# Formalising Linked-Data based Verifiable Credentials for Selective Disclosure

Dan Yamamoto (Internet Initiative Japan Inc.)

Yuji Suga (Internet Initiative Japan Inc.)

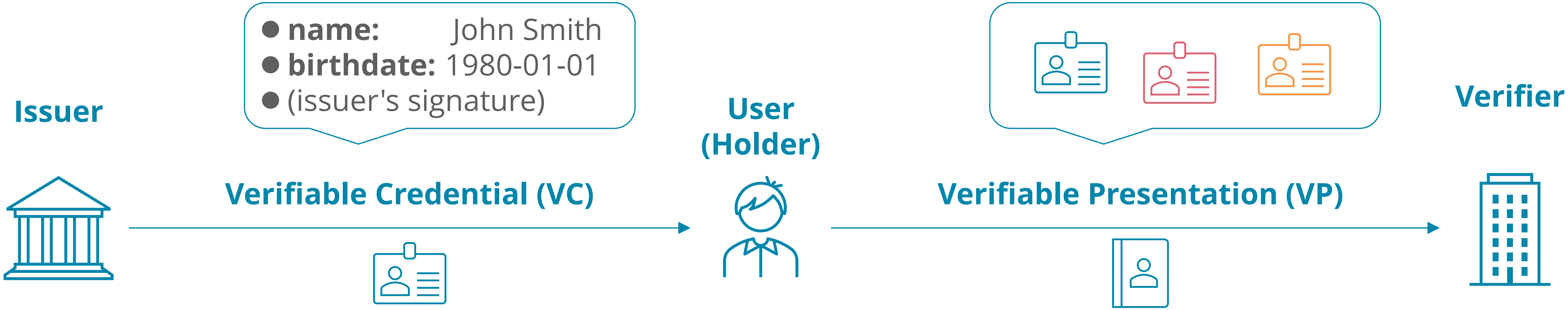
Kazue Sako (Waseda University)

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**



- **name:** John Smith
- **birthdate:** 1980-01-01
- (issuer's signature)

Issuer

Verifiable Credential (VC)

User (Holder)

Verifiable Presentation (VP)

Verifier

- 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, ...

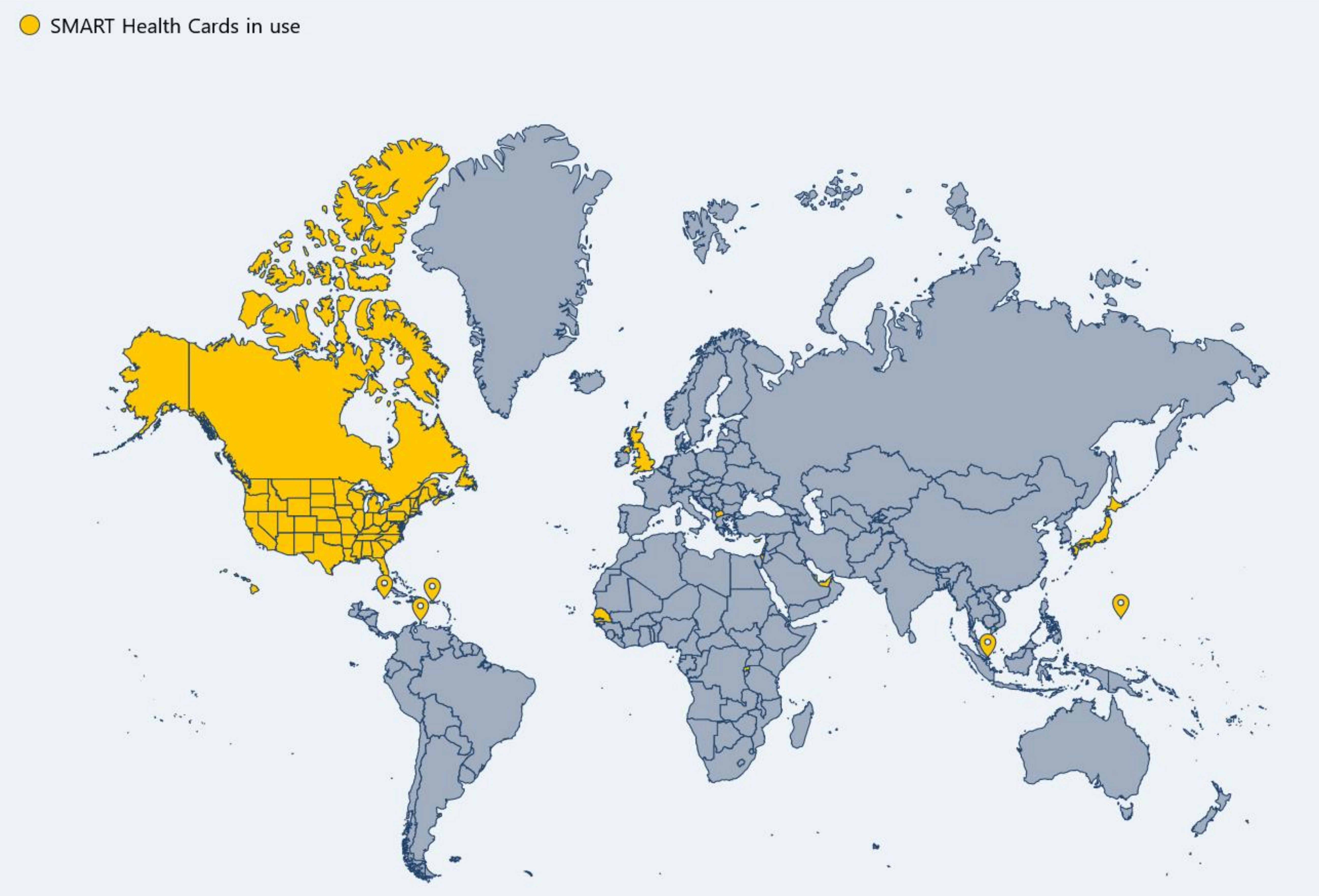
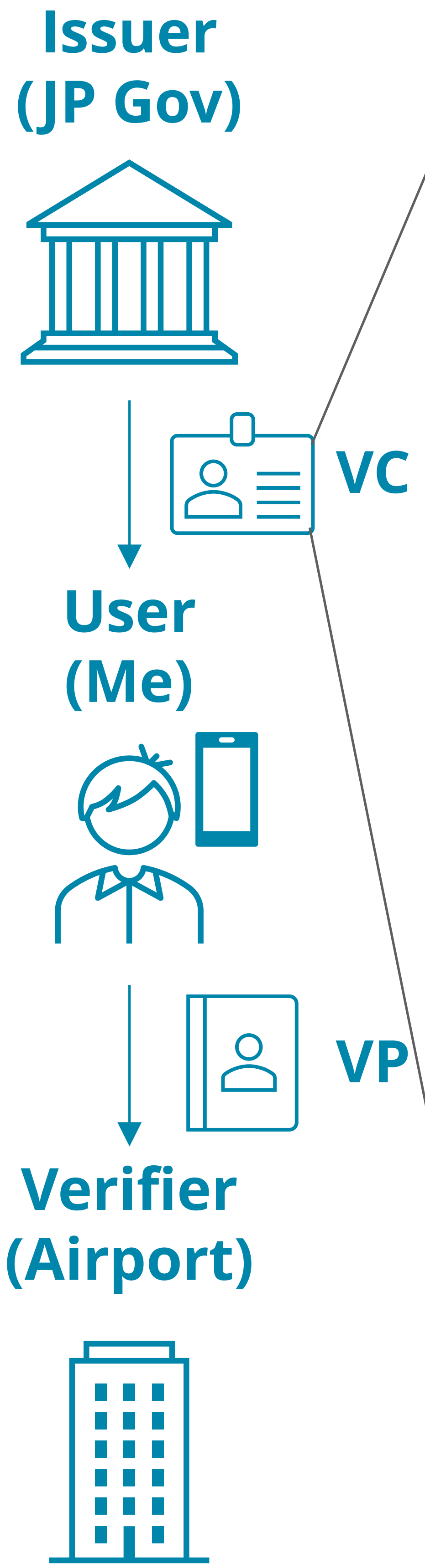
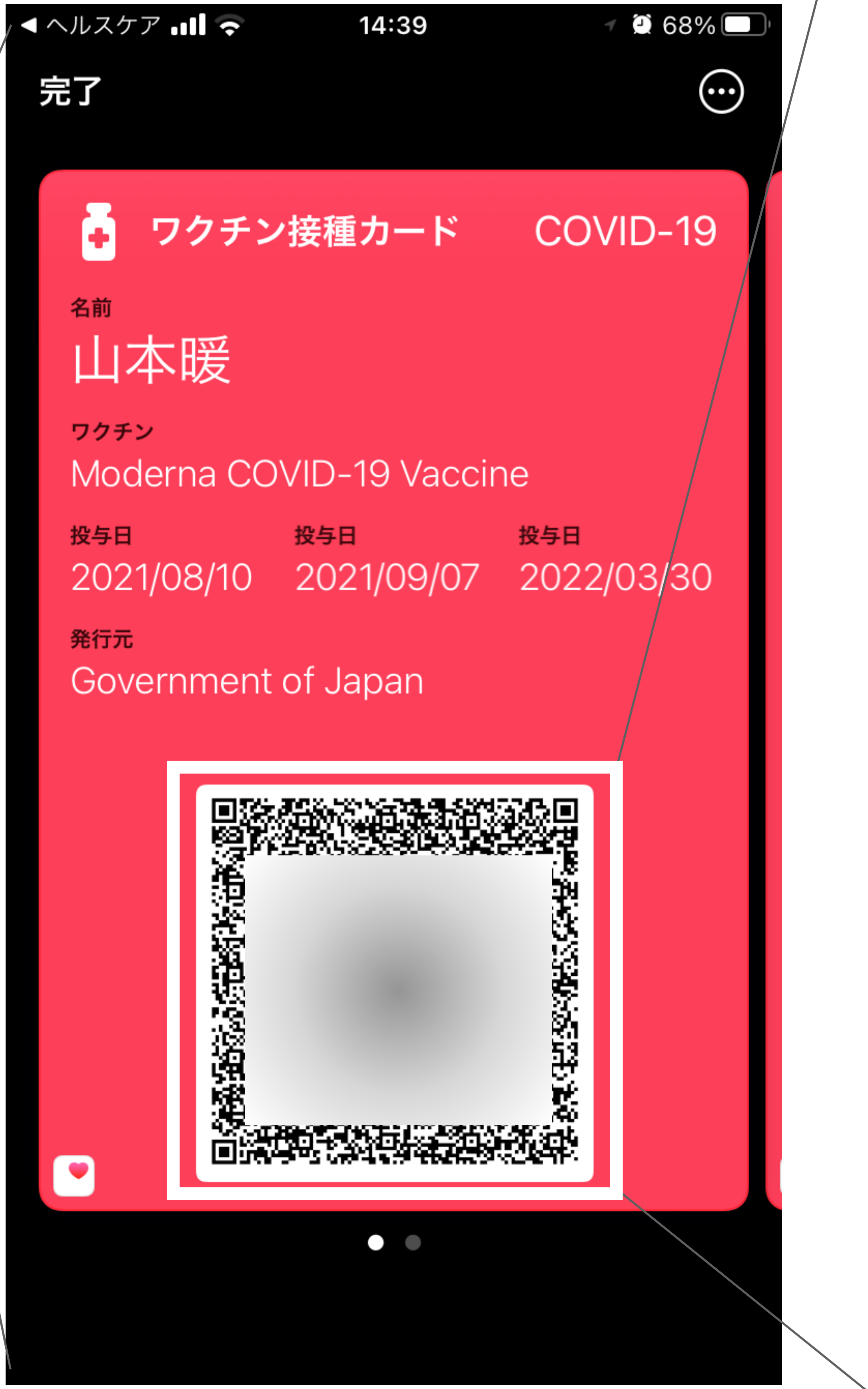


image: https://vci.org

# SMART Health Cards




◀ ヘルスケア 14:39 68%

完了

ワクチン接種カード COVID-19

名前
山本暖

ワクチン
Moderna COVID-19 Vaccine

| 投与日 | 投与日 | 投与日 |
|---|---|---|
| 2021/08/10 | 2021/09/07 | 2022/03/30 |

発行元
Government of Japan

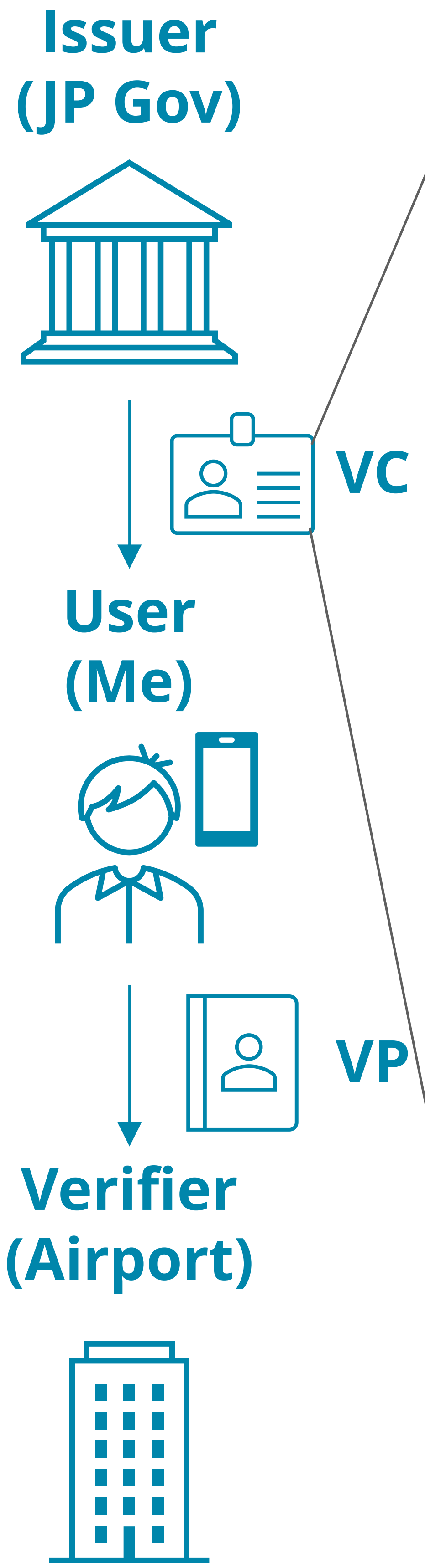
JWT

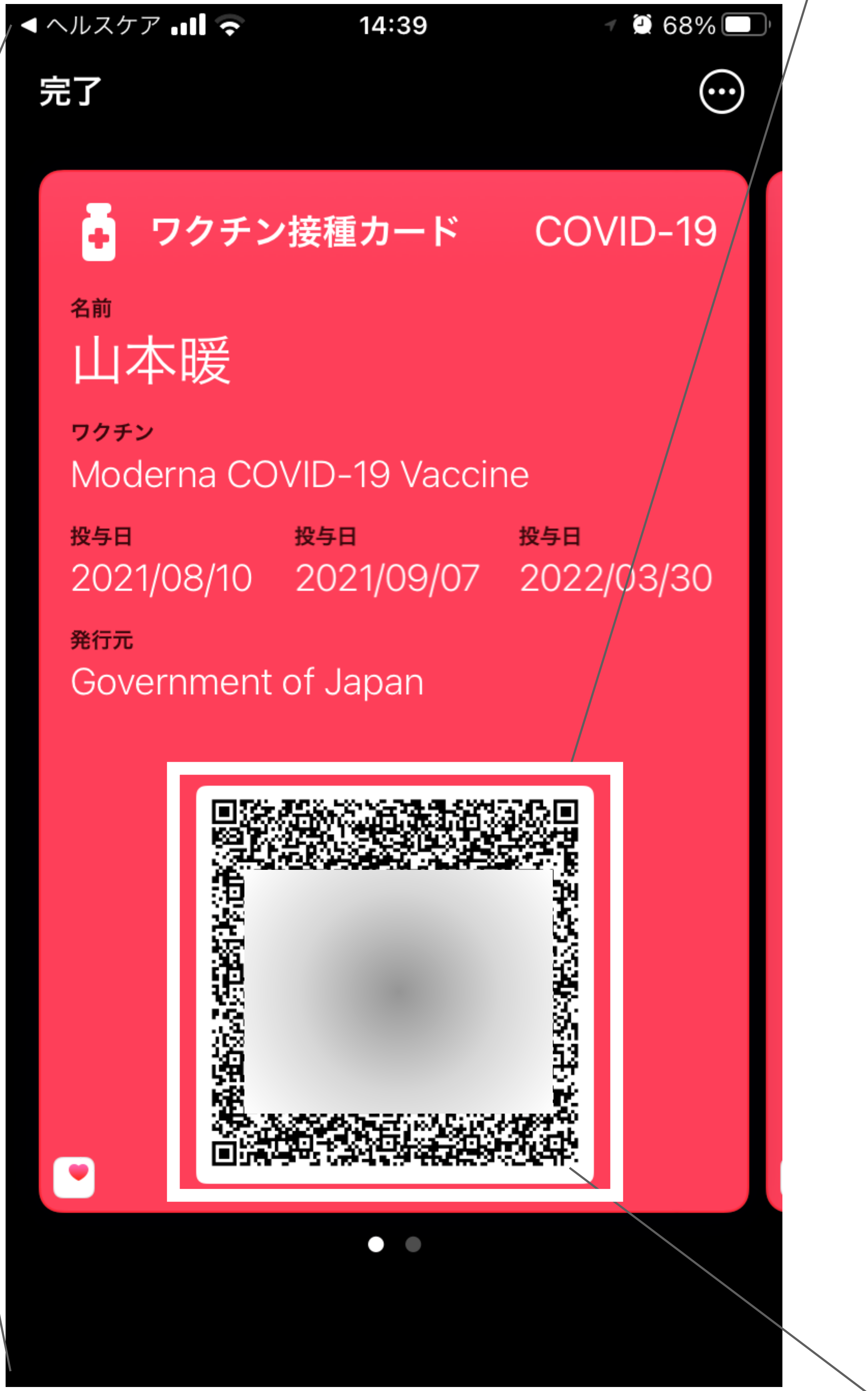
Header

```
{ "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





ワクチン接種カード COVID-19

名前
山本暖

ワクチン
Moderna COVID-19 Vaccine

| 投与日 | 投与日 | 投与日 |
|---|---|---|
| 2021/08/10 | 2021/09/07 | 2022/03/30 |

発行元
Government of Japan

**JWT**

Header

```
{ "iss": "https://vc.vrs.digital.go.jp/issuer",
  "nbf": 1648956149.461584,  // ~= 2022-04-03
  "vc": {
```

- ✓ 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**

```
                "use": "official",
                "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" ...
```

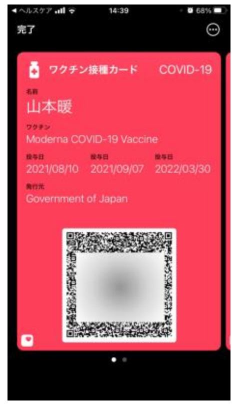
Signature

# VC flavors

## JWT-based VC

**(e.g., SMART Health Cards)**

JWT



◀ ヘルスケア 14:39 68%

完了

ワクチン接種カード COVID-19

名前
山本暖

ワクチン
Moderna COVID-19 Vaccine

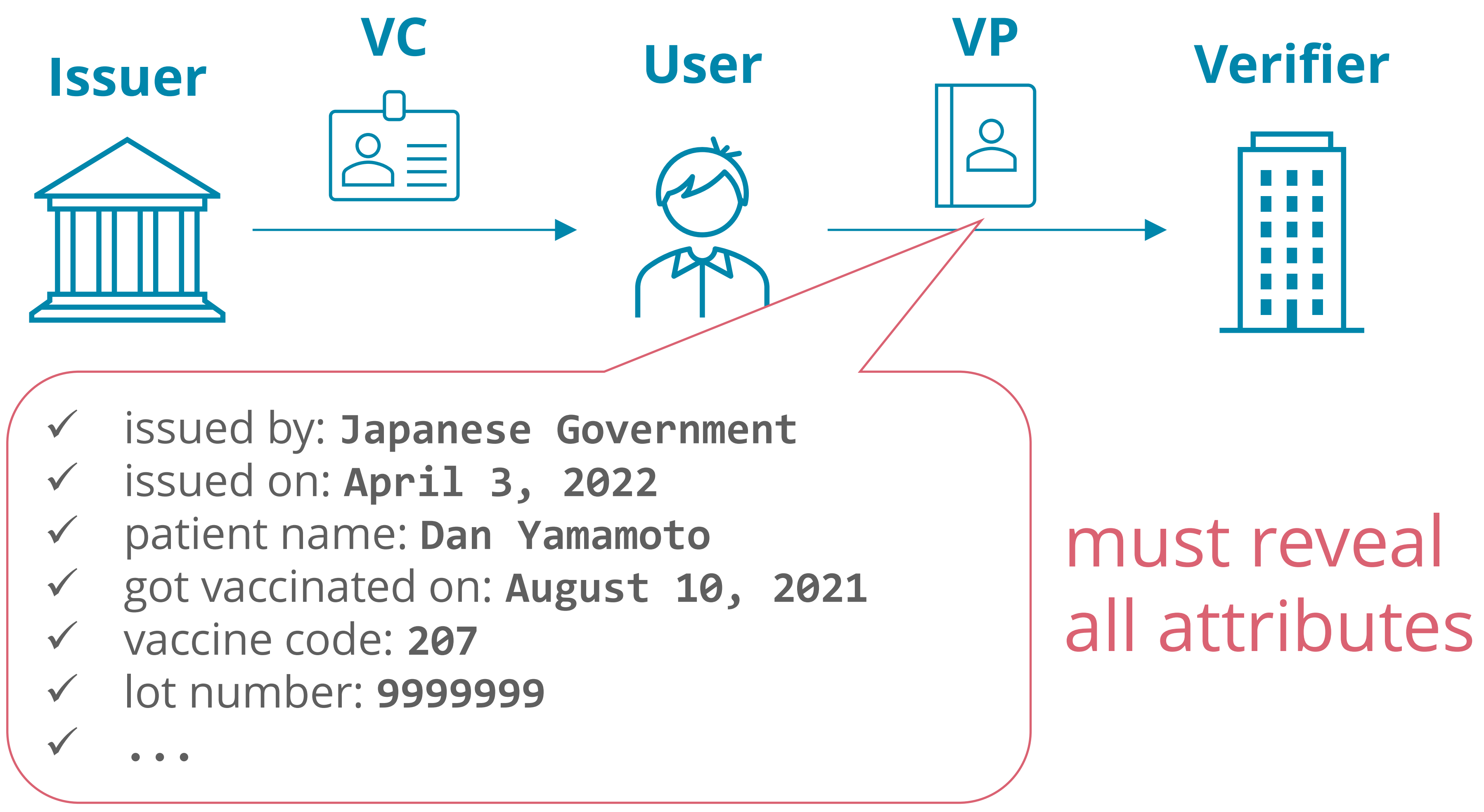
| 接与日 | 接与日 | 接与日 |
|---|---|---|
| 2021/08/10 | 2021/09/07 | 2022/03/30 |

発行元
Government of Japan

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

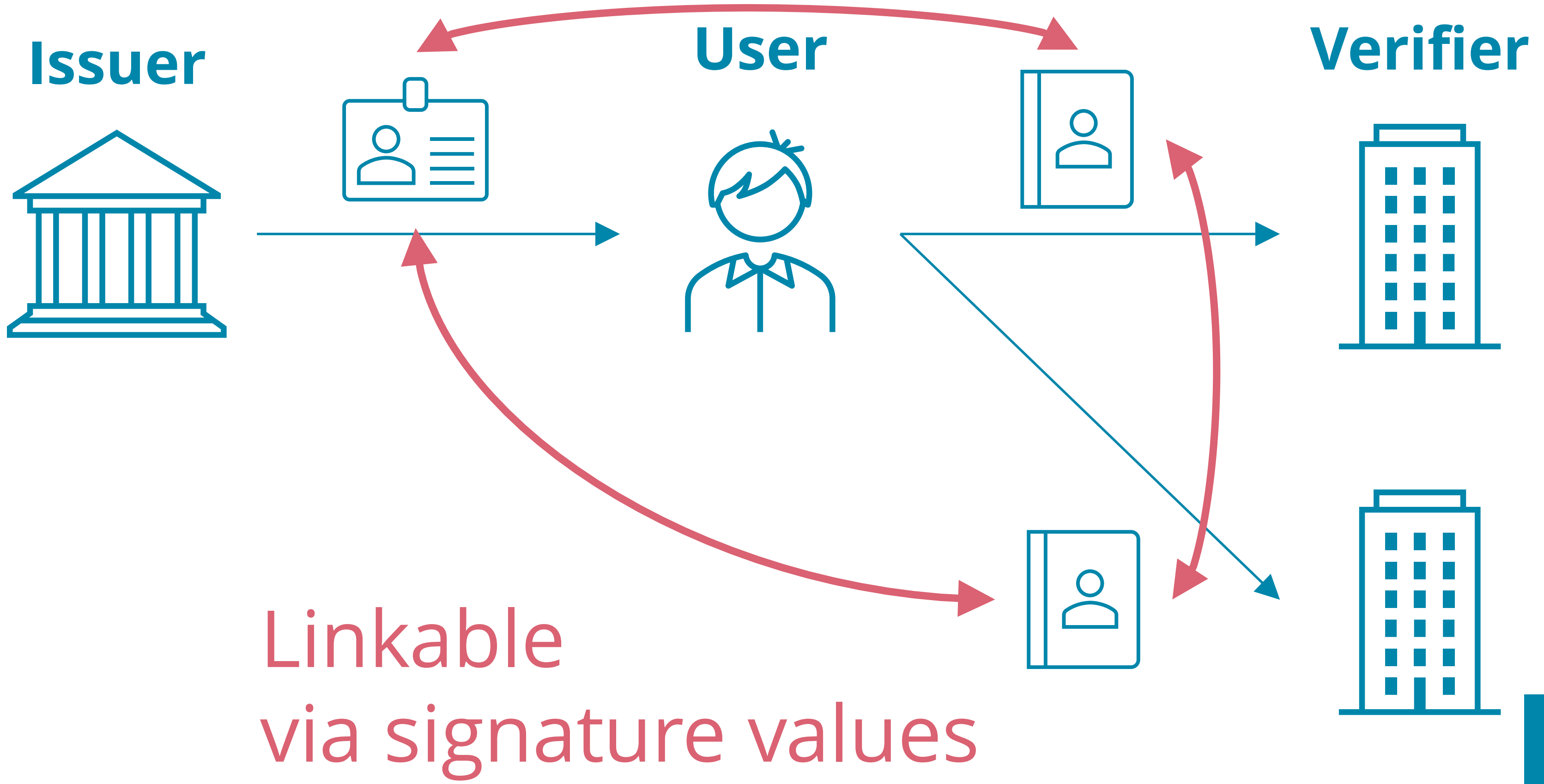
- ✓ Simple, easy to develop
- ✓ Many real world instances
- ✗ No selective disclosure
- ✗ Presentations are linkable

**Not privacy-preserving**



- ✓ 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`
- ✓ `...`

must reveal all attributes

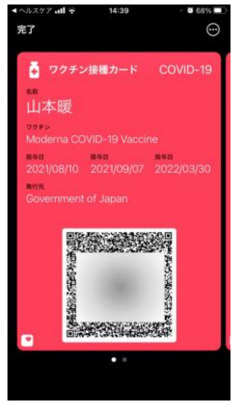


Linkable
via signature values

# VC flavors

## JWT-based VC

**(e.g., SMART Health Cards)**



ワクチン接種カード COVID-19

名前
山本暖

ワクチン
Moderna COVID-19 Vaccine

| 接種日 | 接種日 | 接種日 |
|---|---|---|
| 2021/08/10 | 2021/09/07 | 2022/03/30 |

発行元
Government of Japan

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

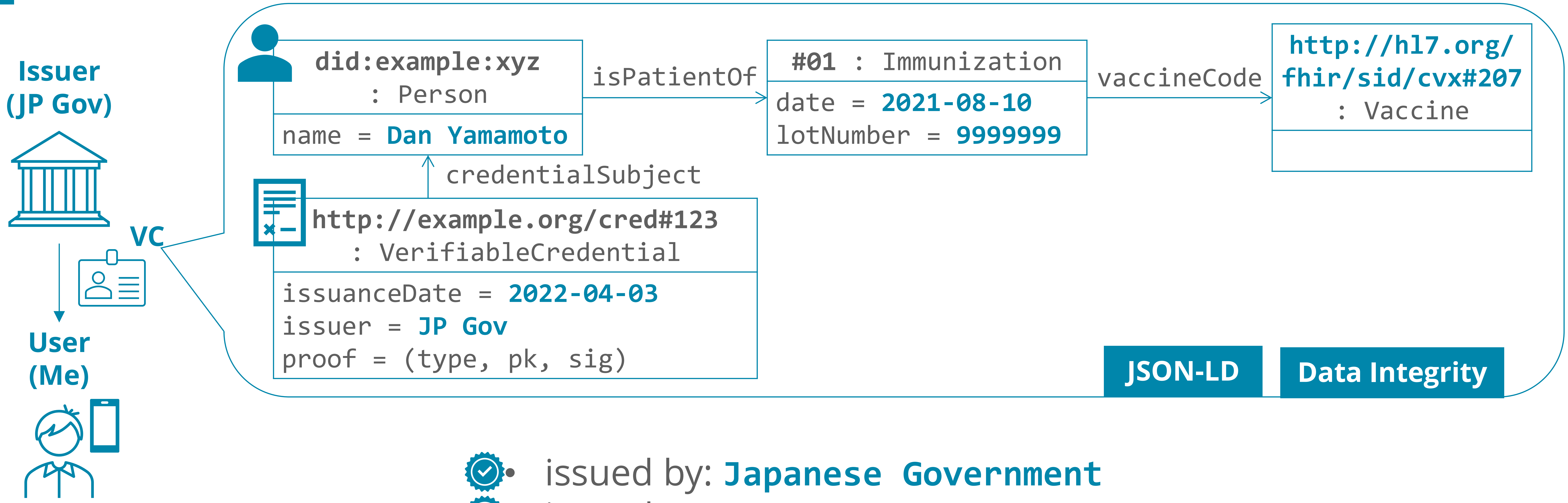
- ✓ Simple, easy to develop
- ✓ Many real world instances
- ✗ No selective disclosure
- ✗ Presentations are linkable

## 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



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

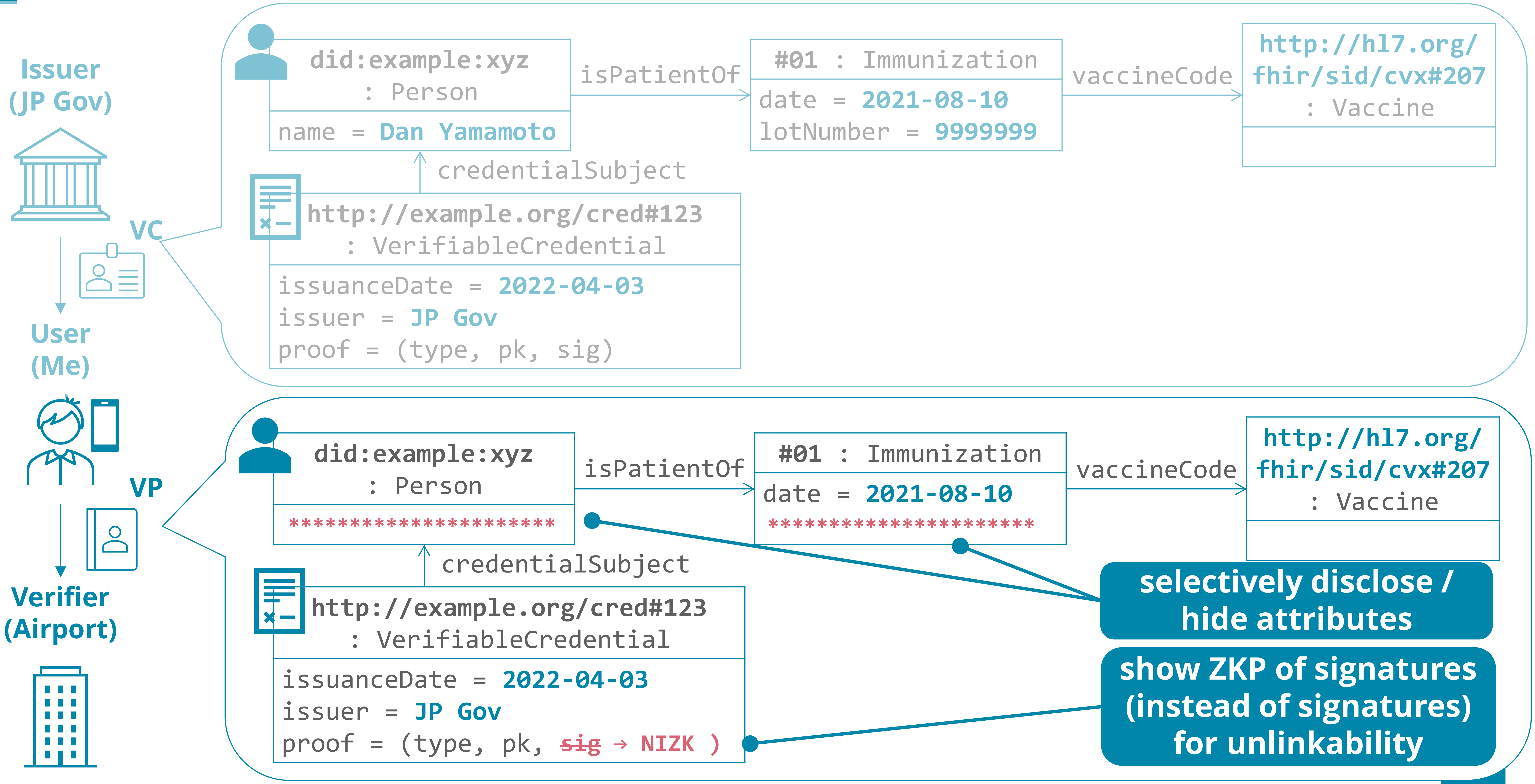
issuanceDate = **2022-04-03**
issuer = **JP Gov**
proof = (type, pk, sig)

**JSON-LD**

**Data Integrity**

- ✓ 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

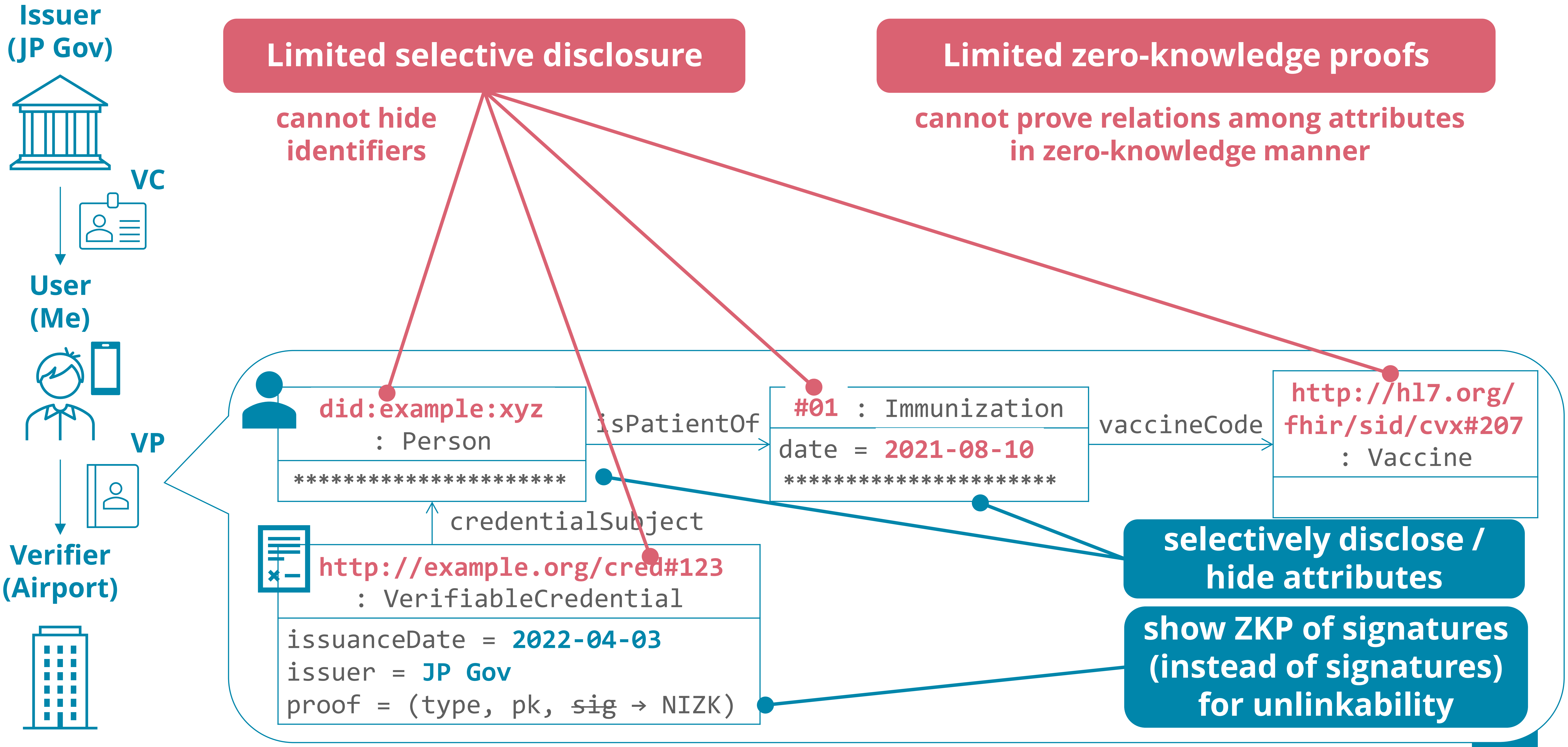
http://example.org/cred#123
: VerifiableCredential

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+)



Issuer (JP Gov)

VC

User (Me)

VP

Verifier (Airport)

**Limited selective disclosure**

cannot hide identifiers

**Limited zero-knowledge proofs**

cannot prove relations among attributes in zero-knowledge manner

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

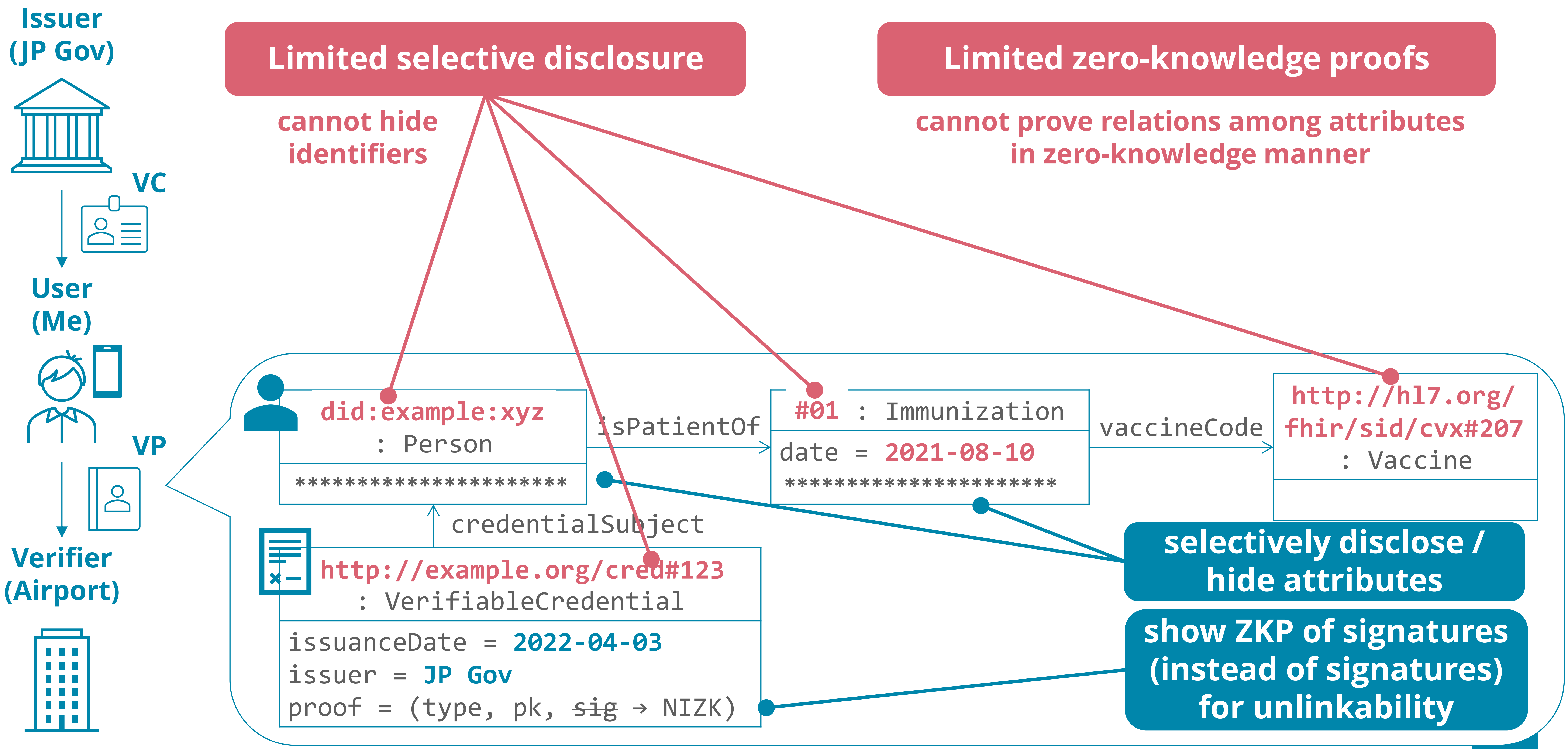
issuer = JP Gov

proof = (type, pk, ~~sig~~ → NIZK)

**selectively disclose / hide attributes**

**show ZKP of signatures (instead of signatures) for unlinkability**

# Our Contribution



Issuer (JP Gov)

VC

User (Me)

VP

Verifier (Airport)

**Limited selective disclosure**

cannot hide identifiers

**Limited zero-knowledge proofs**

cannot prove relations among attributes in zero-knowledge manner

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

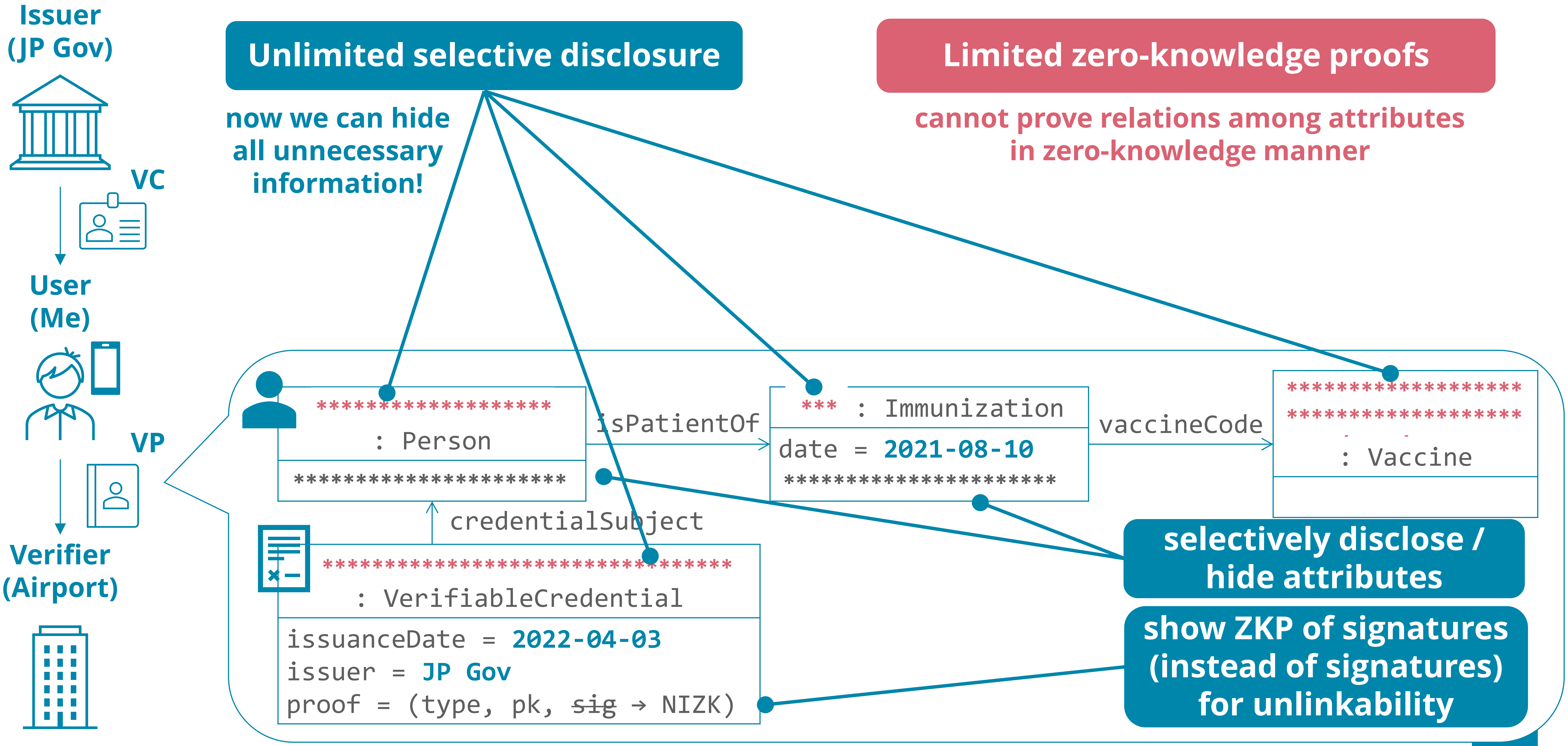
issuer = JP Gov

proof = (type, pk, ~~sig~~ → NIZK)

**selectively disclose / hide attributes**

**show ZKP of signatures (instead of signatures) for unlinkability**

# Our Contribution



Issuer (JP Gov)

VC

User (Me)

VP

Verifier (Airport)

**Unlimited selective disclosure**

now we can hide all unnecessary information!

**Limited zero-knowledge proofs**

cannot prove relations among attributes in zero-knowledge manner

```
******************
      : Person
*********************
```

isPatientOf

```
***  : Immunization
date = 2021-08-10
*********************
```

vaccineCode

```
******************
******************
   : Vaccine
```

credentialSubject

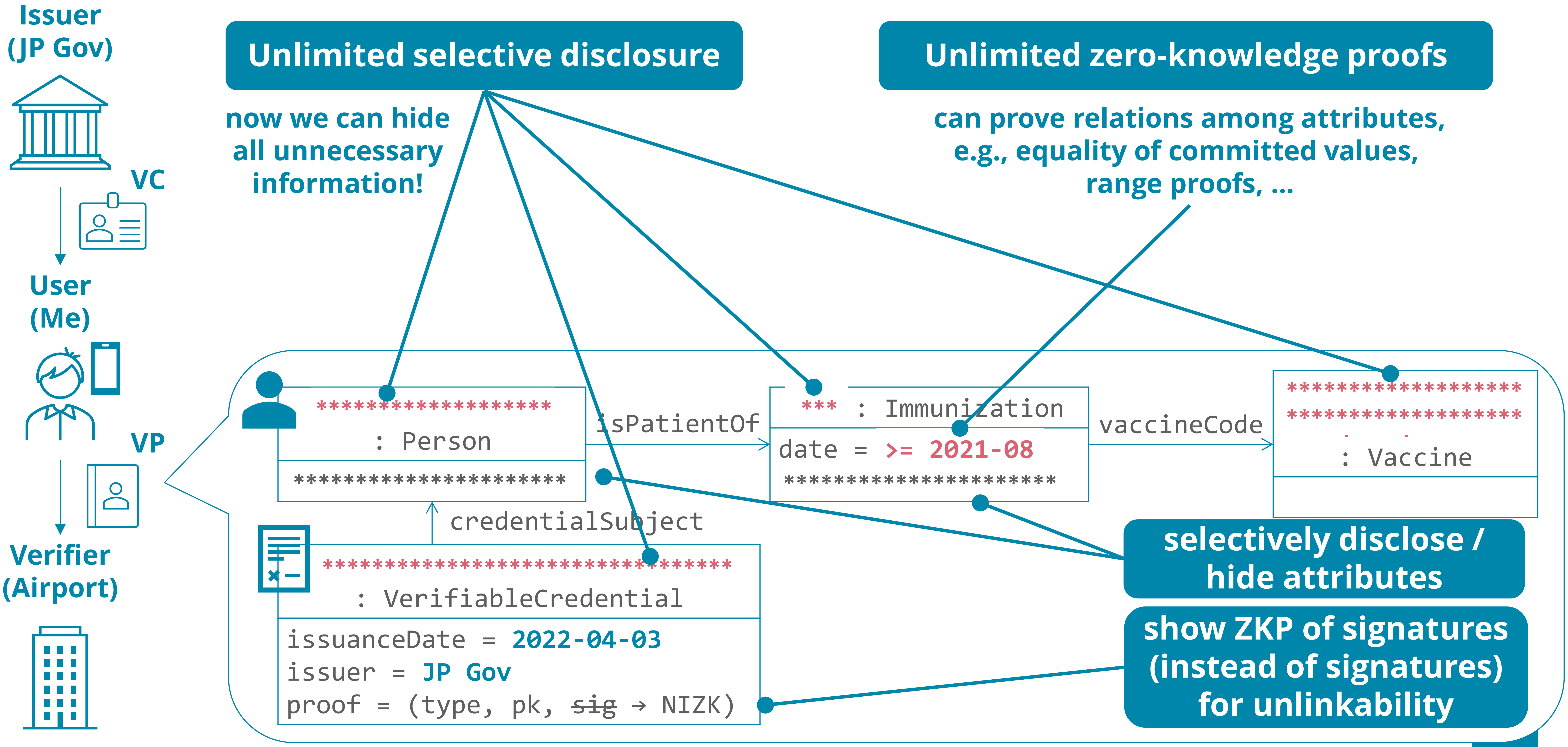
```
********************************
   : VerifiableCredential
issuanceDate = 2022-04-03
issuer = JP Gov
```

proof = (type, pk, ~~sig~~ → NIZK)

**selectively disclose / hide attributes**

**show ZKP of signatures (instead of signatures) for unlinkability**

# Our Contribution



Issuer
(JP Gov)

VC

User
(Me)

VP

Verifier
(Airport)

**Unlimited selective disclosure**

now we can hide
all unnecessary
information!

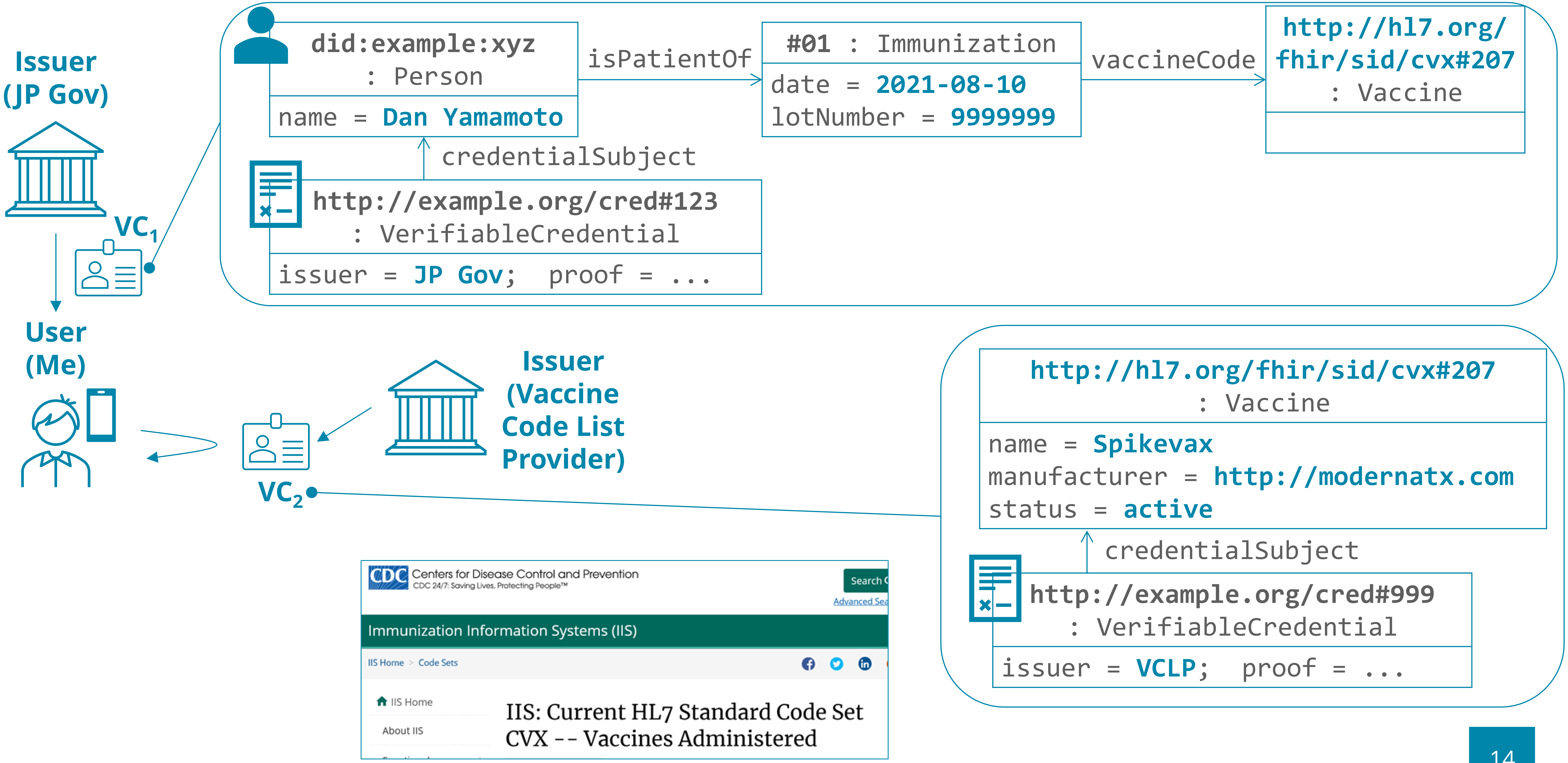
**Unlimited zero-knowledge proofs**

can prove relations among attributes,
e.g., equality of committed values,
range proofs, ...

**selectively disclose / hide attributes**

**show ZKP of signatures (instead of signatures) for unlinkability**

# Possible Future Use Cases



Issuer (JP Gov)

VC$_1$

User (Me)

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

issuer = **JP Gov**; proof = ...

Issuer (Vaccine Code List Provider)

VC$_2$

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

name = **Spikevax**
manufacturer = **http://modernatx.com**
status = **active**

credentialSubject

**http://example.org/cred#999** : VerifiableCredential

issuer = **VCLP**; proof = ...

CDC Centers for Disease Control and Prevention
CDC 24/7: Saving Lives, Protecting People™

Search

Advanced Sea

Immunization Information Systems (IIS)

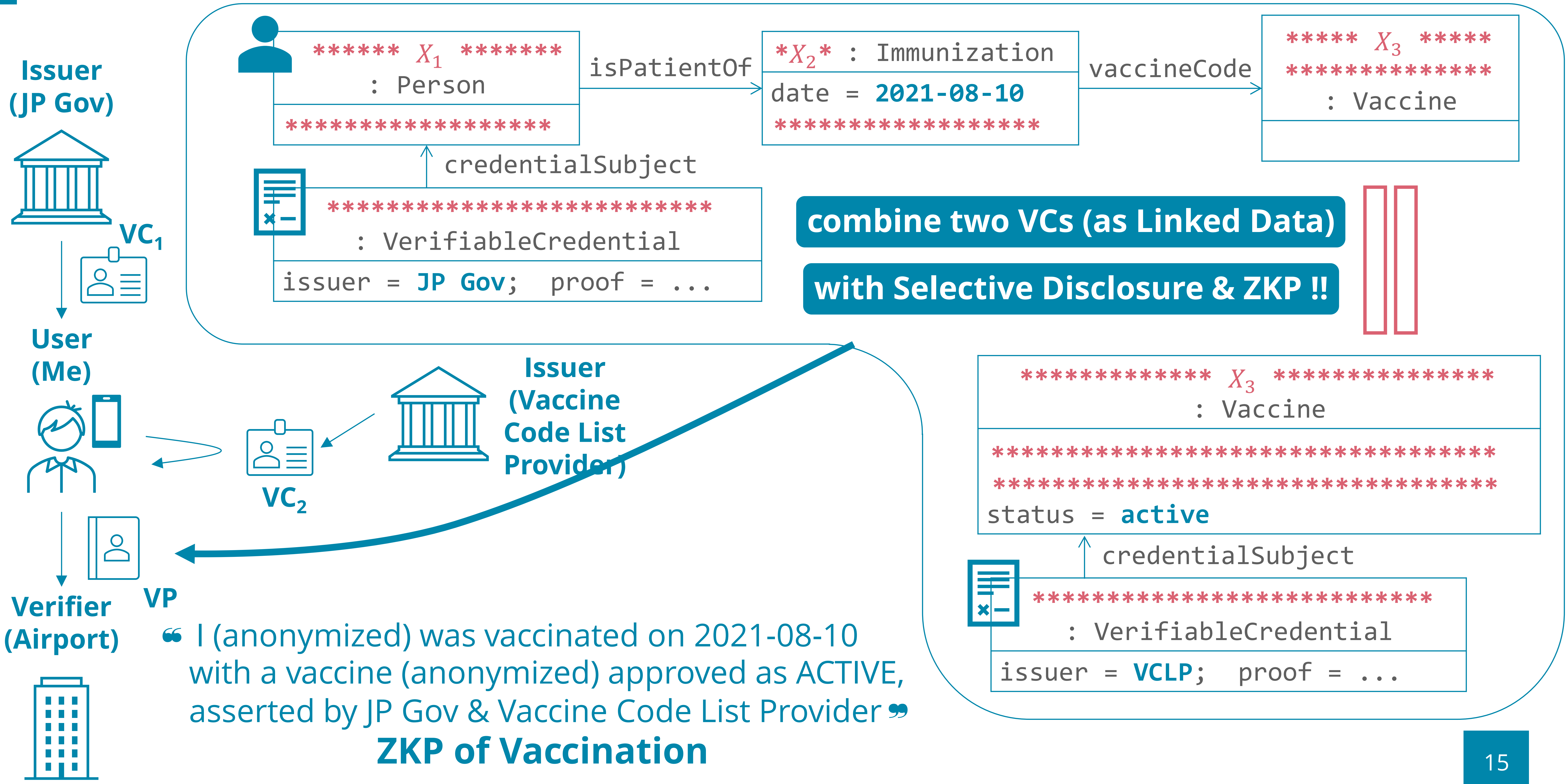
IIS Home > Code Sets

IIS Home

About IIS

IIS: Current HL7 Standard Code Set CVX -- Vaccines Administered

# Possible Future Use Cases



Issuer (JP Gov)

VC$_1$

User (Me)

VC$_2$

Issuer (Vaccine Code List Provider)

Verifier (Airport)

VP

```
****** X1 *******
: Person
******************
```

isPatientOf

```
*X2* : Immunization
date = 2021-08-10
******************
```

vaccineCode

```
***** X3 *****
**************
: Vaccine
```

credentialSubject

```
**************************
: VerifiableCredential
issuer = JP Gov;  proof = ...
```

**combine two VCs (as Linked Data)**

**with Selective Disclosure & ZKP !!**

```
************* X3 ***************
: Vaccine
**********************************
**********************************
status = active
```

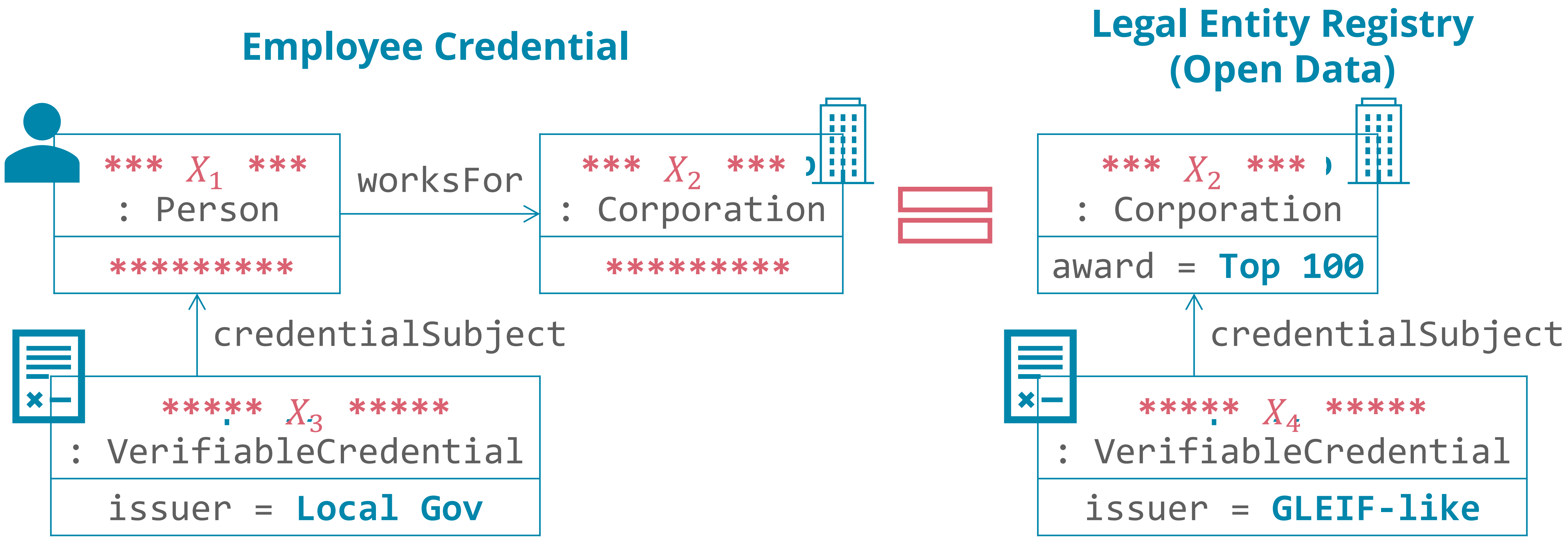
credentialSubject

```
***************************
: VerifiableCredential
issuer = VCLP;  proof = ...
```

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

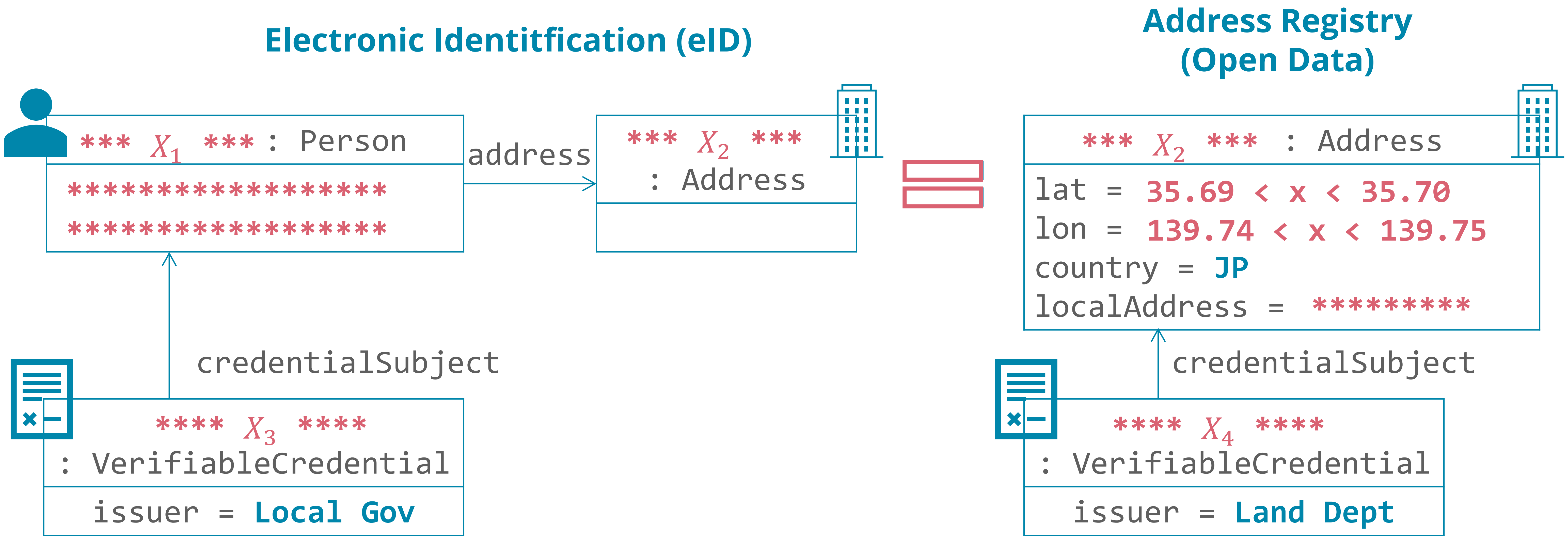
**ZKP of Vaccination**

# 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



**Electronic Identitfication (eID)**

*** $X_1$ *** : Person
*****************
*****************

address

*** $X_2$ ***
: Address

credentialSubject

**** $X_3$ ****
: VerifiableCredential
issuer = **Local Gov**

=

**Address Registry**
**(Open Data)**

*** $X_2$ *** : Address
lat = **35.69 < x < 35.70**
lon = **139.74 < x < 139.75**
country = **JP**
localAddress = *********

credentialSubject

**** $X_4$ ****
: VerifiableCredential
issuer = **Land Dept**

> “ 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

W3C 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

**OpenID Connect for SSI**
(in Progress)

DIF

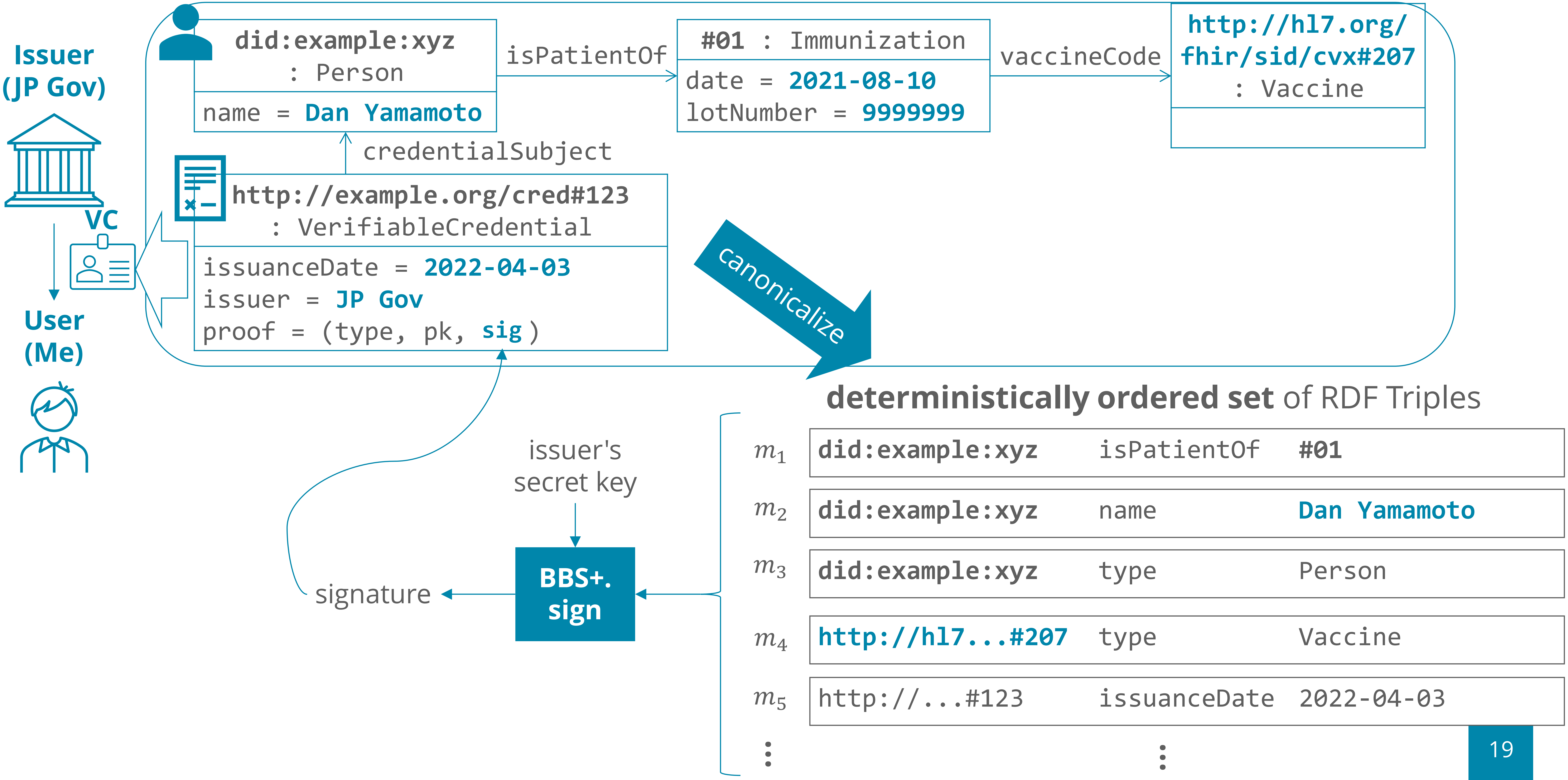
**The BBS Signature Scheme**
(in Progress)

⋮

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

*this work formalizes security & privacy notions for future standardization

# Existing Construction (LDP-BBS+)



Issuer (JP Gov)

VC

User (Me)

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**)

canonicalize

**deterministically ordered set** of RDF Triples

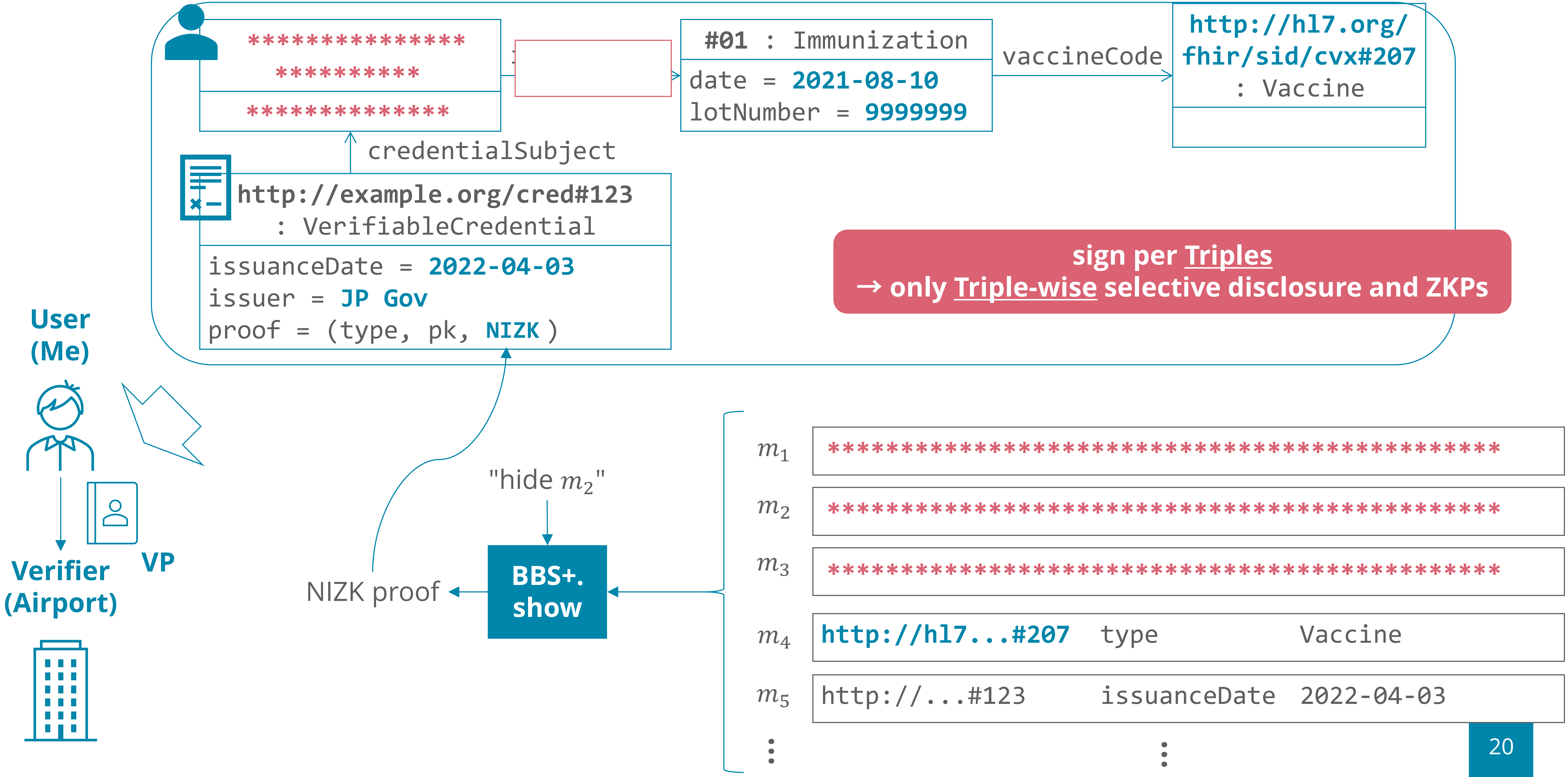
| | | | |
|---|---|---|---|
| $m_1$ | **did:example:xyz** | isPatientOf | **#01** |
| $m_2$ | **did:example:xyz** | name | **Dan Yamamoto** |
| $m_3$ | **did:example:xyz** | type | Person |
| $m_4$ | **http://hl7...#207** | type | Vaccine |
| $m_5$ | http://...#123 | issuanceDate | 2022-04-03 |
| ⋮ |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

issuer's secret key

**BBS+.sign**

signature

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



***************
**********
**************

#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, NIZK )

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

**User (Me)**

**Verifier (Airport)**

**VP**

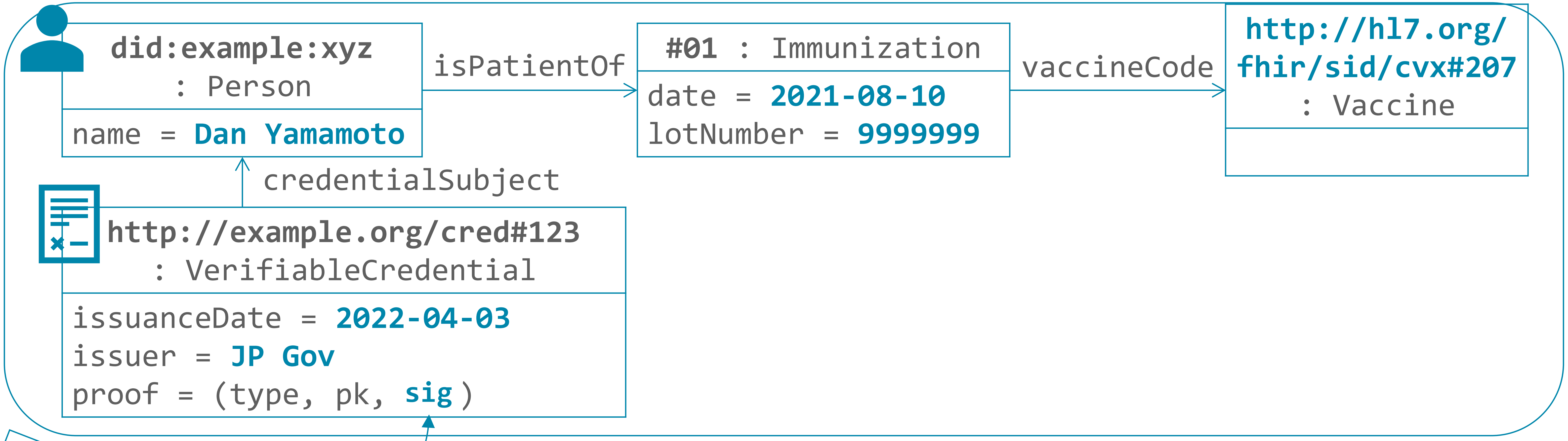
"hide $m_2$"

**BBS+. show**

NIZK proof

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

# Our Construction = **Term-wise** Encoding



did:example:xyz
: Person

name = **Dan Yamamoto**

isPatientOf

**#01** : Immunization

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

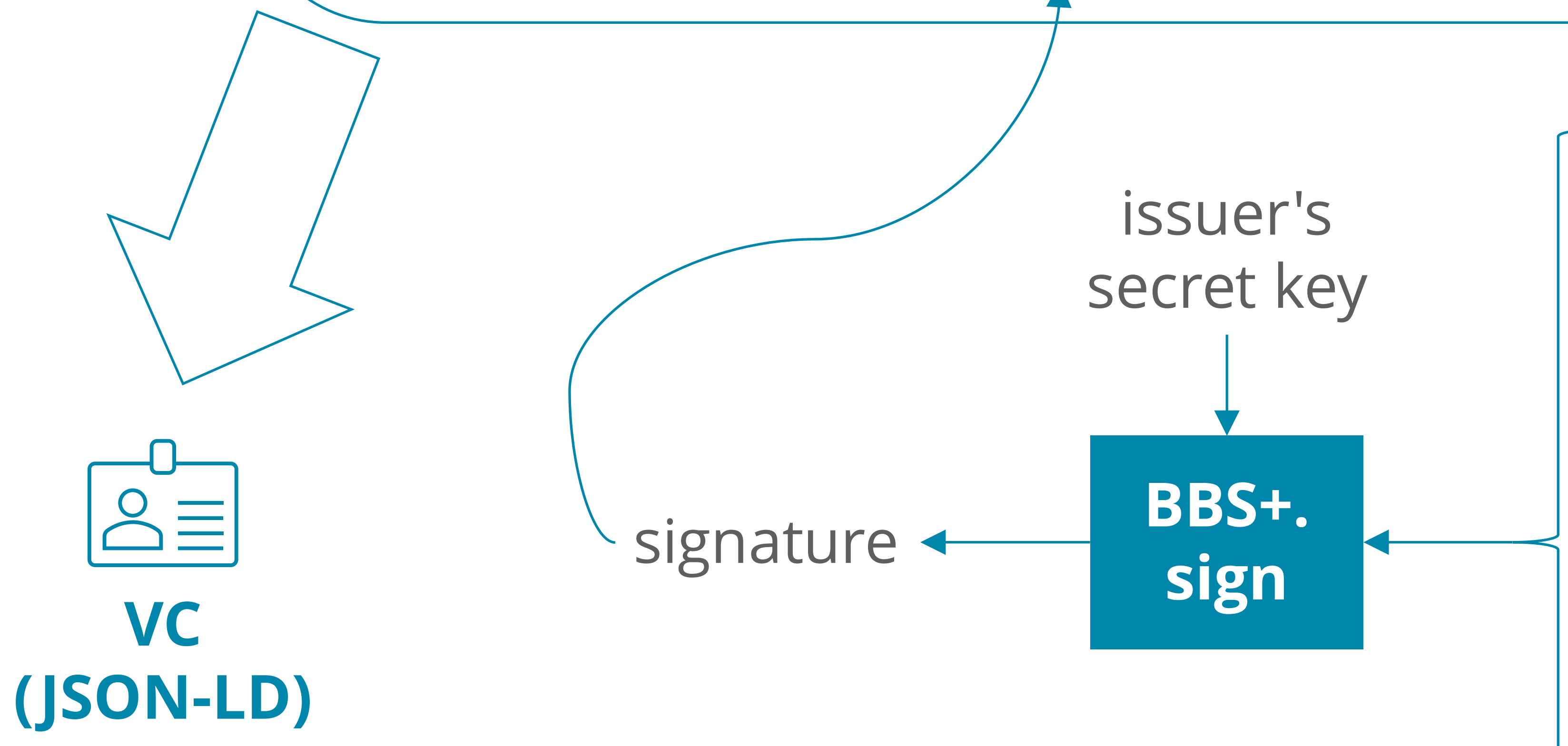
vaccineCode

**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**)



**VC**
**(JSON-LD)**

issuer's
secret key

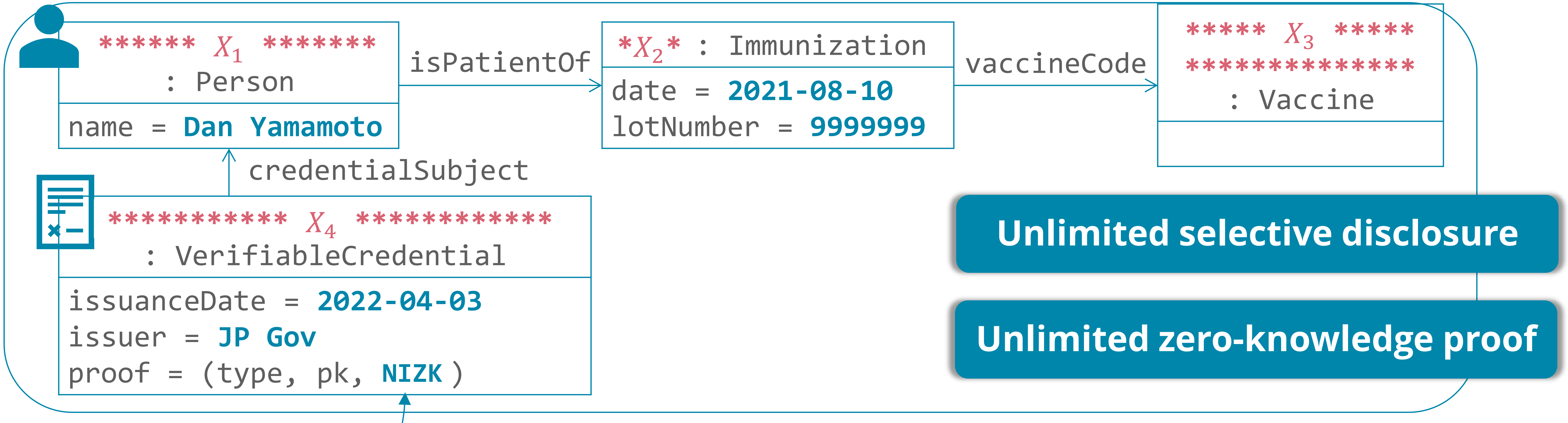
**BBS+.**
**sign**

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 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

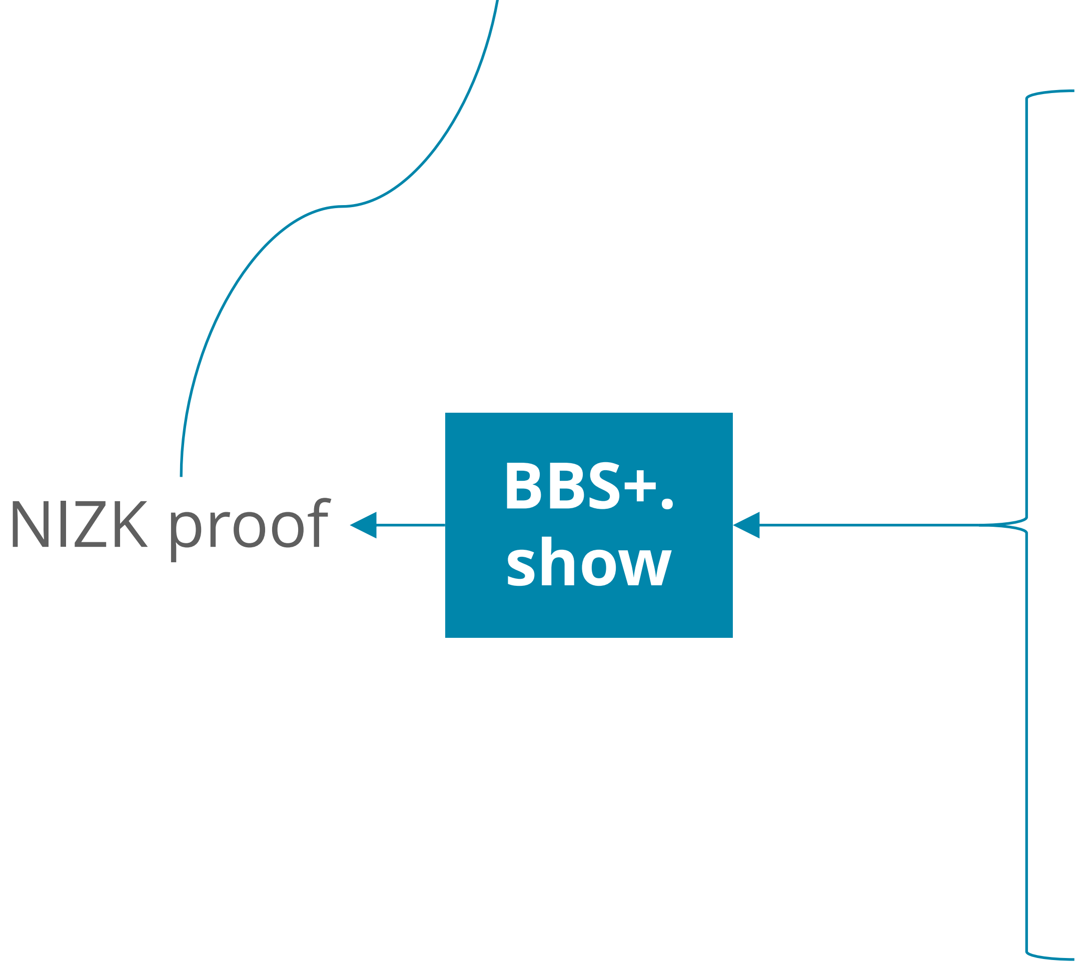
**sign per Terms**
**→ Term-wise selective disclosure and ZKPs**

# Our Construction = **Term-wise** Encoding


****** $X_1$ ******* : Person
name = Dan Yamamoto
isPatientOf
*$X_2$* : Immunization
date = 2021-08-10
lotNumber = 9999999
vaccineCode
***** $X_3$ ***** ************* : Vaccine
credentialSubject
*********** $X_4$ ************ : VerifiableCredential
issuanceDate = 2022-04-03
issuer = JP Gov
proof = (type, pk, NIZK )

**Unlimited selective disclosure**

**Unlimited zero-knowledge proof**



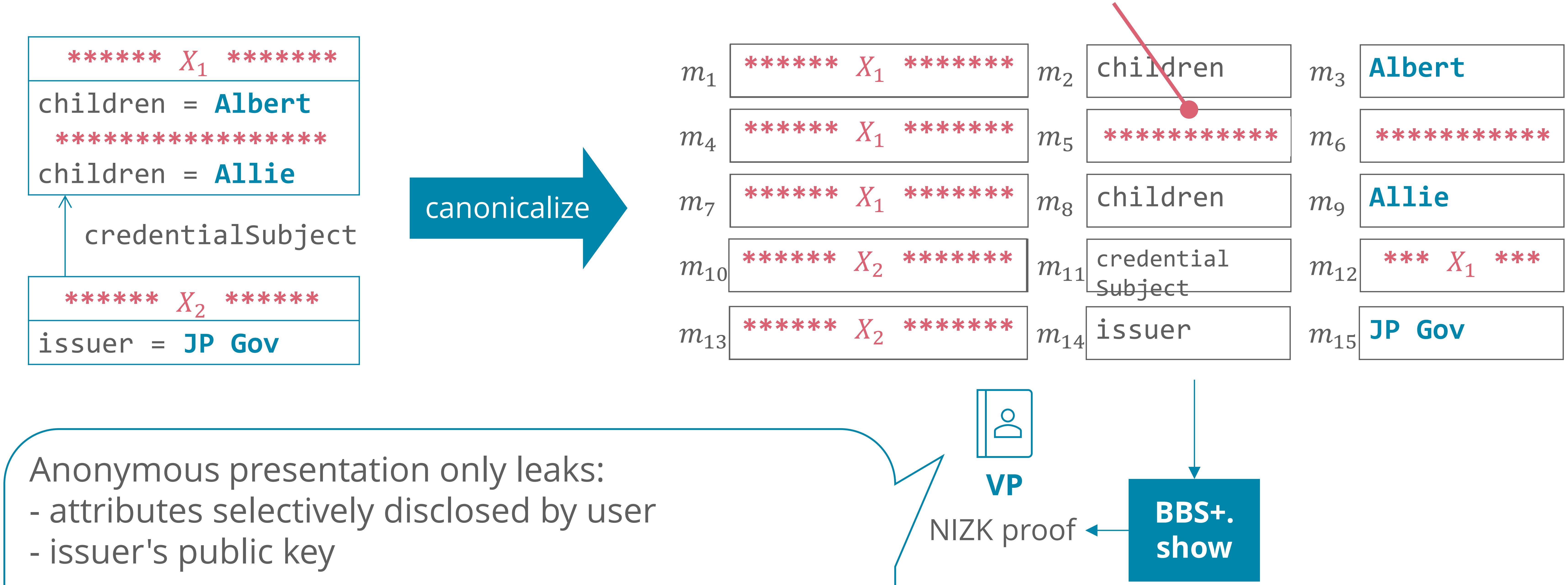
| | | | | | |
|---|---|---|---|---|---|
| $m_1$ | ****** $X_1$ ******* | $m_2$ | isPatientOf | $m_3$ | #01 |
| $m_4$ | ****** $X_1$ ******* | $m_5$ | name | $m_6$ | Dan Yamamoto |
| $m_7$ | ****** $X_1$ ******* | $m_8$ | type | $m_9$ | Person |
| $m_{10}$ | ****** $X_3$ ******* | $m_{11}$ | type | $m_{12}$ | 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

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



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

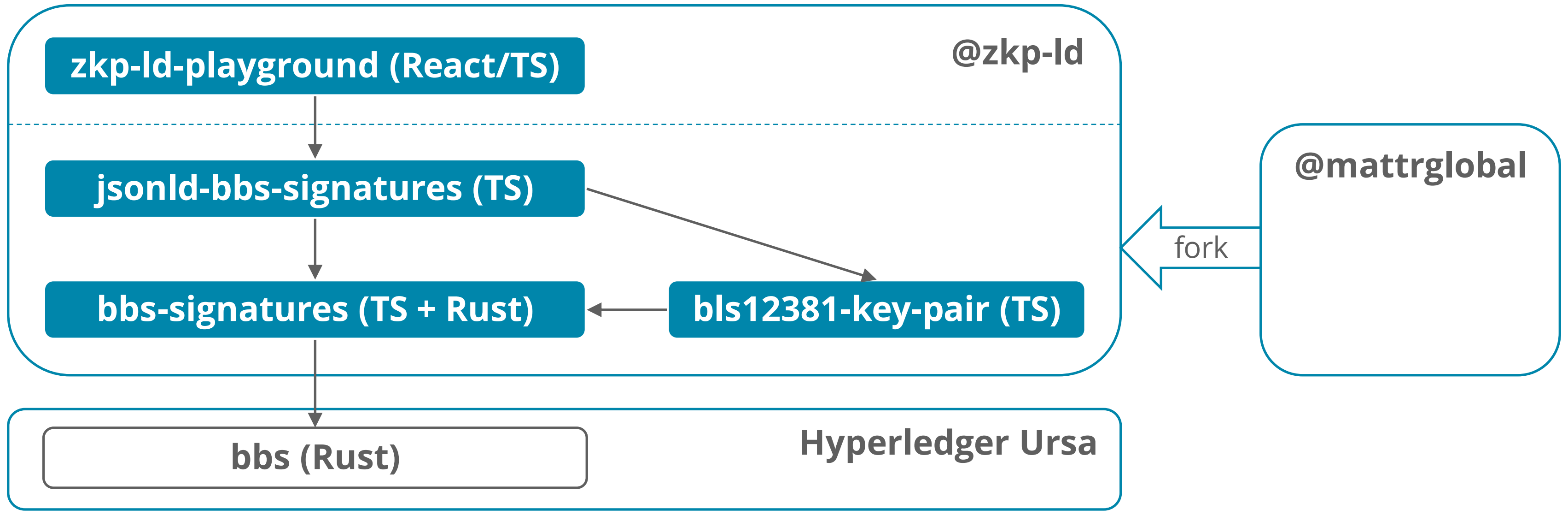
Weakly anonymous presentation additionally leaks:
- total number of attributes: $|\{m_i\}| = 15$
- index $i$ of canonicalized attributes $\{m_i\}$

**workarounds:**
**add dummy attributes**
**& random permutations**

# Implementations and Demo

## Implementations (published on Github and npm)

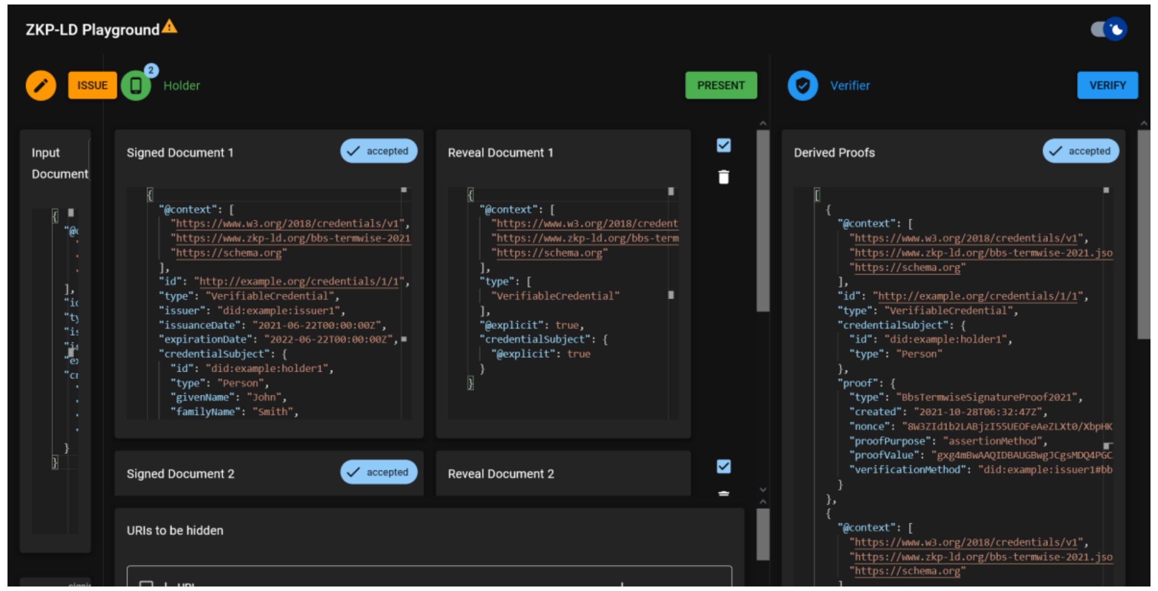
- @zkp-ld/jsonld-signatures-bbs
- @zkp-ld/bls12381-key-pair
- @zkp-ld/bbs-signatures



@zkp-ld
zkp-ld-playground (React/TS)
jsonld-bbs-signatures (TS)
bbs-signatures (TS + Rust)
bls12381-key-pair (TS)
fork
@mattrglobal
bbs (Rust)
Hyperledger Ursa

## 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



Signed Document 1

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.zkp-ld.org/bbs-termwise-2021
    "https://schema.org"
  ],
  "id": "http://example.org/credentials/1/1",
  "type": "VerifiableCredential",
  "issuer": "did:example:issuer1",
  "issuanceDate": "2021-06-22T00:00:00Z",
  "expirationDate": "2022-06-22T00:00:00Z",
  "credentialSubject": {
    "id": "did:example:holder1",
    "type": "Person",
    "givenName": "John",
    "familyName": "Smith",
```

Reveal Document 1

```
{
  "@context": [
    "https://www.w3.org/2018/credent
    "https://www.zkp-ld.org/bbs-term
    "https://schema.org"
  ],
  "type": [
    "VerifiableCredential"
  ],
  "@explicit": true,
  "credentialSubject": {
    "@explicit": true
  }
}
```

Derived Proofs

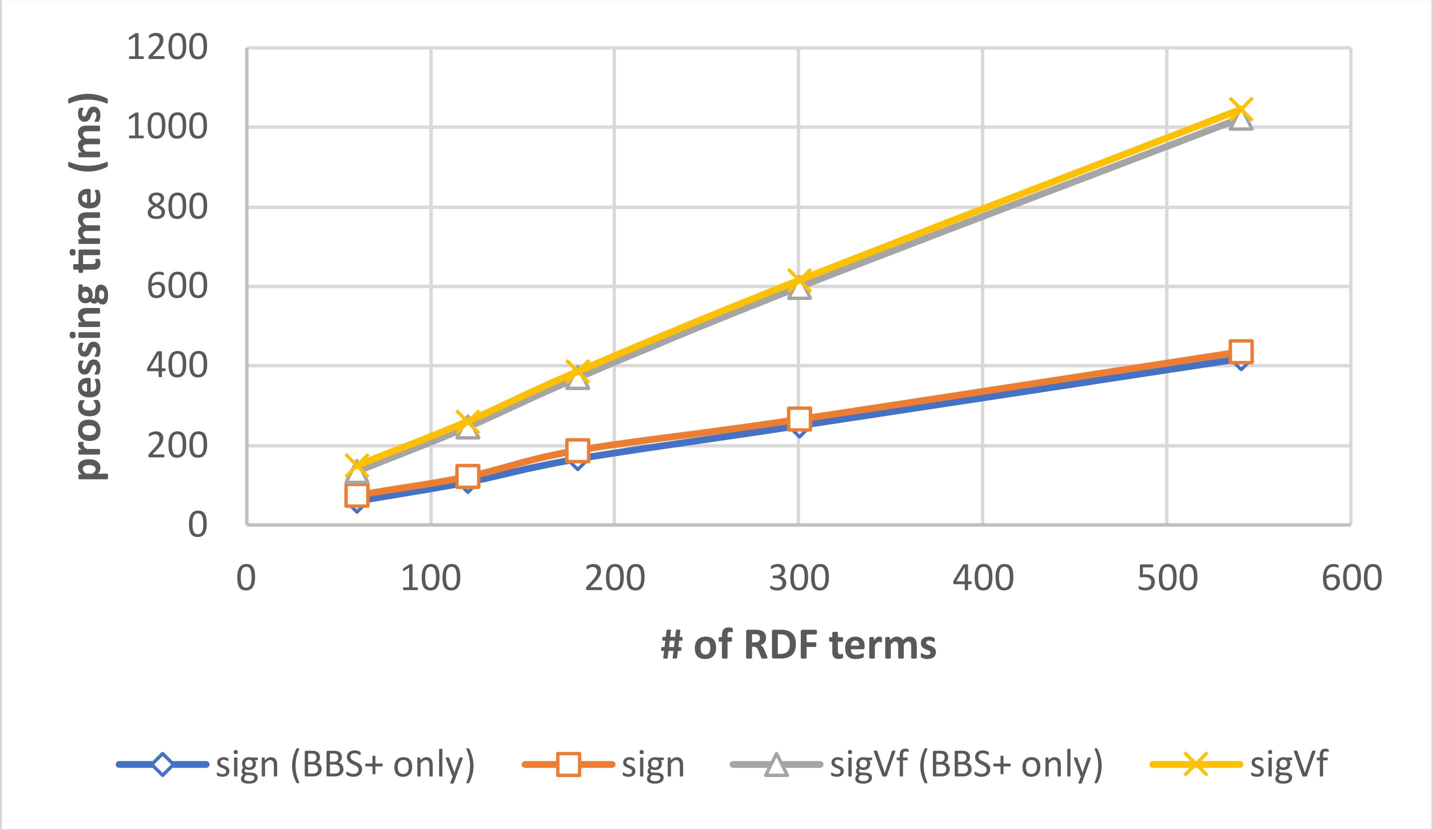
```
[
  {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.zkp-ld.org/bbs-termwise-2021.jso
      "https://schema.org"
    ],
    "id": "http://example.org/credentials/1/1",
    "type": "VerifiableCredential",
    "credentialSubject": {
      "id": "did:example:holder1",
      "type": "Person"
    },
    "proof": {
      "type": "BbsTermwiseSignatureProof2021",
      "created": "2021-10-28T06:32:47Z",
      "nonce": "8W3ZId1b2LABjzI55UEOFeAeZLXt0/XbpHK
      "proofPurpose": "assertionMethod",
      "proofValue": "gxg4mBwAAQIDBAUGBwgJCgsMDQ4PGC
      "verificationMethod": "did:example:issuer1#bb
    }
  },
  {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.zkp-ld.org/bbs-termwise-2021.jso
      "https://schema.org"
```

# Performance Evaluation

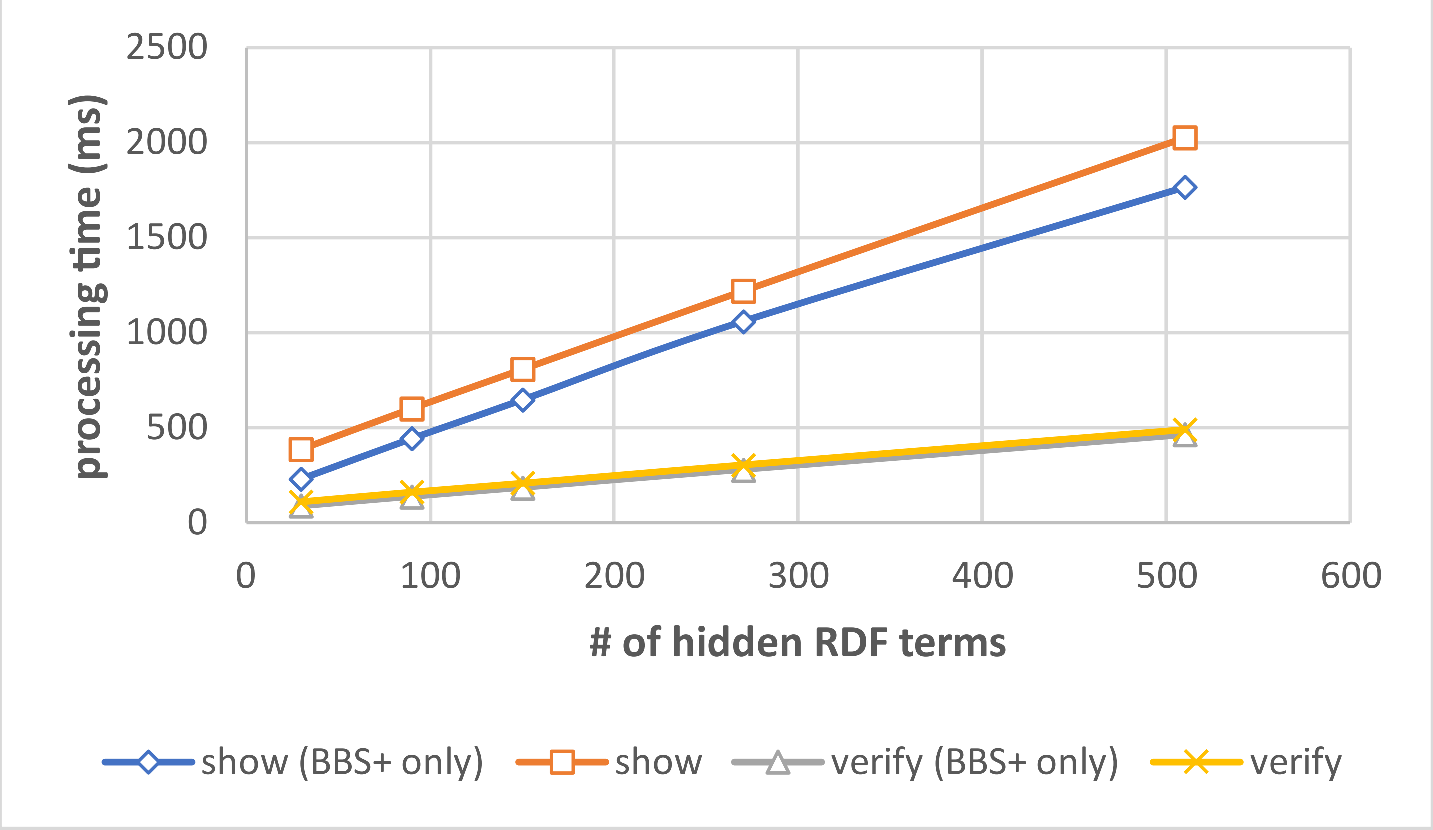
| | size (bits) |
|---|---|
| secret key | 256 |
| public key | 768 |
| signature | 896 |
| proof | $2944 + 256\,n$ |

($n$ : # 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