Formalising Linked-Data based Verifiable Credentials for Selective Disclosure

Dan Yamamoto (Internet Initiative Japan Inc.)

Yuji Suga (Internet Initiative Japan Inc.)

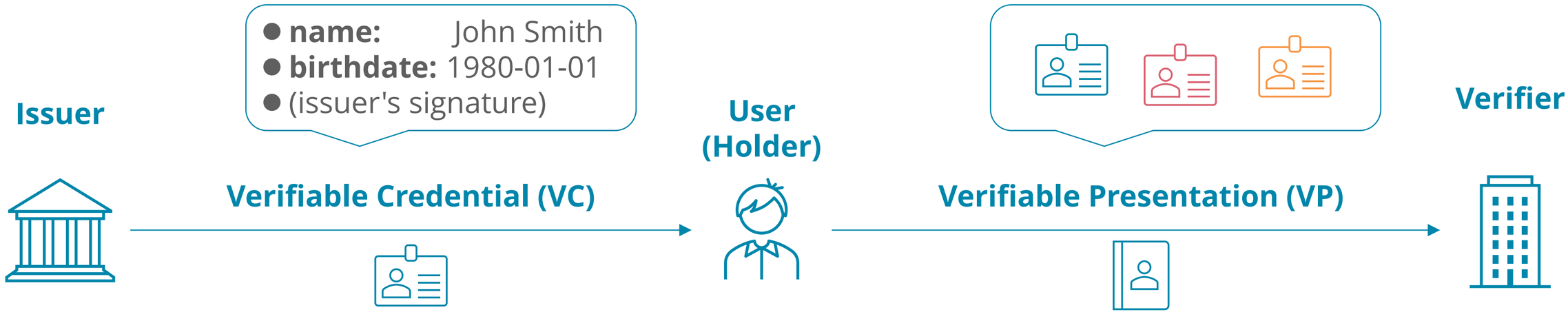
Kazue Sako (Waseda University)

June 6, 2022

Security Standardisation Research conference (SSR 2022) @ Genoa

Verifiable Credentials

- **W3C Recommendation**: Verifiable Credentials Data Model (v1.1, March 2022)
- provides a mechanism to express digital credentials in a way that is **cryptographically secure**, **privacy respecting**, and **machine-verifiable**



- Examples: **SMART Health Cards** / IATA Travel Pass / Azure Active Directory Verifiable Credentials (in public preview)

SMART Health Cards

- Paper or digital versions of clinical information
- developed and standardized by VCI (Vaccination Credential Initiative)
- used in 15 nations: US, UK, Canada, Japan, ...

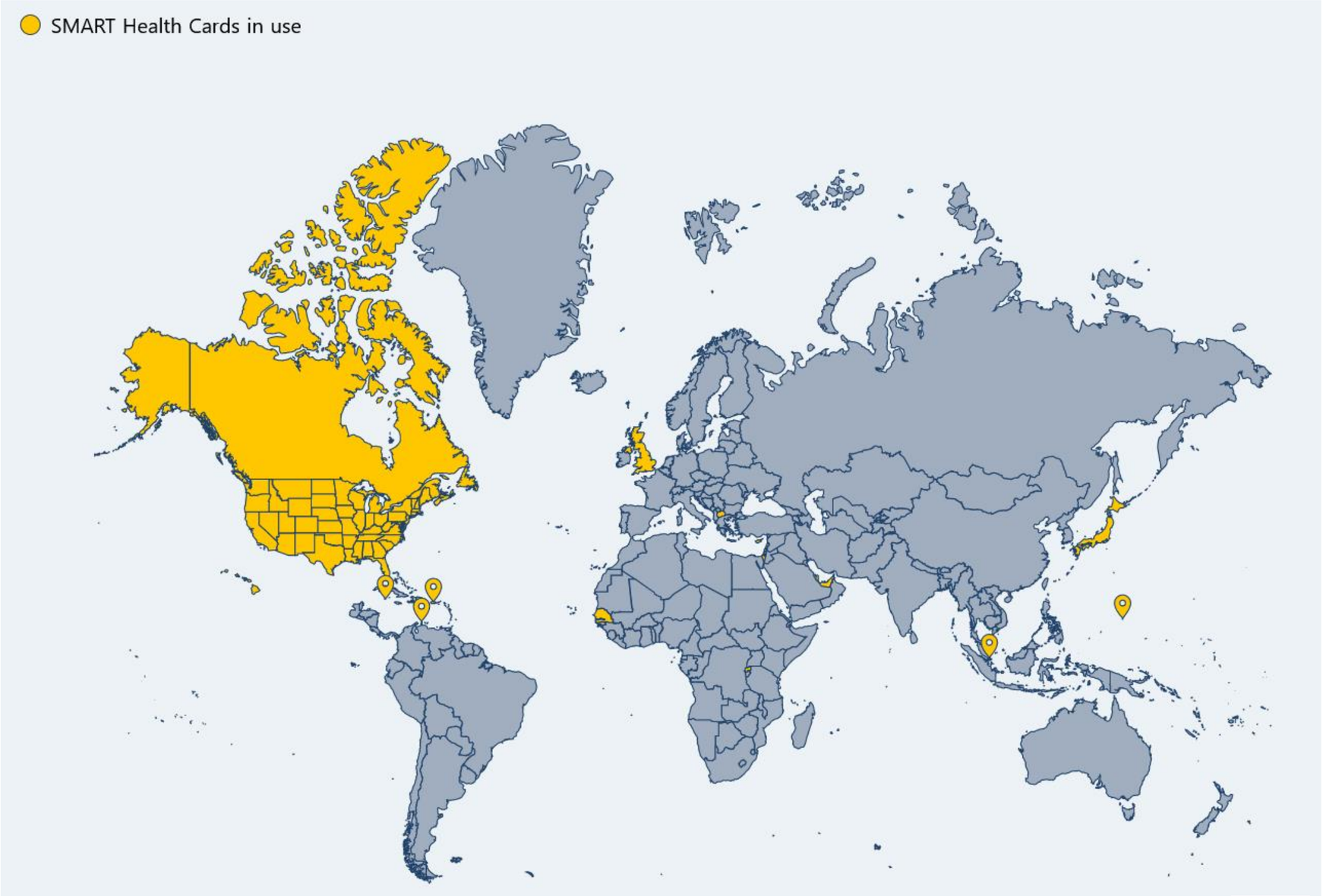
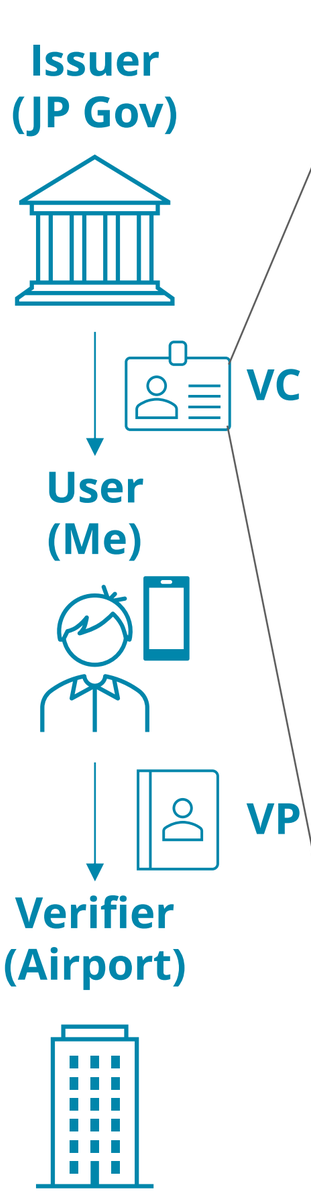


image: https://vci.org

SMART Health Cards



JWT

Header

```
{ "iss": "https://vc.vrs.digital.go.jp/issuer",
  "nbf": 1648956149.461584,  // ~= 2022-04-03
  "vc": {
    "type": ["https://smarthealth.cards#health-card",...],
    "credentialSubject": {
      "fhirVersion": "4.0.1",
      "fhirBundle": { ...,
        "entry": [
          { "fullUrl": "resource:0",
            "resource": {
              "resourceType": "Patient",
              "name": [ ... , {
                  "use": "official",
                  "given": [ "DAN" ], "family": "YAMAMOTO",
                }],
              "birthDate": "xxxx-xx-xx"
            } },
          { "fullUrl": "resource:1",
            "resource": {
              "resourceType": "Immunization",
              "status": "completed",
              "occurrenceDateTime": "2021-08-10",
              "vaccineCode": { "coding": [ {
                    "system": "http://hl7.org/fhir/sid/cvx",
                    "code": "207"
                  } ] },
              "patient": { "reference": "resource:0" },
              "lotNumber": "9999999" ...
```

Signature

SMART Health Cards

Issuer (JP Gov)

VC

User (Me)

VP

Verifier (Airport)

JWT

Header

```
{ "iss": "https://vc.vrs.digital.go.jp/issuer",
  "nbf": 1648956149.461584,  // ~= 2022-04-03
  "vc": {
                    "given": [ "DAN" ], "family": "YAMAMOTO",
                  }],
                "birthDate": "1980-05-03"
              } },
            { "fullUrl": "resource:1",
              "resource": {
                "resourceType": "Immunization",
                "status": "completed",
                "occurrenceDateTime": "2021-08-10",
                "vaccineCode": { "coding": [ {
                      "system": "http://hl7.org/fhir/sid/cvx",
                      "code": "207"
                    } ] },
                "patient": { "reference": "resource:0" },
                "lotNumber": "9999999" ...
```

- ✓ issued by: **Japanese Government**
- ✓ issued on: **April 3, 2022**
- ✓ patient name: **Dan Yamamoto**
- ✓ got vaccinated on: **August 10, 2021**
- ✓ vaccine code: **207**
- ✓ lot number: **9999999**

Signature

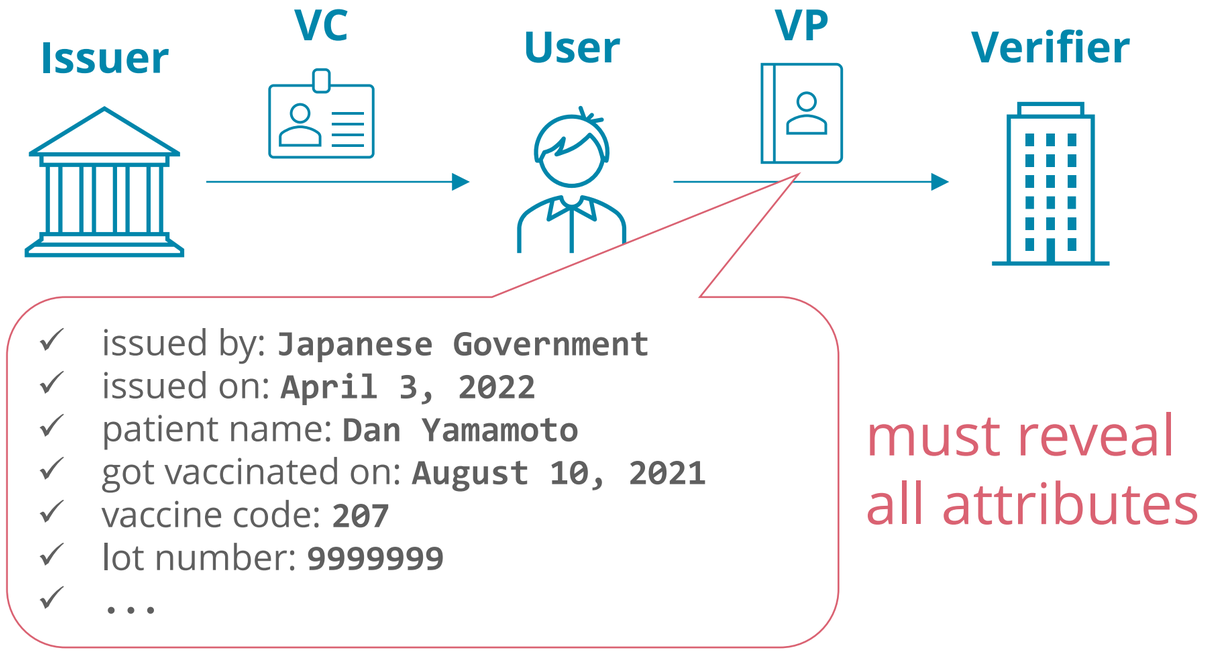
VC flavors

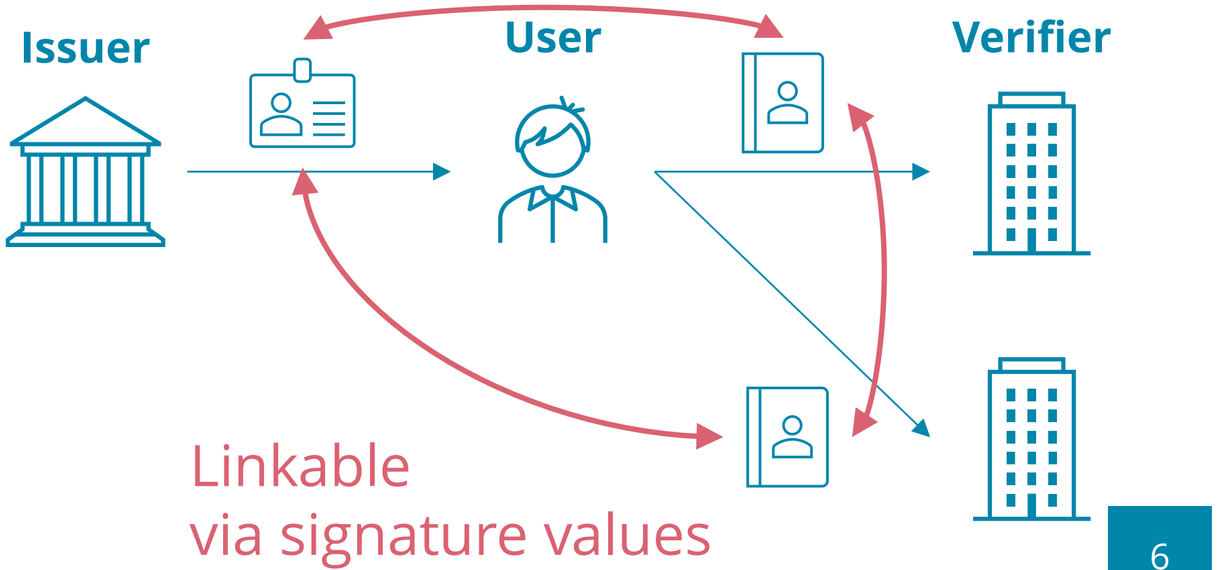
JWT-based VC
(e.g., SMART Health Cards)

doc format = **JSON**
proof format = **JWT**
sig scheme = **RSA, ECDSA, EdDSA, …**

- ✓ Simple, easy to develop
- ✓ Many real world instances
- ✗ No selective disclosure
- ✗ Presentations are linkable

Not privacy-preserving





VC flavors

JWT-based VC
(e.g., SMART Health Cards)

doc format = **JSON**
proof format = **JWT**
sig scheme = **RSA, ECDSA, EdDSA, …**

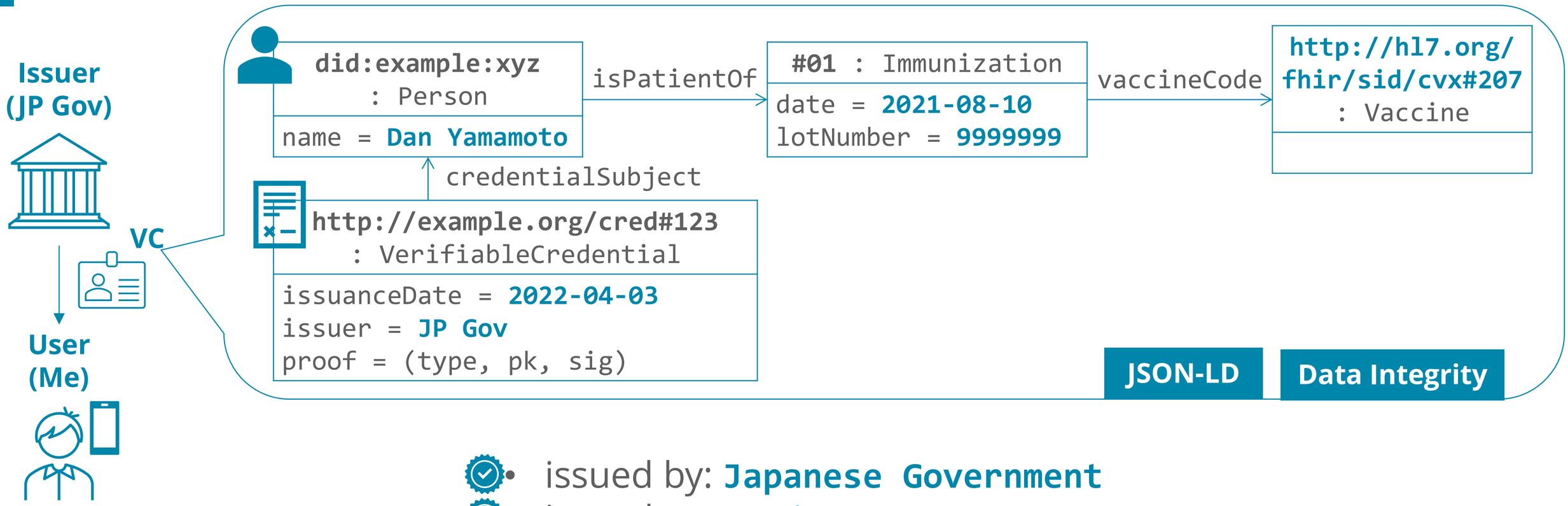
- ✓ Simple, easy to develop
- ✓ Many real world instances
- ✗ No selective disclosure
- ✗ Presentations are linkable

Linked-Data based VC
(LDP-BBS+)

doc format = **JSON-LD**
proof format = **Data Integrity** (LD Proof)
sig scheme = **BBS+**

- ✗ Relatively complicated
- ✗ Still work in progress
- ✓ Selective disclosure
- ✓ Unlinkable Presentations

LD-based Health Cards



Verifier
(Airport)

- issued by: **Japanese Government**
- issued on: **April 3, 2022**
- patient name: **Dan Yamamoto**
- got vaccinated on: **August 10, 2021**
- vaccine code: **207**
- lot number: **9999999**

Selective Disclosure & Unlinkable Presentations

Issuer
(JP Gov)

VC

User
(Me)

VP

Verifier
(Airport)

did:example:xyz
: Person

name = **Dan Yamamoto**

isPatientOf

#01 : Immunization

date = **2021-08-10**
lotNumber = **9999999**

vaccineCode

http://hl7.org/fhir/sid/cvx#207
: Vaccine

credentialSubject

http://example.org/cred#123
: VerifiableCredential

issuanceDate = **2022-04-03**
issuer = **JP Gov**
proof = (type, pk, sig)

did:example:xyz
: Person

****

isPatientOf

#01 : Immunization

date = **2021-08-10**
****

vaccineCode

http://hl7.org/fhir/sid/cvx#207
: Vaccine

credentialSubject

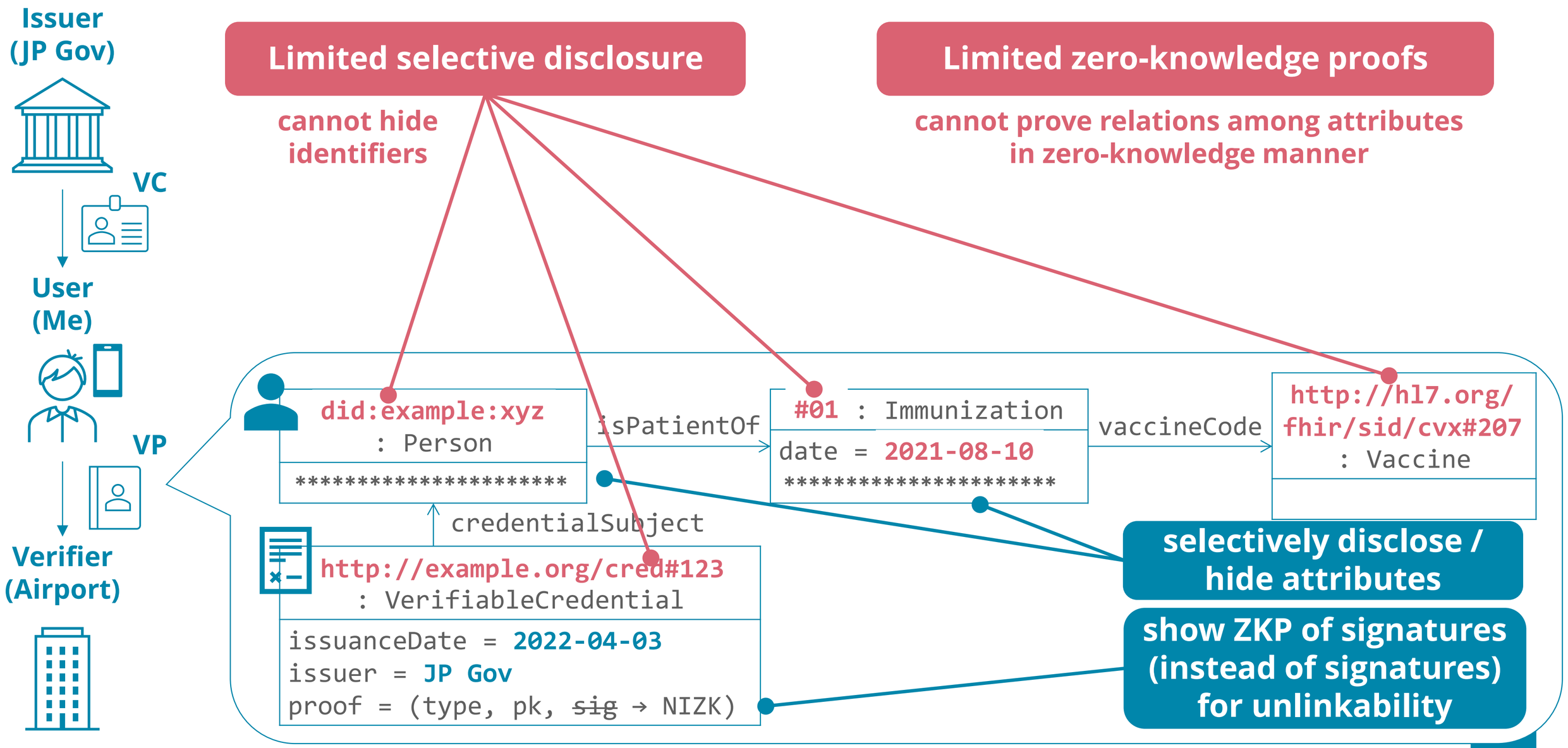
http://example.org/cred#123
: VerifiableCredential

issuanceDate = **2022-04-03**
issuer = **JP Gov**
proof = (type, pk, ~~**sig**~~ → **NIZK**)

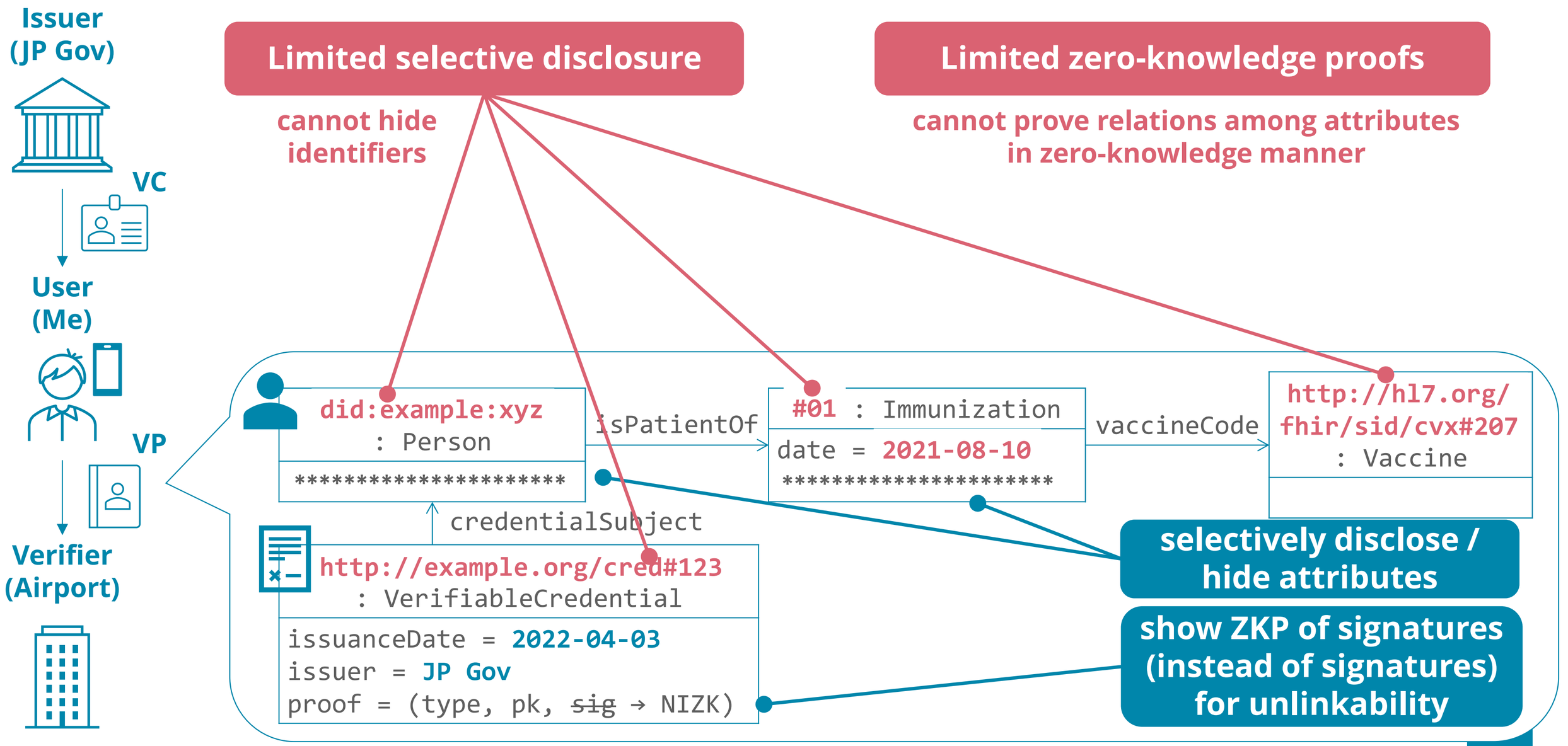
selectively disclose / hide attributes

show ZKP of signatures (instead of signatures) for unlinkability

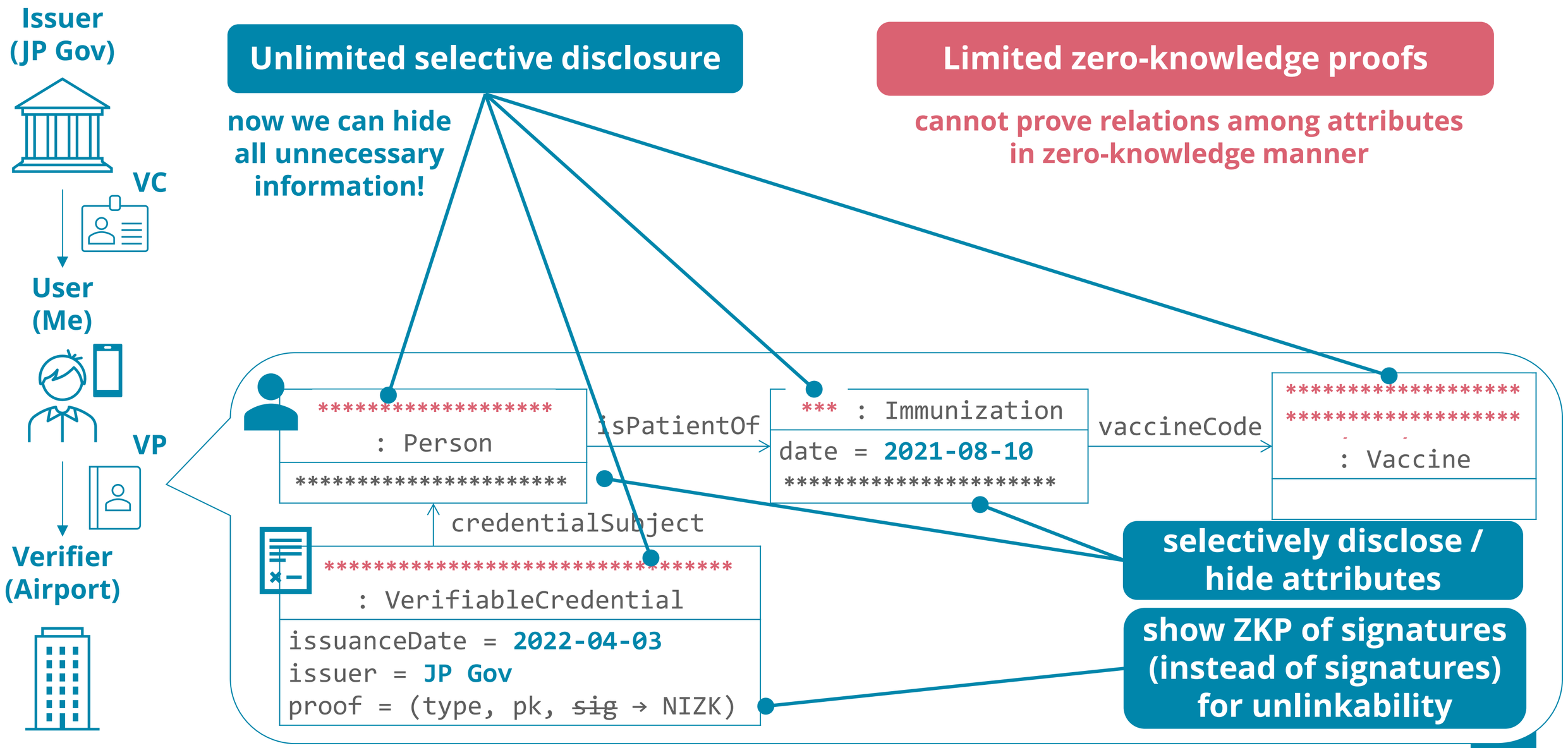
Limitations of Existing Construction (LDP-BBS+)



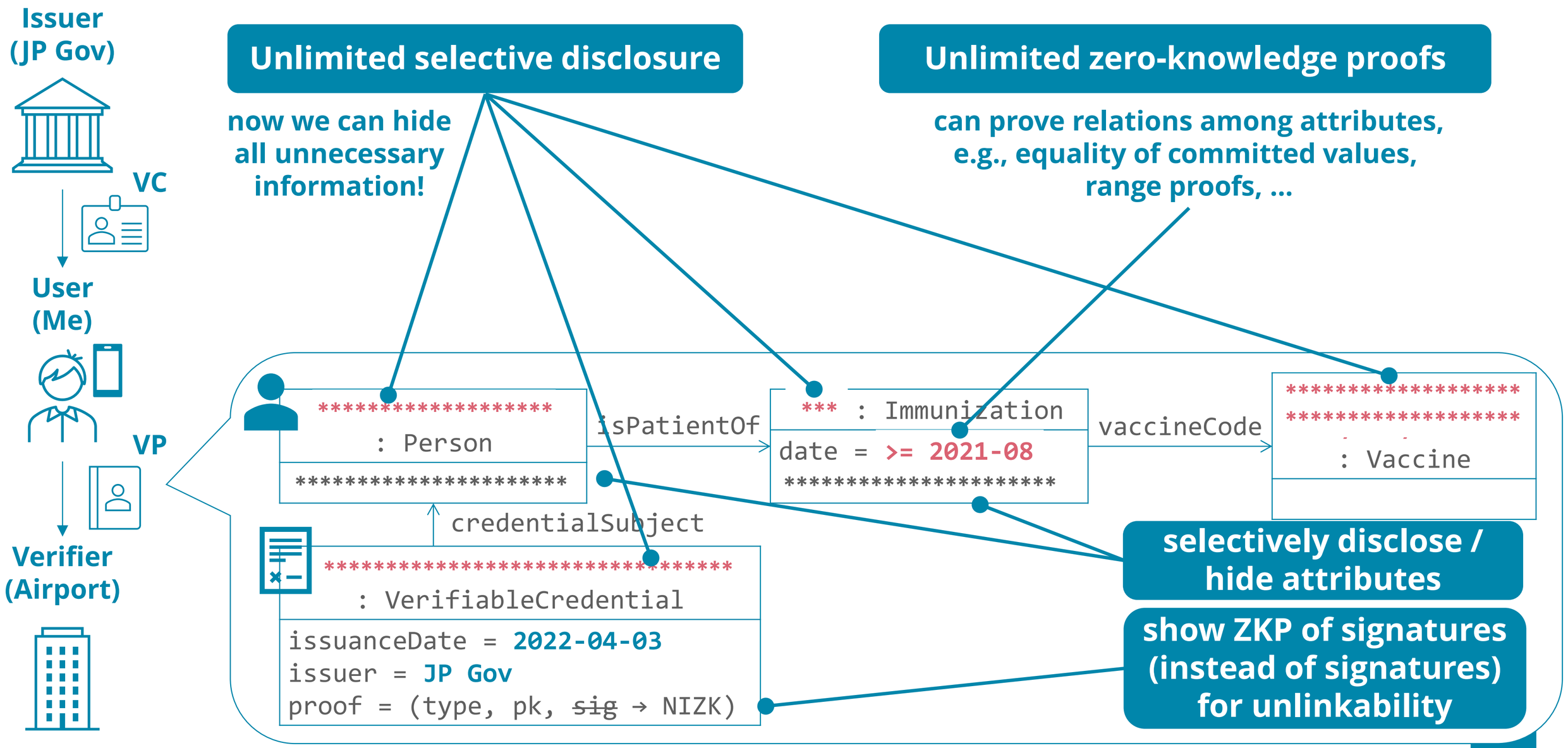
Our Contribution



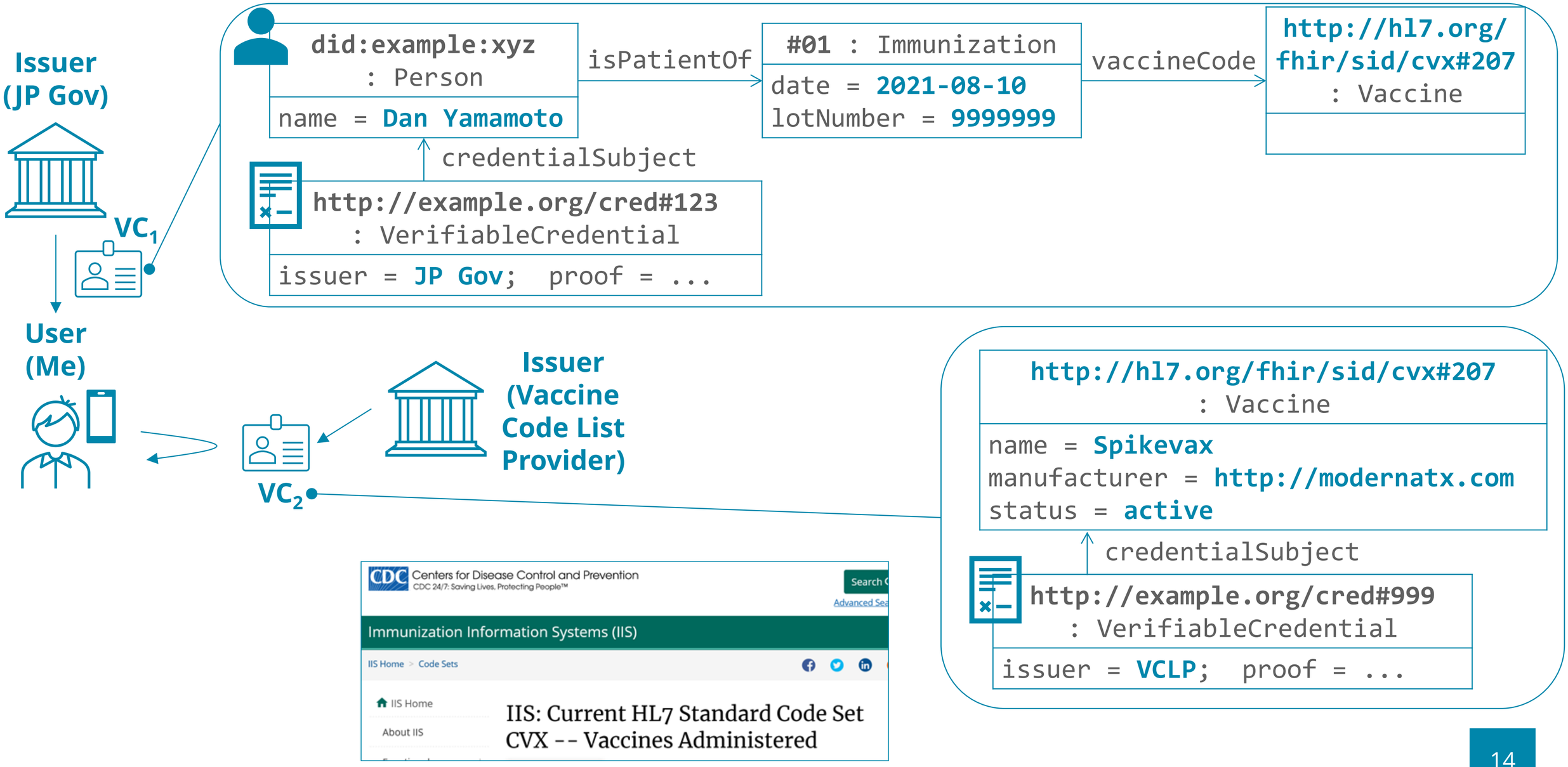
Our Contribution



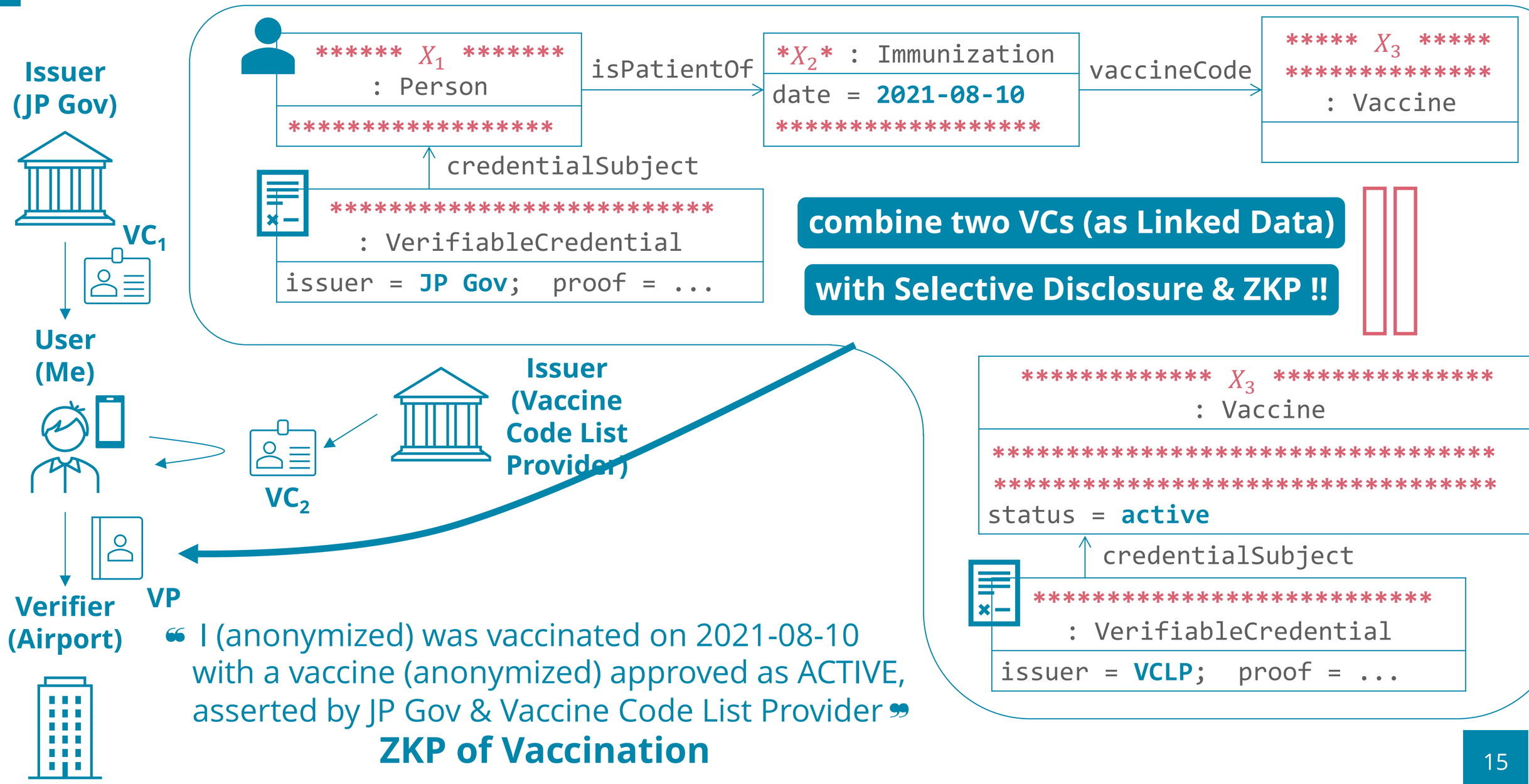
Our Contribution



Possible Future Use Cases



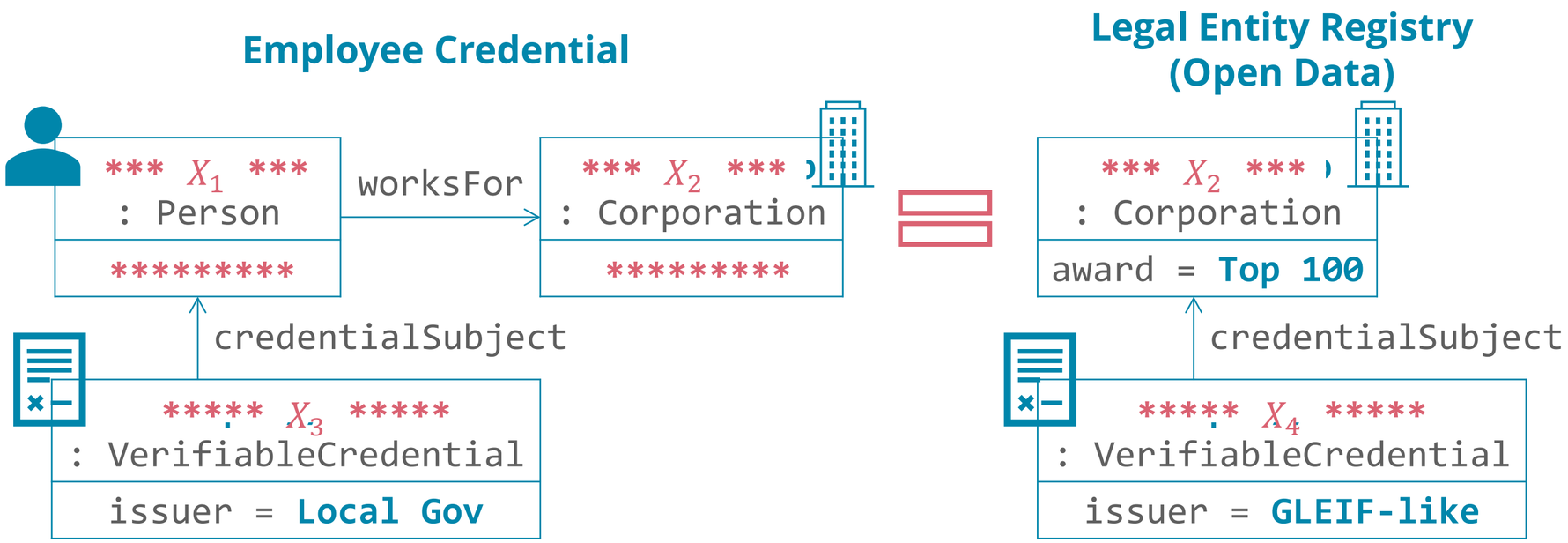
Possible Future Use Cases



❝ I (anonymized) was vaccinated on 2021-08-10 with a vaccine (anonymized) approved as ACTIVE, asserted by JP Gov & Vaccine Code List Provider ❞

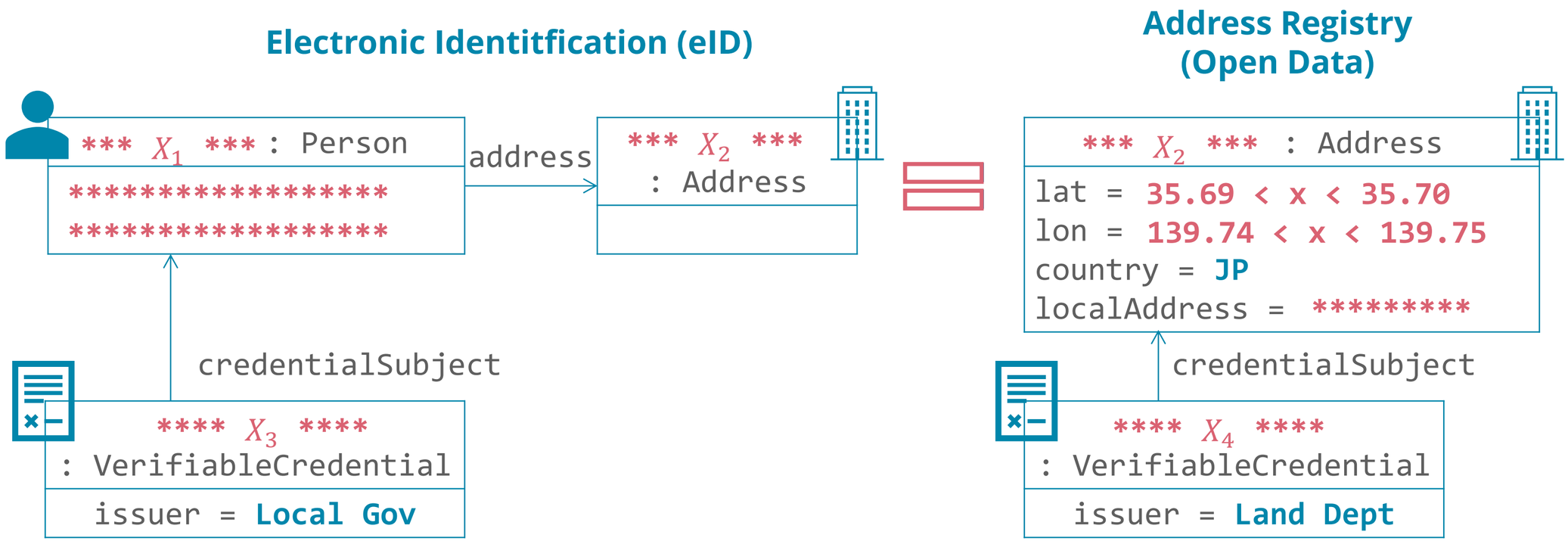
ZKP of Vaccination

Other Use Cases: ZKP of Employer



❝ I (anonymized) work for
a company (anonymized) that received the Top 100 award,
asserted by Local Gov & GLEIF-like organization ❞

Other Use Cases: ZKP of Residence



❝ I (anonymized) live in a place (anonymized)
that is geographically located in (35.69, 139.74) --- (35.70, 139.75),
asserted by Local Gov & Land Department ❞

Related Standardization Efforts

JSON-LD, RDF, ...

Verifiable Credentials Data Model
W3C Recommendation

Data Integrity
W3C Draft Community Group Report (in Progress)

BBS+ Signatures 2020 (LDP-BBS+)
W3C Draft Community Group Report (in Progress)

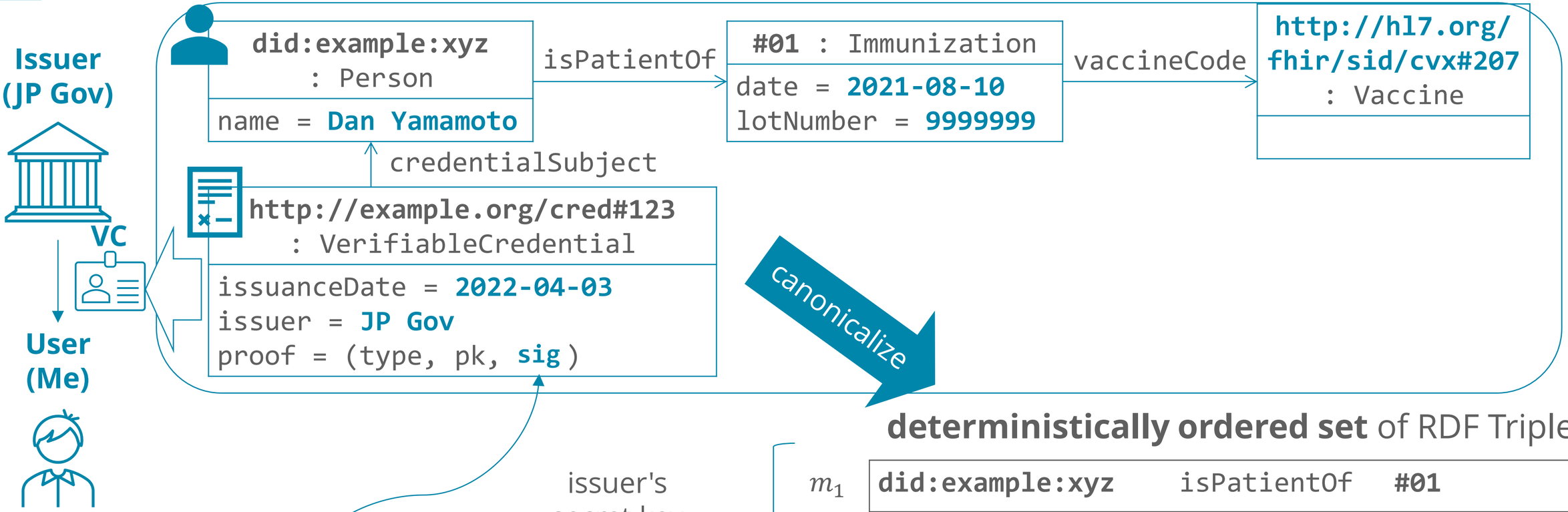
OpenID Connect for SSI
(in Progress)

The BBS Signature Scheme
(in Progress)

Ours: LDP-BBS++?
(not on any standardization process yet)

*this work formalizes security & privacy notions for future standardization

Existing Construction (LDP-BBS+)



deterministically ordered set of RDF Triples

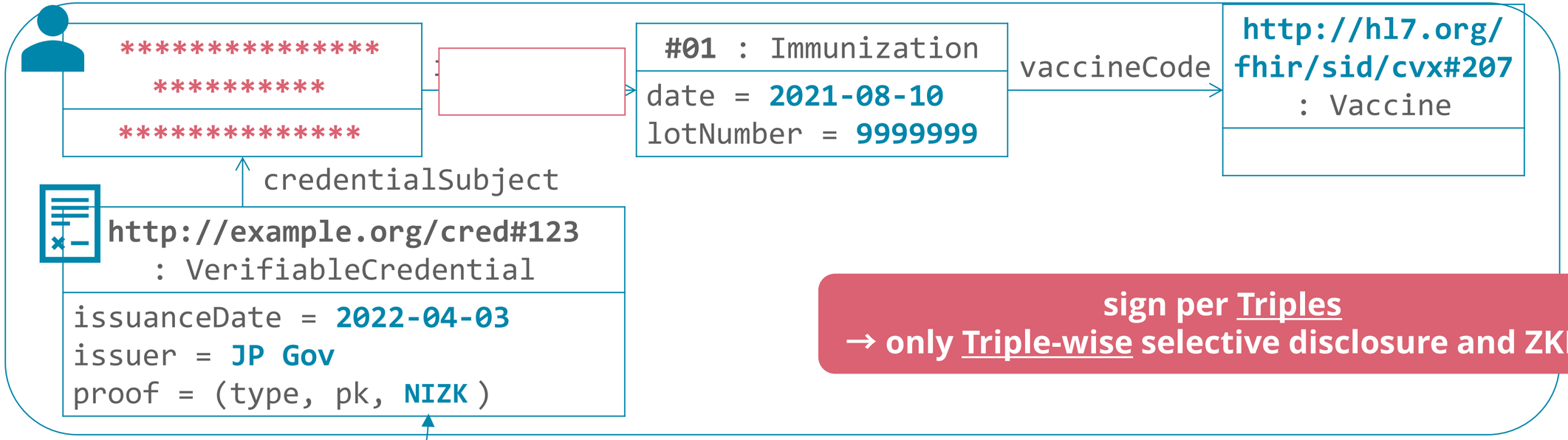
m_1	**did:example:xyz**	isPatientOf	**#01**
m_2	**did:example:xyz**	name	**Dan Yamamoto**
m_3	**did:example:xyz**	type	Person
m_4	**http://hl7...#207**	type	Vaccine
m_5	http://...#123	issuanceDate	2022-04-03
⋮		⋮	

issuer's
secret key

**BBS+.
sign**

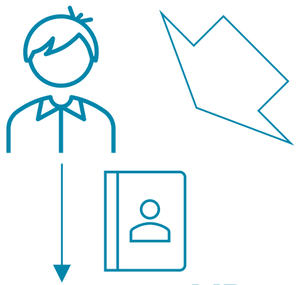
signature

Existing Construction (LDP-BBS+) = **Triple-wise** Encoding



sign per Triples
→ only Triple-wise selective disclosure and ZKPs

User (Me)



Verifier (Airport)

VP

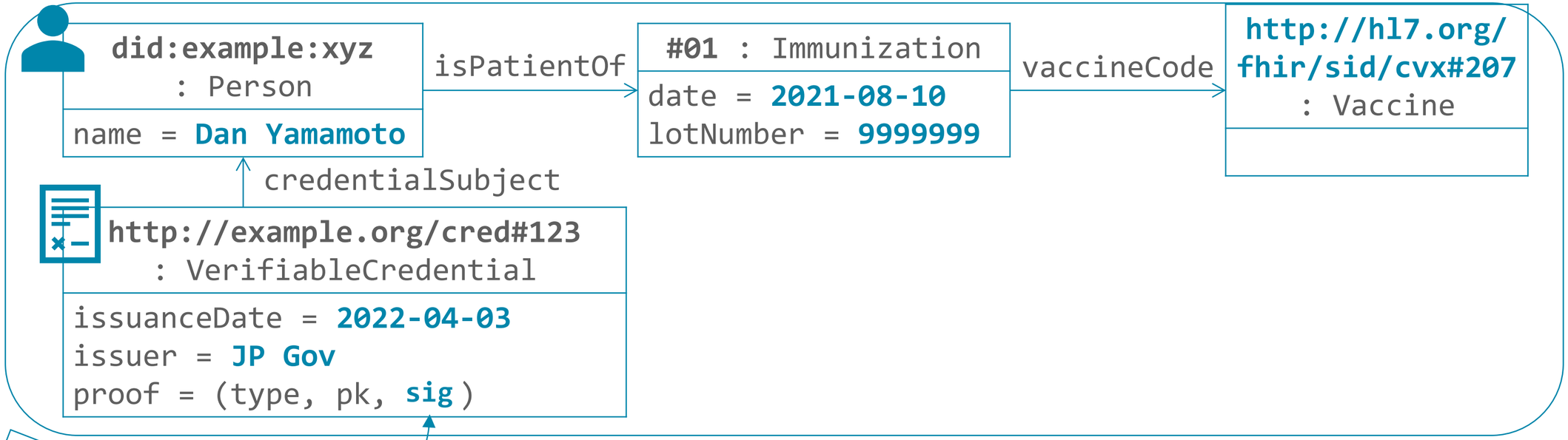
"hide m_2"

NIZK proof

BBS+. show

m_1	**********
m_2	**********
m_3	**********
m_4	http://hl7...#207 type Vaccine
m_5	http://...#123 issuanceDate 2022-04-03
⋮	⋮

Our Construction = **Term-wise** Encoding



VC
(JSON-LD)

issuer's
secret key

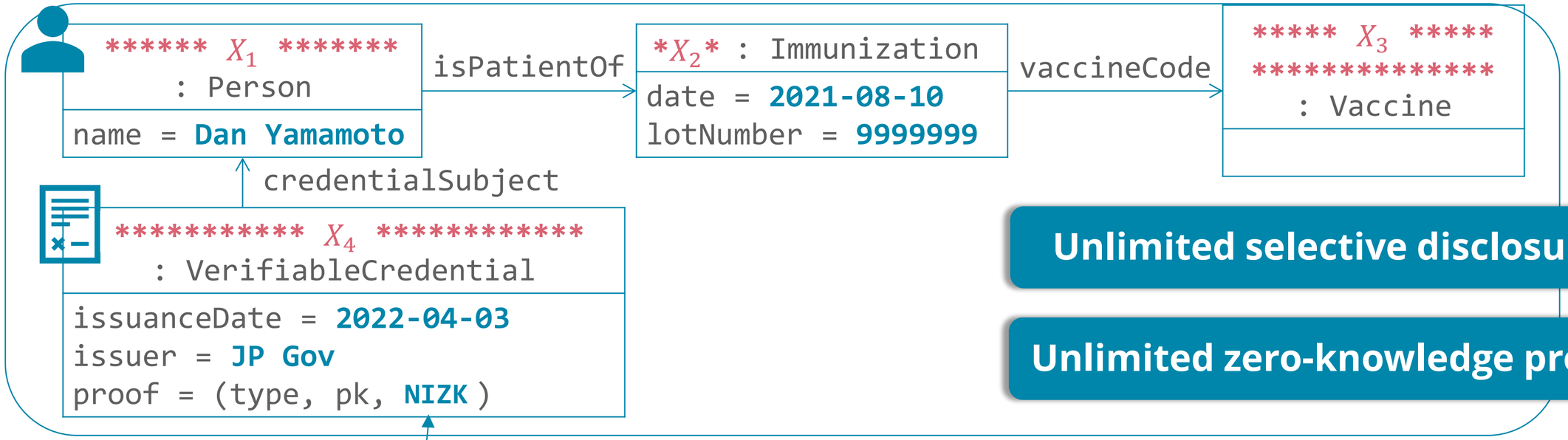
BBS+.
sign

signature

m_1	did:example:xyz	m_2	isPatientOf	m_3	#01
m_4	did:example:xyz	m_5	name	m_6	Dan Yamamoto
m_7	did:example:xyz	m_8	type	m_9	Person
m_{10}	http://hl7...#207	m_{11}	type	m_{12}	Vaccine
m_{13}	http://...#123	m_{14}	issuanceDate	m_{15}	2022-04-03
⋮	⋮	⋮	⋮	⋮	⋮

sign per Terms
→ Term-wise selective disclosure and ZKPs

Our Construction = **Term-wise** Encoding



Unlimited selective disclosure

Unlimited zero-knowledge proof

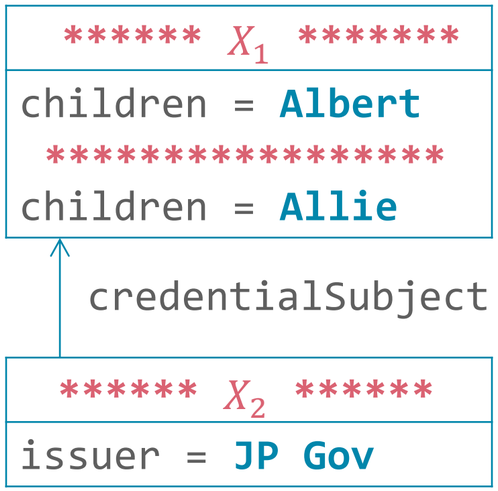
NIZK proof ← **BBS+. show**

m_1	****** X_1 *******	m_2	isPatientOf	m_3	#01
m_4	****** X_1 *******	m_5	name	m_6	Dan Yamamoto
m_7	****** X_1 *******	m_8	type	m_9	Person
m_{10}	****** X_3 *******	m_{11}	type	m_{12}	Vaccine
m_{13}	****** X_4 *******	m_{14}	issuanceDate	m_{15}	≥2022-01-01
⋮	⋮	⋮	⋮	⋮	⋮

Security and Privacy

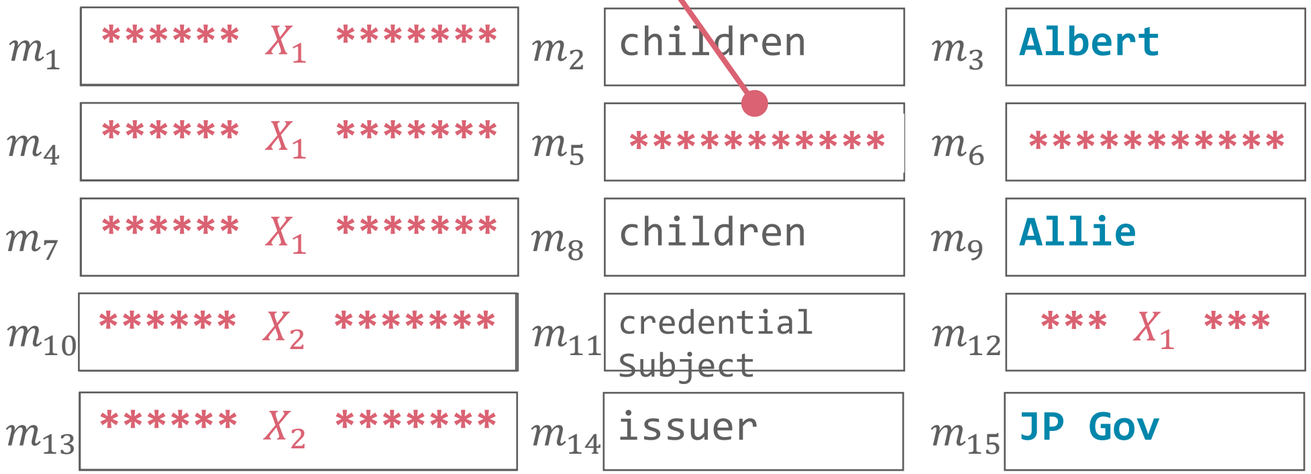
- We defined game-based notions of **unforgeability** and **anonymity** based on Sanders' definition (@ PKC '20)
- and proved:
  - Our construction is **unforgeable**
    if the underlying anonymous credential (e.g., BBS+) is unforgeable
  - Our construction is **weakly anonymous**
    if the underlying anonymous credential (e.g., BBS+) is anonymous

Anonymity vs. Weak Anonymity



canonicalize

Adversary knows:
m_5 must be lexicographically larger than m_2
(if lexicographically sort is used for canonicalization)



VP

NIZK proof

BBS+. show

Anonymous presentation only leaks:
- attributes selectively disclosed by user
- issuer's public key

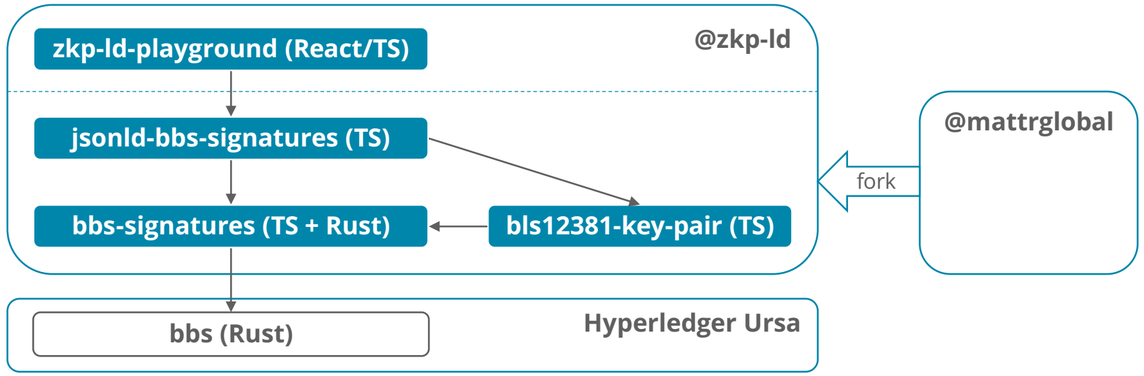
Weakly anonymous presentation additionally leaks:
- total number of attributes: $|\{m_i\}| = 15$
- index i of canonicalized attributes $\{m_i\}$

workarounds:
add dummy attributes
& random permutations

Implementations and Demo

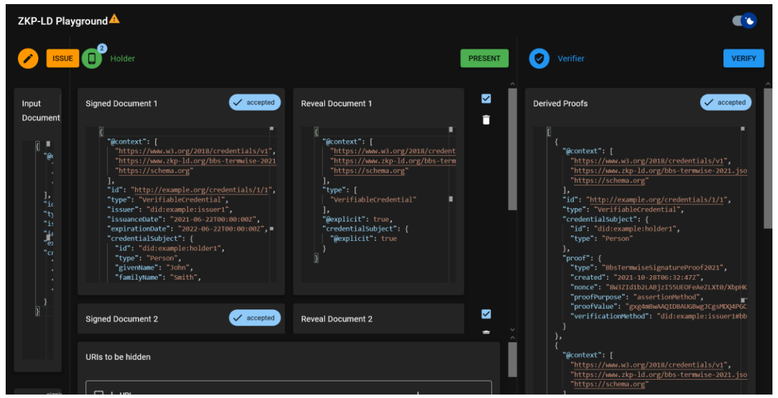
Implementations (published on Github and npm)

- @zkp-ld/jsonld-signatures-bbs
- @zkp-ld/bls12381-key-pair
- @zkp-ld/bbs-signatures



ZKP-LD Playground <https://playground.zkp-ld.org>

- a playground for developers
- you can sign & verify LD-based credential and show & verify presentations on browser

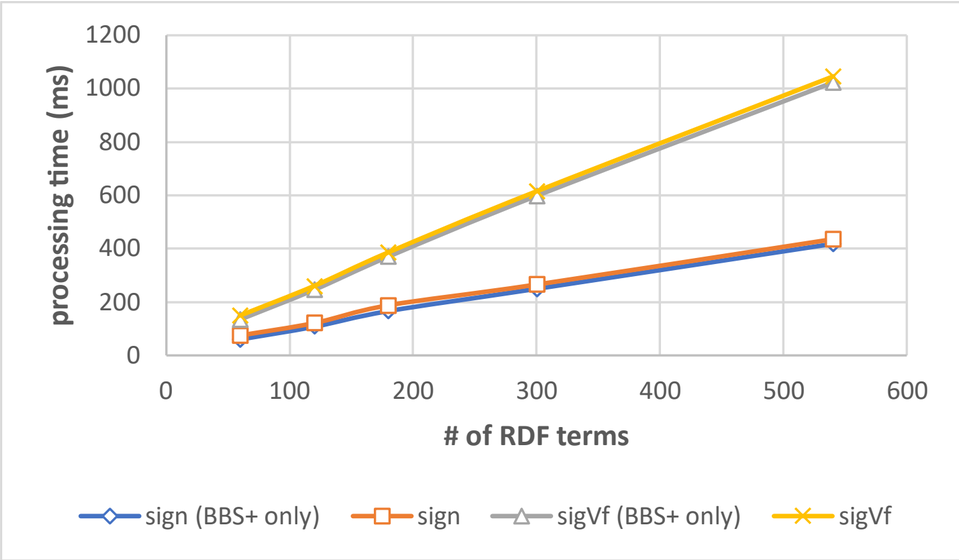


Performance Evaluation

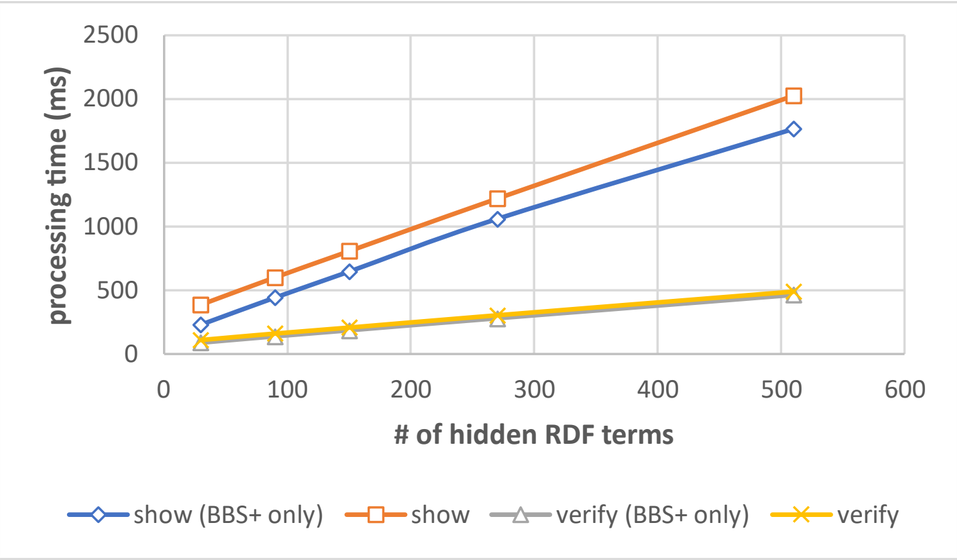
size (bits)	
secret key	256
public key	768
signature	896
proof	$2944 + 256\,n$

(n : # of hidden terms)

VC: sign / sigVf



VP: show / verify



- i7-10750H (6 cores 12 threads) CPU, 32GB RAM, Google Chrome
- takes at most 1 sec to handle < 200 RDF terms
- (the issuance of bound credentials has not yet been implemented & evaluated)

Conclusions

1. Constructed a LD-based VC scheme with fully selective disclosure
2. Proposed novel use cases using LD-based VCs with ZKP
3. Formalized LD-based VC and its security and privacy notion
4. Proved the security and privacy of our construction
5. Provided OSS implementations and Web-based demo

Future Work

- Fully anonymous construction
- Revocation, Delegation, Pseudonyms, Issuer-Hiding
- Constant proof sizes and verification times