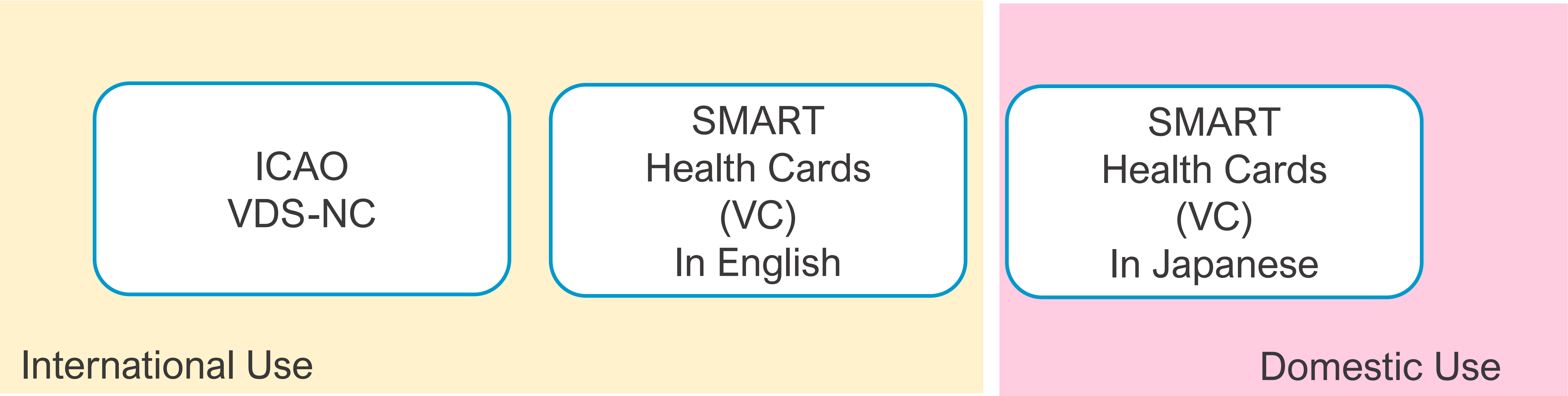
Joint ITU/WHO Workshop on
“Future of Verifiable Health Credentials Beyond
2023.9.11

Selective Disclosure for Privacy

Kazue Sako
Dept. Computer Science and Engineering
Waseda University

COVID-19 Vaccination Certificates in Japan



ICAO
VDS-NC

SMART
Health Cards
(VC)
In English

International Use

SMART
Health Cards
(VC)
In Japanese

Domestic Use

More than 22M certificates has been issued by Aug. 27, 2023.

https://www.mhlw.go.jp/stf/covid-19/certificate.html

VC: Verifiable Credentials

Claims signed by Issuer (Japanese Government)

1. Vaccinated person’s information: name, date of birth, etc.
2. Vaccination record: type of vaccine, date of vaccination, etc.
3. Passport number and Nationality

Digital signature of Japanese Government

For Future VC: Verifiable Credentials

Claims signed by Issuer (Japanese Government)

1. Vaccinated person’s information: name, date of birth, etc.
2. Vaccination record: type of vaccine, date of vaccination, etc.
3. Passport number and Nationality

Digital signature of Japanese Government

Do I have to disclose my passport number just to show I am vaccinated?

Issues with ordinary digital signatures

Claims signed by Issuer (Japanese Government)

1. Vaccinated person's information: name, date of birth, etc.
2. Vaccination record: type of vaccine, date of vaccination, etc.
3. Passport number and Nationality

Digital signature of Japanese Government

I need to disclose all my info on the credential to verify the signature

New type of digital signatures (eg. BBS + Signatures)

Claims signed by Issuer (Japanese Government)

1. Vaccinated person’s information: name, [redacted] etc.
2. Vaccination record: type of vaccine, date of vaccination, etc.
3. [redacted]

Digital signature of Japanese Government

I can hide some of my info and still the signature can be verified!

Selective Disclosure

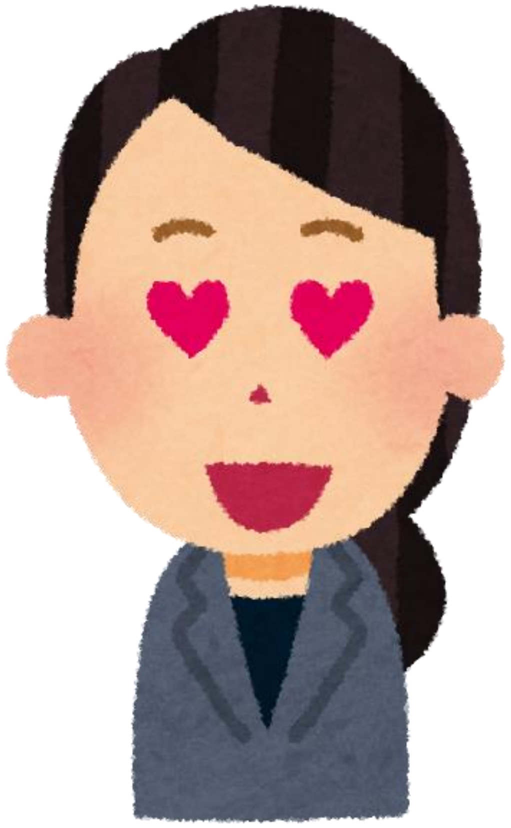
New type of digital signatures (eg. BBS + Signatures)

Claims signed by Issuer (Japanese Government)

1. Vaccinated person’s information: name, date of birth, etc.
2. Vaccination record: type of vaccine, date of vaccination, etc.
3. [redacted]

Digital signature of Japanese Government

I can hide my date of birth yet prove I am 20+ and still the signature can be verified!



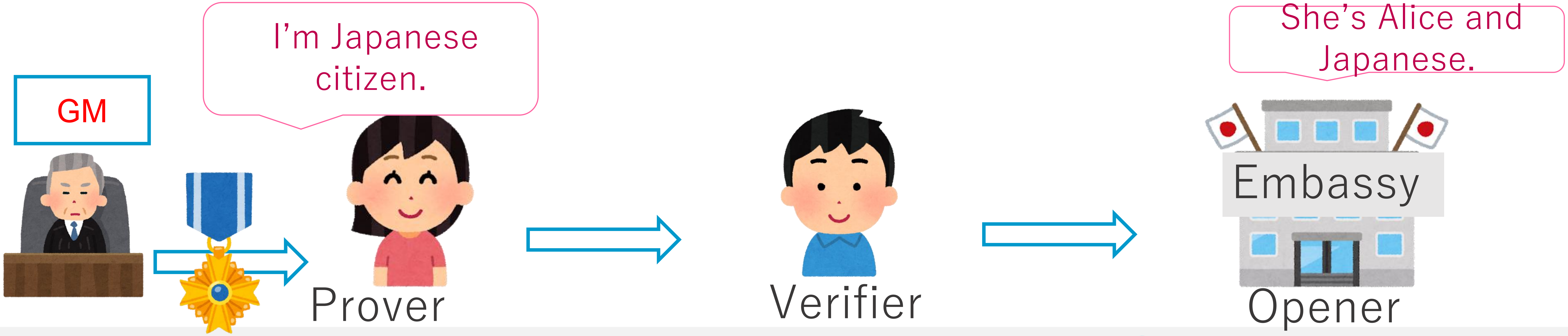
Predicate Proofs

Don’t think of continuation of paper certificates.
Digital Certificates can do more.

Start from what we want to have,
Not what we already have.

ISO/IEC 29191-2013:
Requirements for Partially Anonymous, Partially Unlinkable Authentication

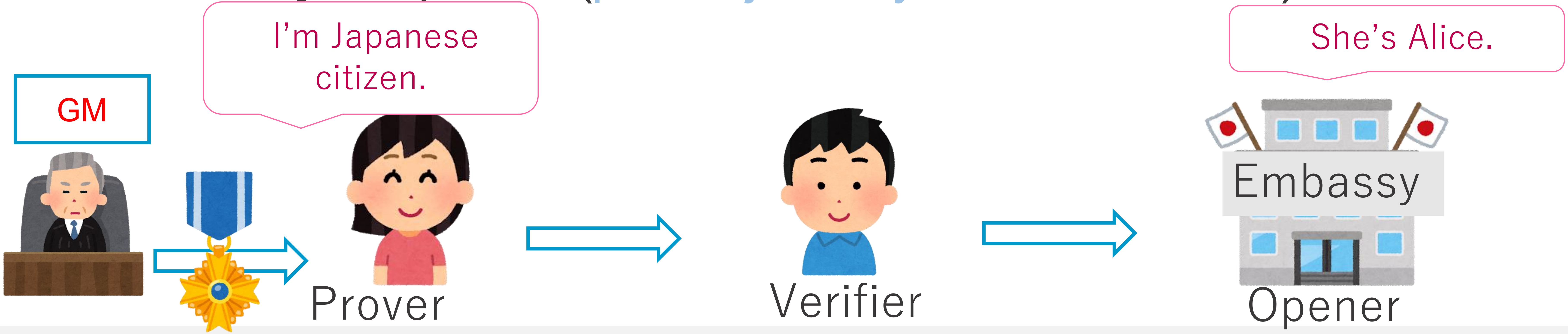
This protocol allows Alice(Prover) to prove some thing to Designated Officer(Opener) while showing its subset to Bob(Verifier) who is in between Alice and Opener.



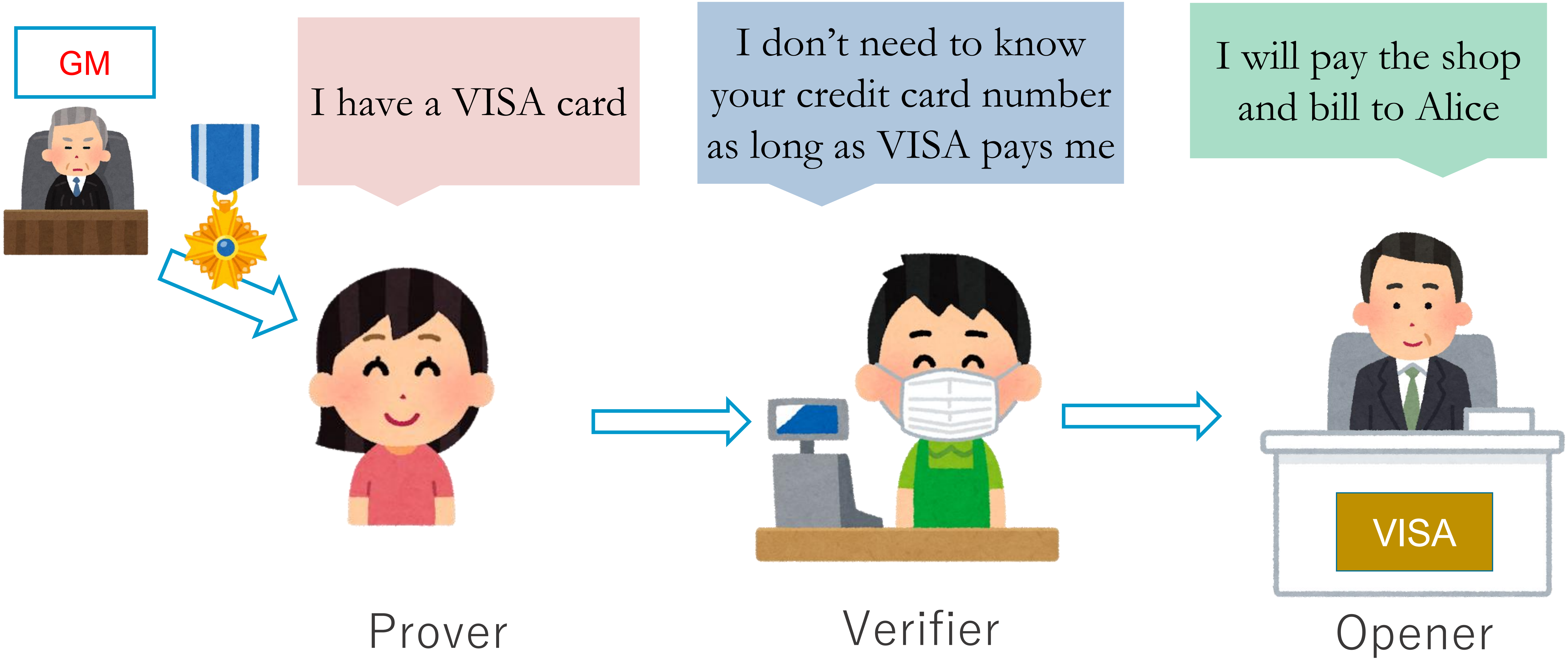
ISO/IEC 29191-2013:
Requirements for Partially Anonymous, Partially Unlinkable Authentication

Group Manager issues membership certificates to users

1. User can prove he/she belongs to the group without disclosing any information that can be used to identify/trace him/her. (anonymous/unlinkable)
2. User can designate an opener who can later identify the prover (partially anonymous/unlinkable)



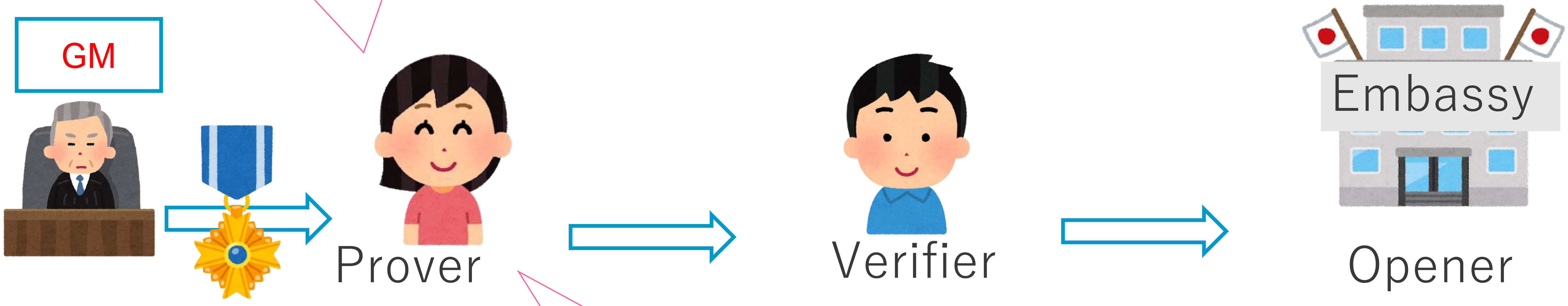
ISO 29191-2013: Usecases
Requirements for Partially Anonymous, Partially Unlinkable Authentication


GM
I have a VISA card
I don't need to know your credit card number as long as VISA pays me
I will pay the shop and bill to Alice
VISA
Prover
Verifier
Opener

Combining ISO 29191-2013 and Selective Disclosure

Alice only wants to show a subset of information on credentials

Alice can disclose a larger set of claims to Opener while showing only its subset to Bob.



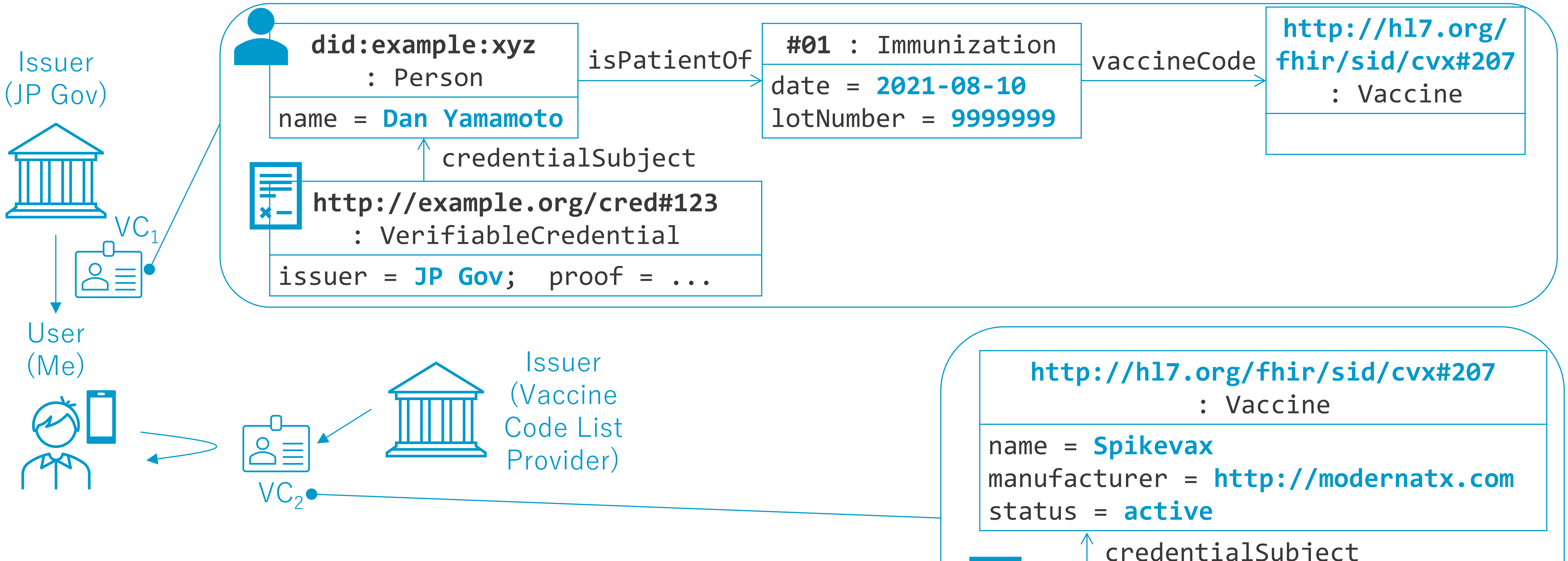
But Verifier can later forward it to Opener to learn more details

More flexible use of digital credentials

Using Linked Data format for credentials, we can link data!

(slides borrowed from my co-author)

Possible Future Use Cases



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

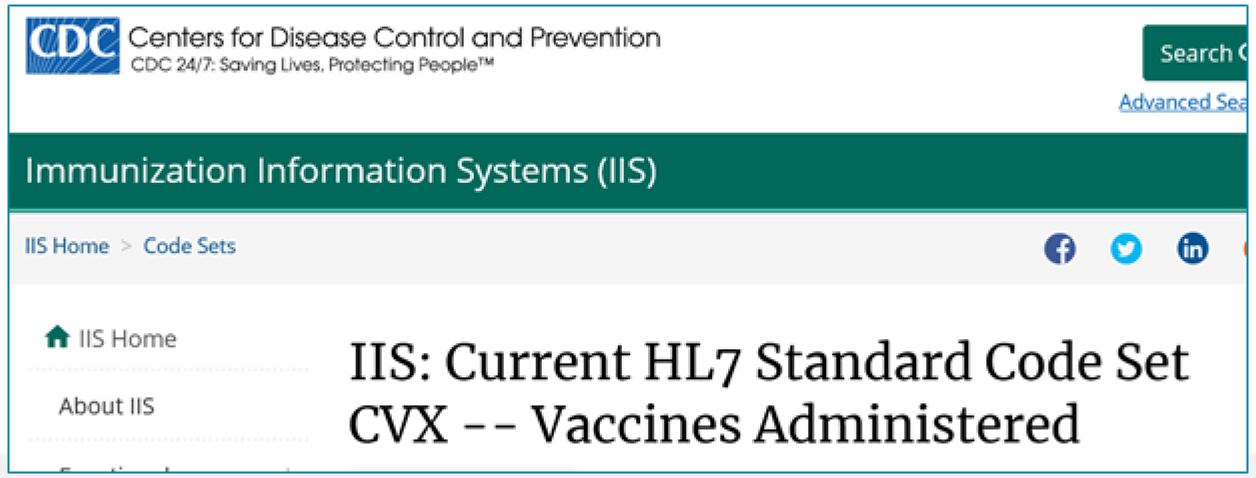
credentialSubject

http://example.org/cred#123
: VerifiableCredential
issuer = **JP Gov**; proof = ...

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™

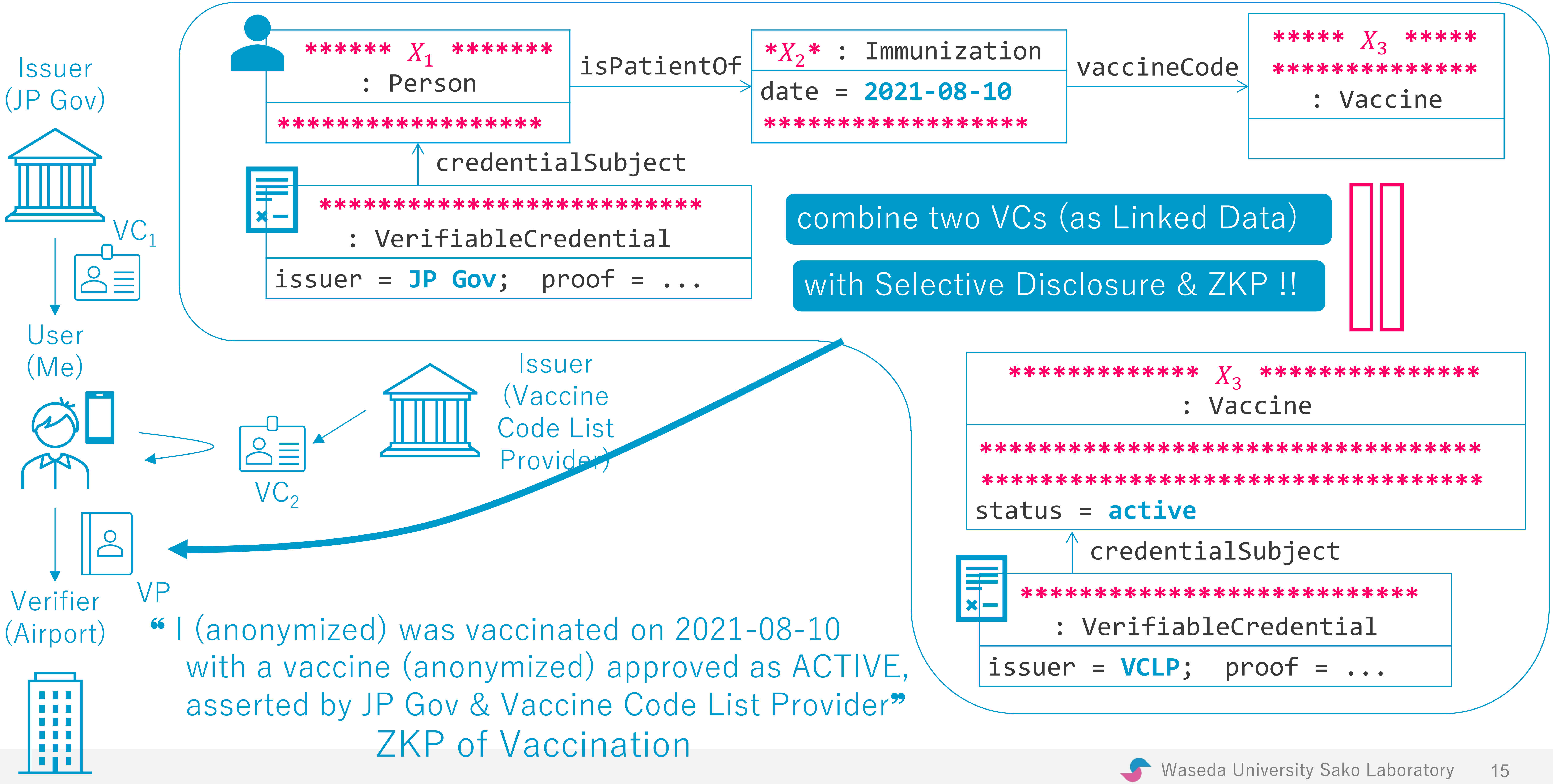
Immunization Information Systems (IIS)

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)

Issuer (Vaccine Code List Provider)

VC_2

Verifier (Airport)

VP

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

isPatientOf

X_2 : Immunization
date = **2021-08-10**
****

vaccineCode

***** X_3 *****
****
: Vaccine

credentialSubject

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

combine two VCs (as Linked Data)

with Selective Disclosure & ZKP !!

************ X_3 **************
: 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

Summary:

- Verifiable credentials are great tool to authenticate claims made by authority
- However, ordinary digital signatures restricts its use: show everything on the credentials or nothing
- New technology using new digital signatures allows
  - Selective Disclosure
  - Predicate proofs

  to achieve minimum disclosure for privacy
- Combining with ISO29191 allows more flexible flow of authorized data
- Start from what we want to have, not from what we already have.

Thank you for your attention!