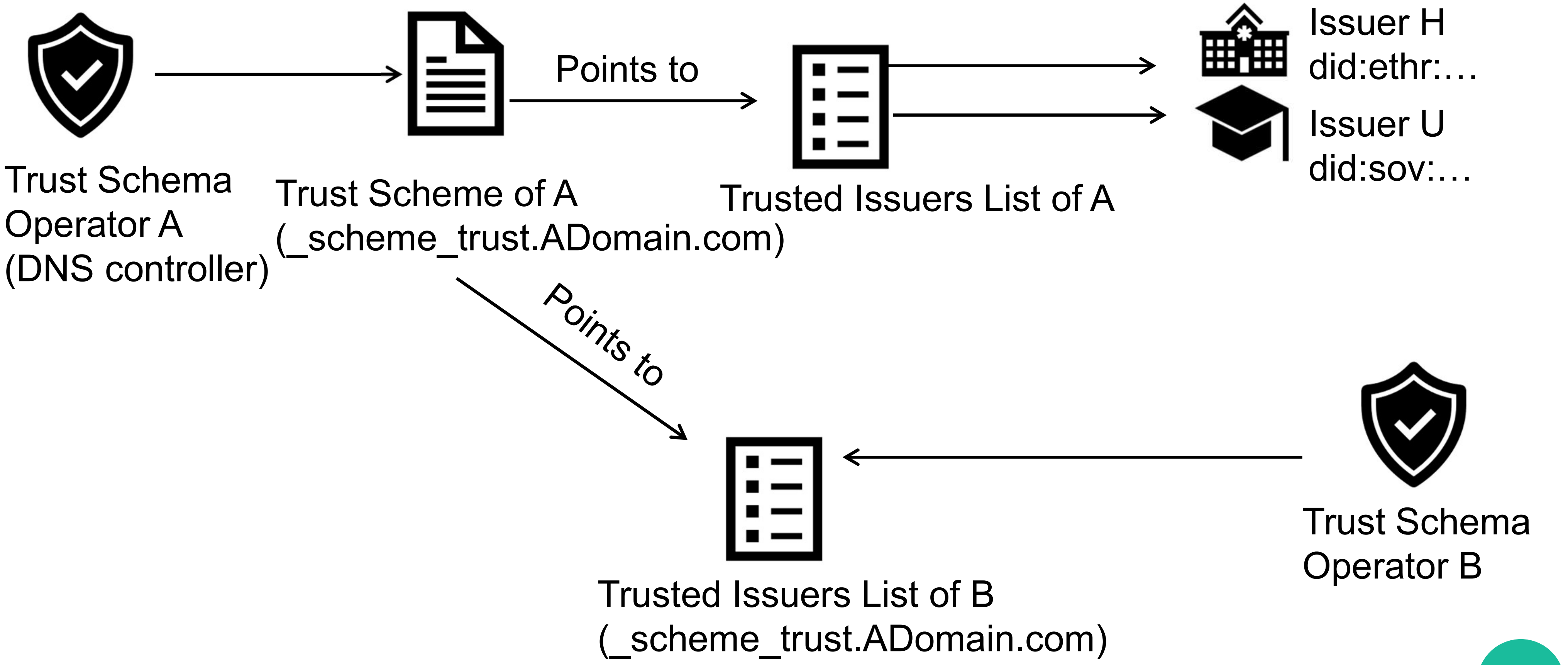
A.Grüner et al. "A Quantifiable Trust Model for Blockchain-Based Identity Management
doi: 10.1109/Cybermatics_2018.2018.00250

TRust mAnagement INfrastructure (TRAIN)

RoT

Johnson Jeyakumar et al ," A novel approach to establish trust in verifiable credential issuers in Self-sovereign identity ecosystems using TRAIN
doi: 10.18420/OID2022_02

TRAIN



Trust Schema Operator A (DNS controller)

Trust Scheme of A (_scheme_trust.ADomain.com)

Points to

Trusted Issuers List of A

Issuer H
did:ethr:…

Issuer U
did:sov:…

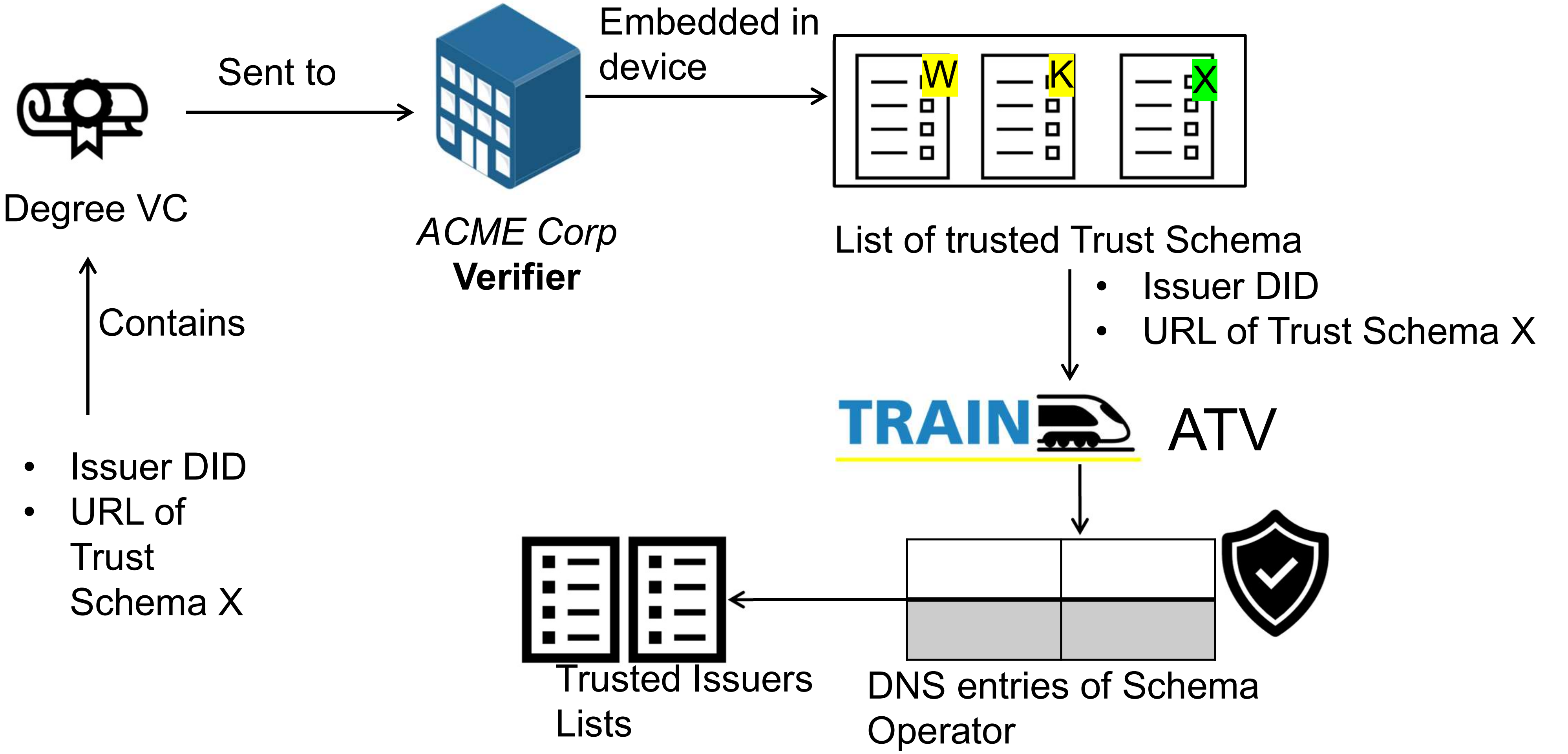
Points to

Trusted Issuers List of B (_scheme_trust.ADomain.com)

Trust Schema Operator B

TRAIN Automatic Trust Verifier (ATV)

RoT



Sent to

Embedded in device

Degree VC

ACME Corp
Verifier

List of trusted Trust Schema

- Issuer DID
- URL of Trust Schema X

Contains

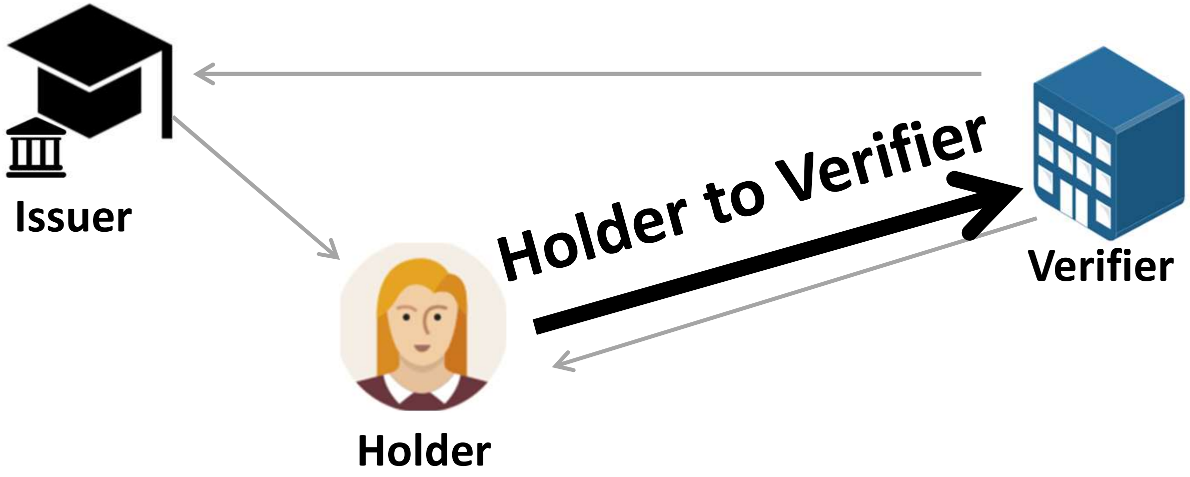
- Issuer DID
- URL of Trust Schema X

ATV

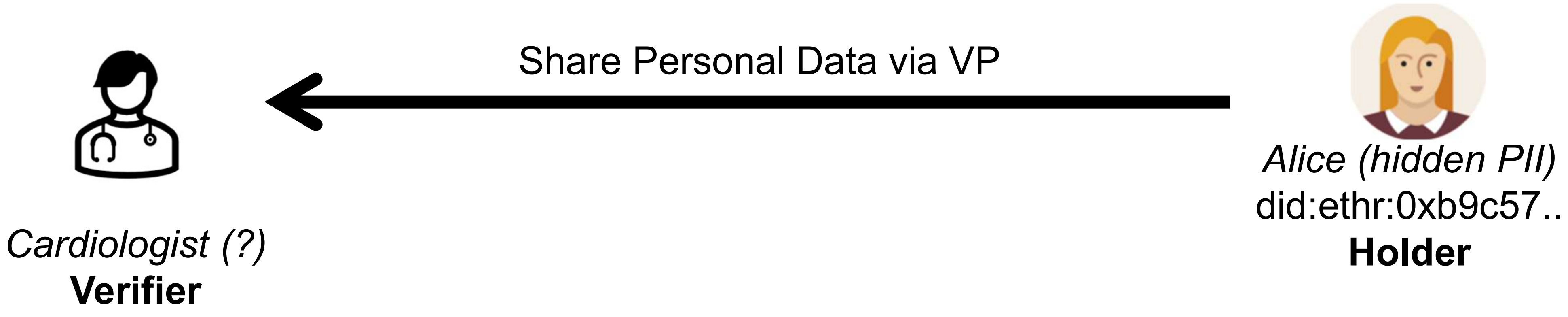
Trusted Issuers Lists

DNS entries of Schema Operator

Access Control to VC



How can the Holder Trust the Verifier ?



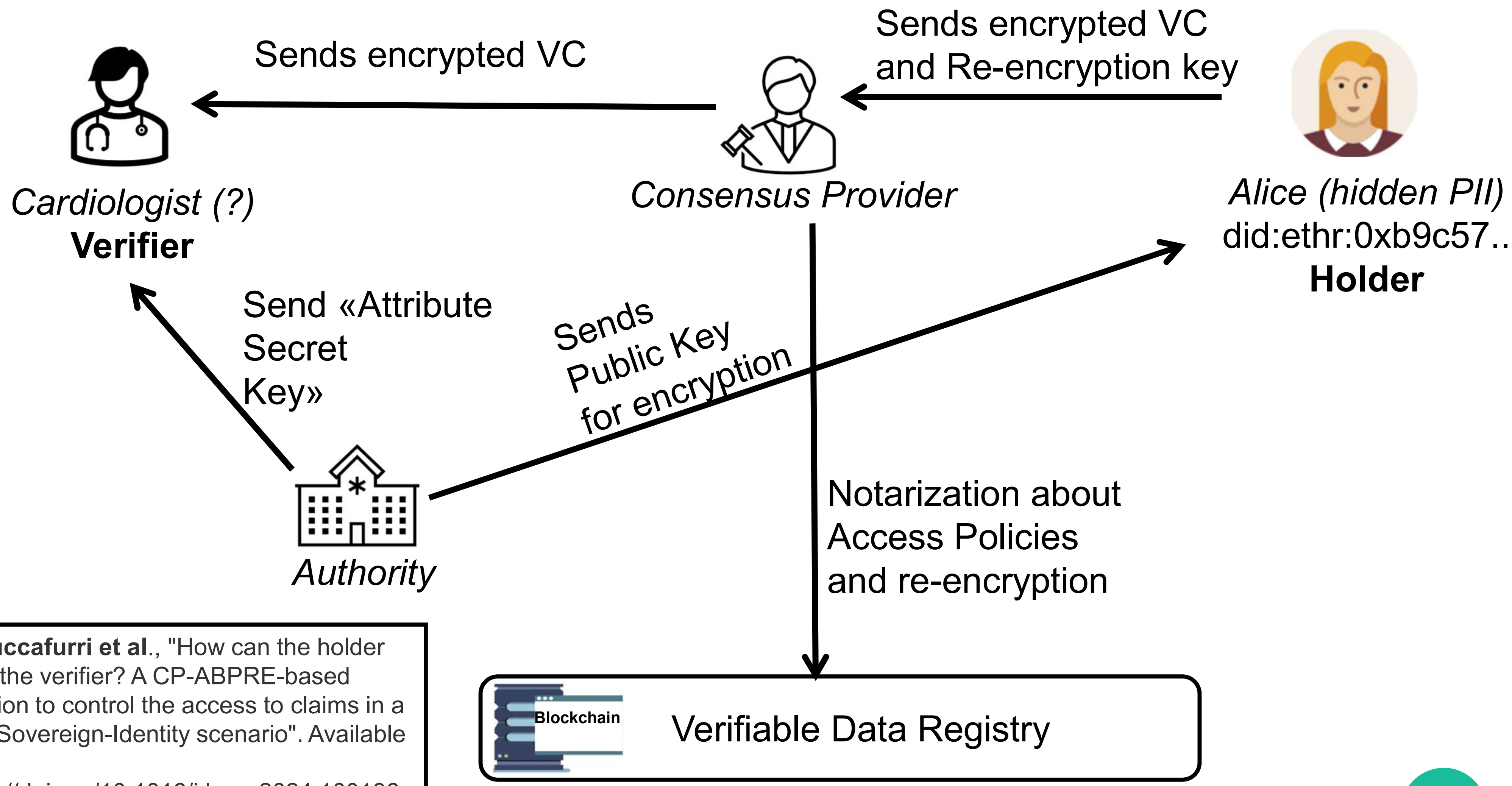
Share Personal Data via VP

Cardiologist (?)
Verifier

Alice (hidden PII)
did:ethr:0xb9c57..
Holder

- Same solutions as before with Holder in the place of Verifier
- Capabilities Access Control
  - CipherPolicy Attribute-Based Proxy Re-Encryption
  - ReEncryption to change Access Policies

Attribute-Based-Access Control to VCs



Sends encrypted VC

Sends encrypted VC and Re-encryption key

Cardiologist (?)
Verifier

Consensus Provider

Alice (hidden PII)
did:ethr:0xb9c57..
Holder

Send «Attribute Secret Key»

Sends Public Key for encryption

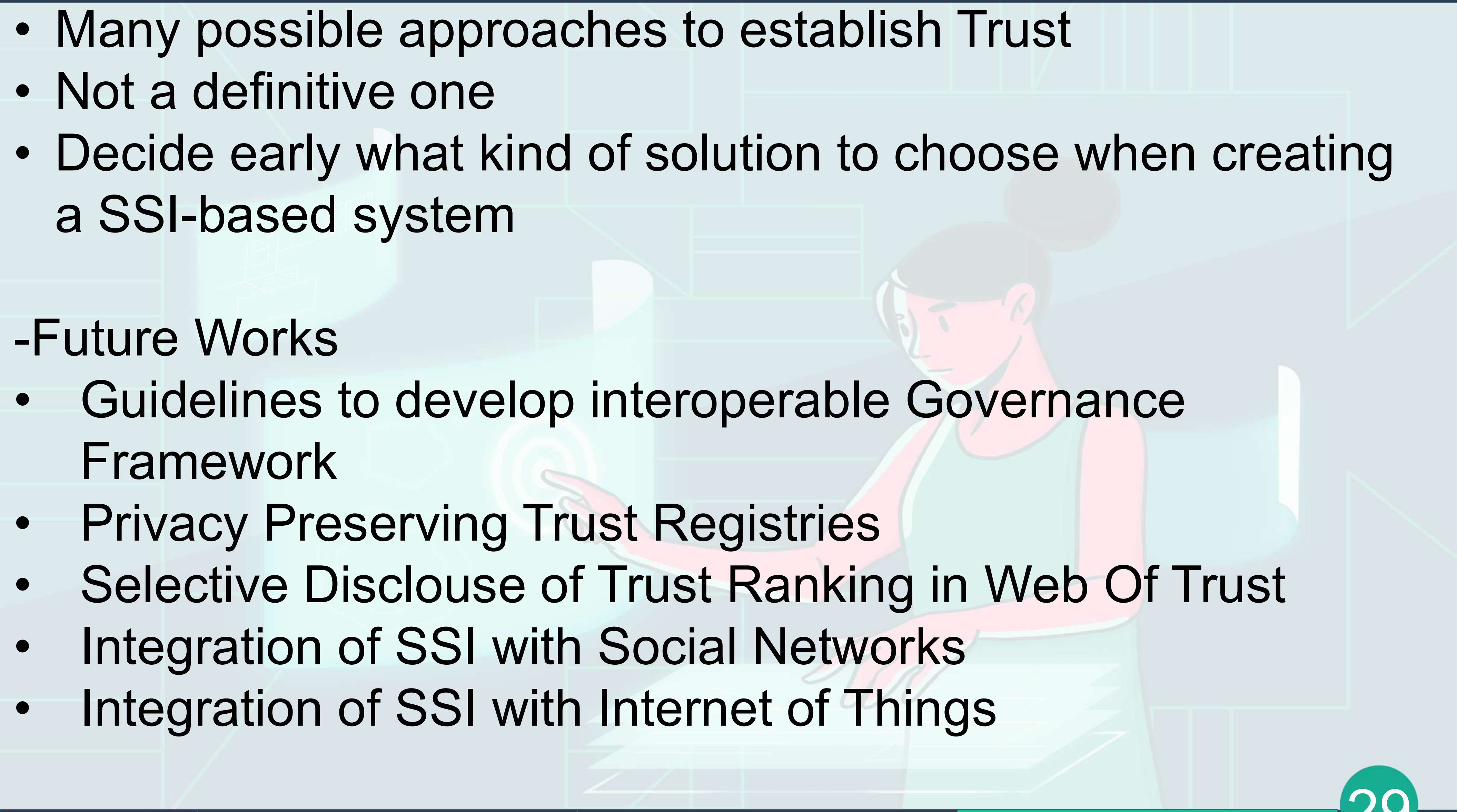
Authority

Notarization about Access Policies and re-encryption

Verifiable Data Registry

F. Buccafurri et al., "How can the holder trust the verifier? A CP-ABPRE-based solution to control the access to claims in a Self-Sovereign-Identity scenario". Available at: https://doi.org/10.1016/j.bcra.2024.100196.

Conclusions and Future Works



- Many possible approaches to establish Trust
- Not a definitive one
- Decide early what kind of solution to choose when creating a SSI-based system

-Future Works

- Guidelines to develop interoperable Governance Framework
- Privacy Preserving Trust Registries
- Selective Disclouse of Trust Ranking in Web Of Trust
- Integration of SSI with Social Networks
- Integration of SSI with Internet of Things

References

W3C-VC (2021): "Verifiable Credentials Data Model 1.1." W3C Technical Report. Available at: https://www.w3.org/TR/vc-data-model.

W3C-DID (2021): "Decentralized Identifiers (DIDs) v1.0." W3C Technical Report. Available at: https://www.w3.org/TR/did-core.

Trust Over IP Foundation: “Introduction to Trust Over IP” whitepaper available at : https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf

N. Naik et al., "Does Sovrin Network Offer Sovereign Identity?," 2021 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 2021, pp. 1-6, doi: 10.1109/ISSE51541.2021.9582472.

A. De Salve, A. Lisi, P. Mori, L. Ricci, and C. Turco, "Self-Sovereign Identity for Privacy-Preserving Shipping Verification System," in Proceedings of the 2022 5th International Conference on Blockchain Technology and Applications (ICBTA '22), Association for Computing Machinery, New York, NY, USA, 2023, pp. 147–157. https://doi.org/10.1145/3581971.3581992.

A. De Salve et al."A Multi-Layer Trust Framework for Self-Sovereign Identity on Blockchain." *Online Social Networks and Media*, Volumes 37–38, 2023, Article 100265, ISSN 2468-6964. Available at: https://doi.org/10.1016/j.osnem.2023.100265

R. Mukta et al. "CredTrust: Credential Based Issuer Management for Trust in Self-Sovereign Identity." 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, Finland, 2022, pp. 334-339. doi: 10.1109/Blockchain55522.2022.00053

A. Grüner et al. "A Quantifiable Trust Model for Blockchain-Based Identity Management," *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Halifax, NS, Canada, 2018, pp. 1475-1482, doi: 10.1109/Cybermatics_2018.2018.00250. .

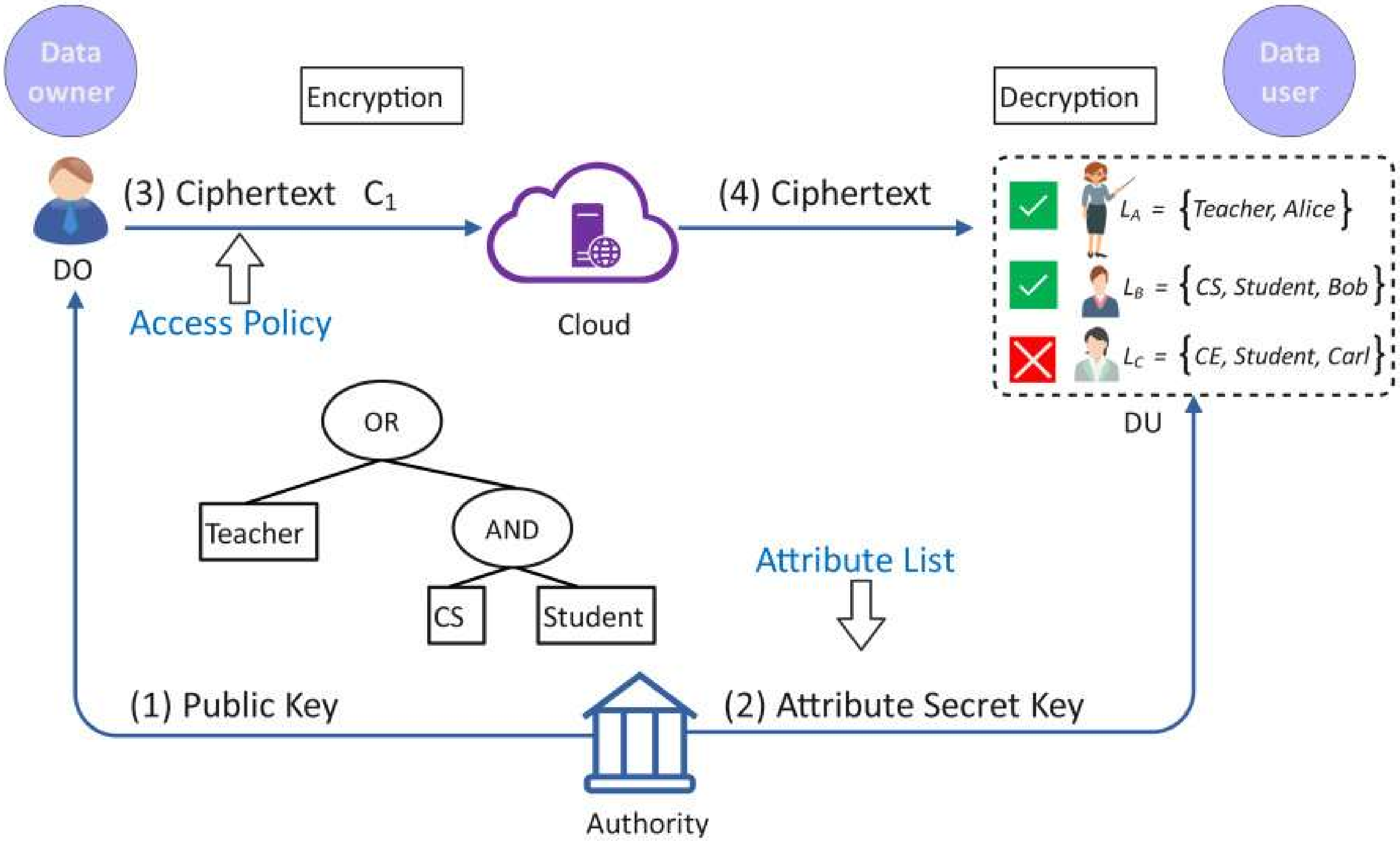
Johnson Jeyakumar et al ," A novel approach to establish trust in verifiable credential issuers in Self-sovereign identity ecosystems using TRAIN ," , Open Identity Summit 2022. DOI: 10.18420/OID2022_02. Bonn: Gesellschaft für Informatik e.V.. PISSN: 1617-5468. ISBN: 978-3-88579-719-7. pp. 27-38. Regular Research Papers. Copenhagen, Denmark. 07.-08. July 2022

F. Buccafurri et al., "How can the holder trust the verifier? A CP-ABPRE-based solution to control the access to claims in a Self-Sovereign-Identity scenario," Blockchain: Research and Applications, Volume 5, Issue 3, 2024, Article 100196, ISSN 2096-7209. Available at: https://doi.org/10.1016/j.bcra.2024.100196.

Thank you

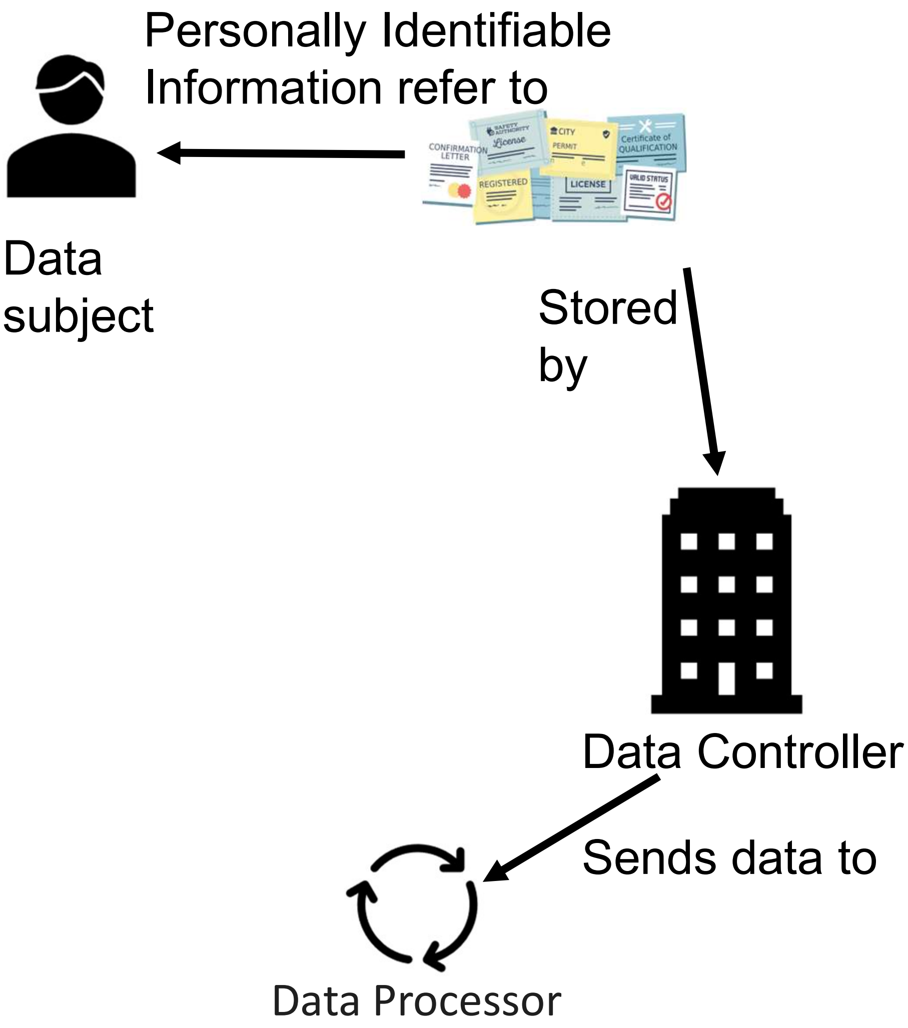
Any question?

Appendix 1


Data owner
Encryption
Decryption
Data user
DO
(3) Ciphertext C₁
Access Policy
Cloud
(4) Ciphertext
✓ L_A = {Teacher, Alice}
✓ L_B = {CS, Student, Bob}
✗ L_C = {CE, Student, Carl}
DU
OR
Teacher
AND
CS
Student
Attribute List
(1) Public Key
(2) Attribute Secret Key
Authority

GDPR, Identity and Sovereignty

Traditional Digital Identity



Personally Identifiable Information refer to

Data subject

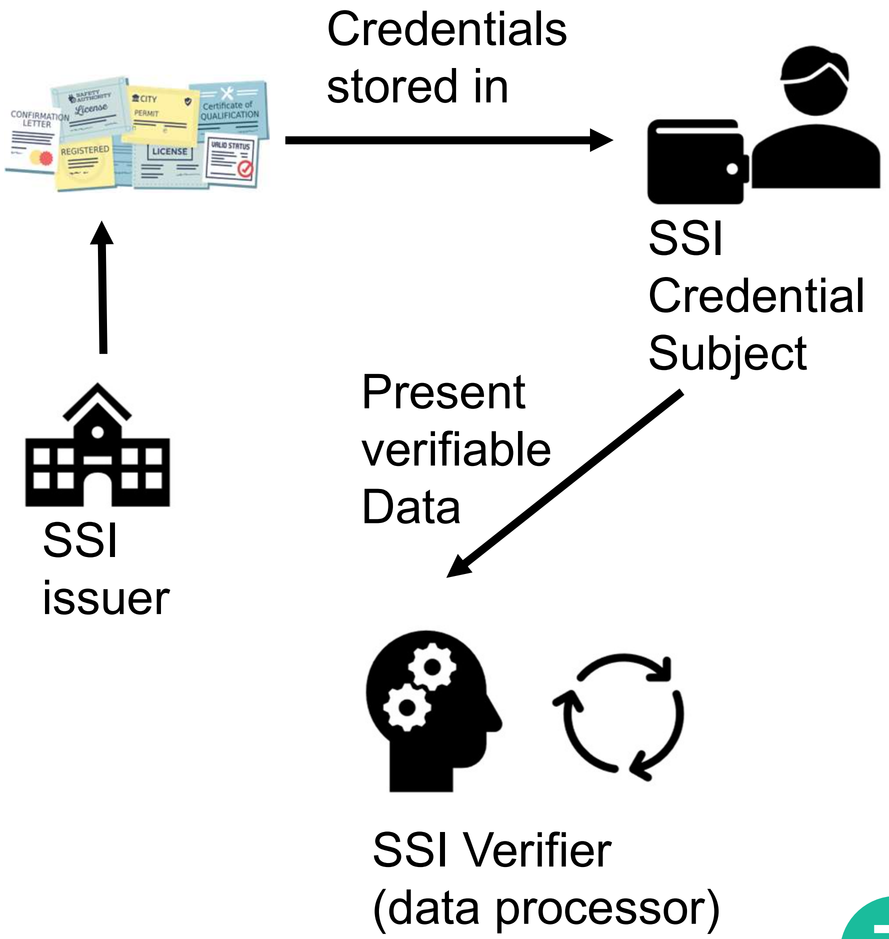
Stored by

Data Controller

Sends data to

Data Processor

Self Sovereign Identity



Credentials stored in

SSI Credential Subject

SSI issuer

Present verifiable Data

SSI Verifier (data processor)