2024 コンピュータセキュリティシンポジウム
ブロックチェーンワークショップ BWS

SSI / DID よりVC でしょ

早稲田大学基幹理工学部情報理工学科
佐古和恵

謝辞：井口さん

今日のメッセージ

SSI、DIDはなんだと思っていますか？

概念だとしたらどんな概念？
技術だとしたらどんな技術？
マーケティングワードになっていませんか？

公開鍵暗号技術のメリットを社会に普及させるとしたら、
標準的なVC（＆VP）のフォーマットを普及させるべきでは？

自己紹介 佐古和恵　早稲田大学 理工学術院　教授

- 大学理学部(数学)卒業後, NECに入社.
- ISO/IEC JTC 1 WG2, WG5 国際エキスパート、W3C RCH-WG Invited Expert
- 第26代日本応用数理学会会長、2017-8年度電子情報通信学会副会長、2021-2年度　情報処理学会理事
- 国際会議Asiacrypt, CT-RSA, FC, PKC, ESORICS, ACNS, AsiaCCS 等プログラム委員長.
- FC Steering committee, FC　2013, 2025 実行(共同)委員長

Financial Cryptography and Data Security 2025
April 14-18, 2025
Miyako Island, Japan

Third time in Asia in its 29 years history

SHIGIRA RESORT
SEVEN MILES

Famous for Miyako Bue

シギラセブンマイルズ
リゾート

Venue (Variety of seven hotels)

Lots of activities















※チームビルディングのお時間帯/ご料金については営業担当へお問い合わせください。

See you in Miyako Island Next April

http://fc25.ifca.ai

Home

Call for Papers

Sponsorship

Code of Conduct

Financial Cryptography and Data Security 2025

Twenty-Ninth International Conference
14–18 April 2025
Hotel Shigira Mirage
Miyakojima, Japan

Program Chairs Christina Garman
Pedro Moreno-Sanchez

General Chairs Rafael Hirschfeld
Kazue Sako

自己紹介 佐古和恵　早稲田大学 理工学術院　教授

- 大学理学部（数学）卒業後, NECに入社.
- ISO/IEC JTC 1 WG2, WG5 国際エキスパート、W3C RCH-WG Invited Expert
- 第26代日本応用数理学会会長、2017-8年度電子情報通信学会副会長、2021-2年度　情報処理学会理事
- 国際会議Asiacrypt, CT-RSA, FC, PKC, ESORICS, ACNS, AsiaCCS 等プログラム委員長.
- FC Steering committee, FC　2013, 2025 実行(共同)委員長
- 一般社団法人MyDataJapan副理事長
- 内閣官房 Trusted Web推進委員会TFメンバー、
- デジタル庁 DIWアドバイザリーボード構成員、
- 経産省 Web3.0・ブロックチェーンを活用したデジタル公共財等構築実証事業
  スペシャルアドバイザー
- 金融庁　金融審議会、デジタル・分散型金融への対応のあり方等に関する研究会
- **2016-2020 Sovrin Foundation Board of Trustee**

黒歴史 2022.5.20

DPF研究会
2022.5.20

DXとトラストと検証可能性

早稲田大学基幹理工学部情報理工学科
佐古和恵

黒歴史　p44

私が実現したいこと

Self-Sovereign Identity 自己主権型アイデンティティ　DID/VC

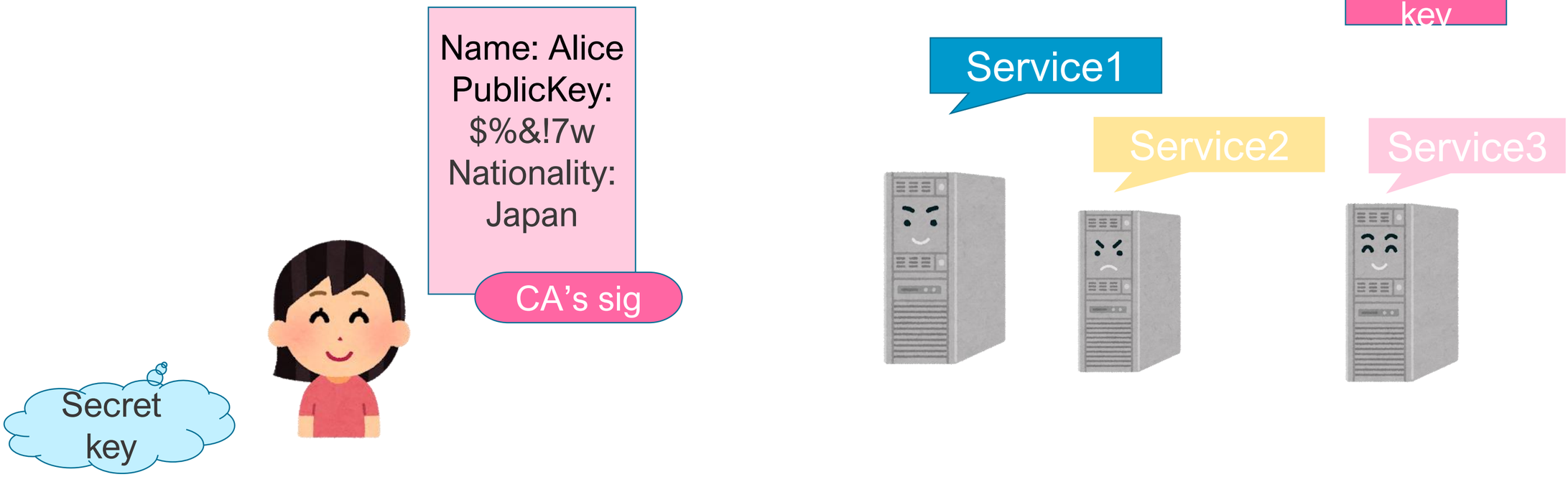
W3C World Wide Web Consortium
Distributed Identifiers WG (DID)
Verifiable Credentials WG (VC)

HYPERLEDGER INDY

sovrin

Self-sovereign Identityの実現方法 DID+VC

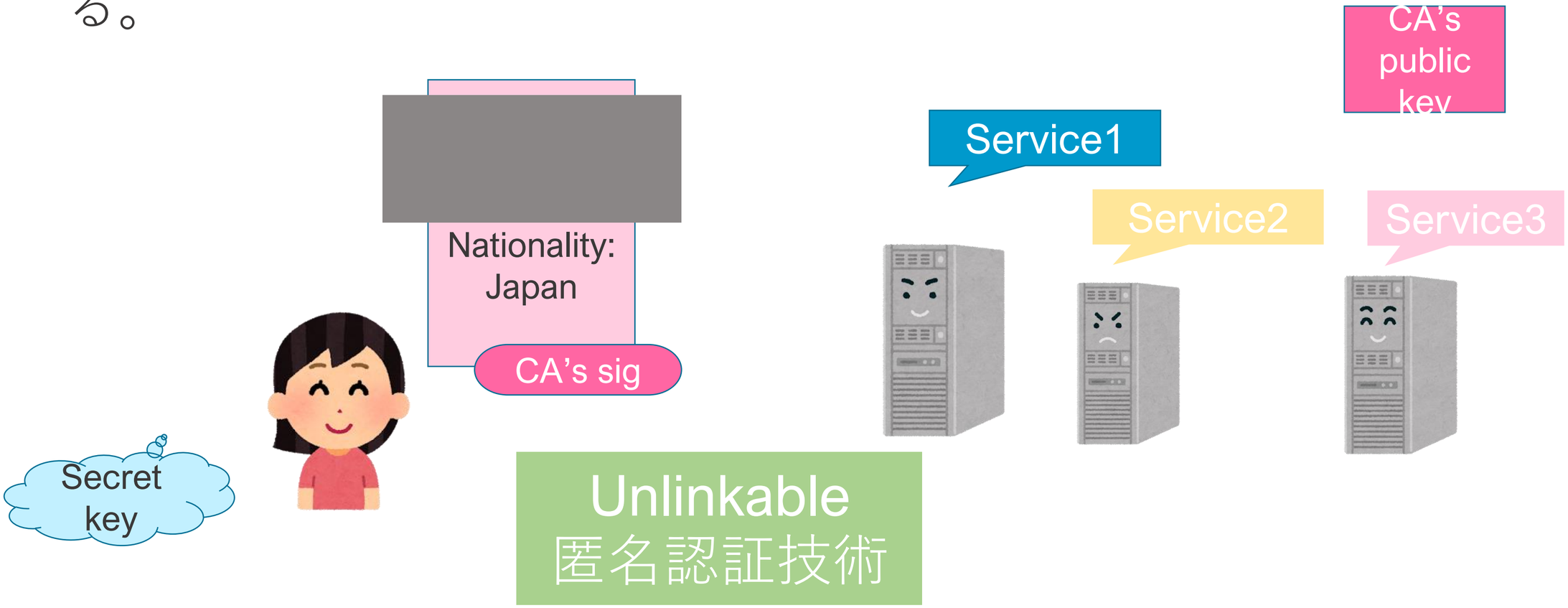
自分の公開鍵＋秘密鍵（Distributed Identifier)
に、保証された属性(Verifiable Credentials)をそれぞれ付与して、必要に応じて必要なだけの属性を開示する。



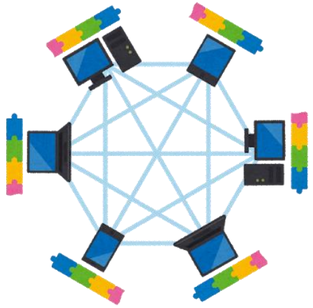
Self-sovereign Identityの実現方法 DID+VC

自分の公開鍵＋秘密鍵（Distributed Identifier)

に、保証された属性(Verifiable Credentials)をそれぞれ付与して、必要に応じて必要なだけの属性を開示する。



CA’s public keys on blockchain!



CA’s public key

CA’s public key

CA’s public key

CA’s public key

Name: Alice
PublicKey:
$%&!7w

CA’s sig

Name: Alice
PublicKey:
$%&!7w
Nationality:
Japan

CA’s sig

Name: Alice
PublicKey:
$%&!7w
Graduated from
Waseda

CA’s sig

Secret key

Name: Alice
PublicKey:
$%&!7w
Resident of
Tokyo

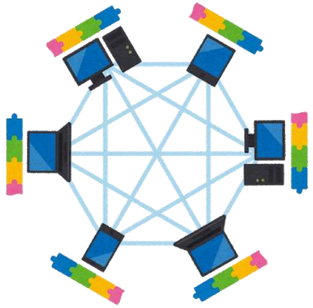
CA’s sig

Service1

Service2

Service3

CA’s public keys on blockchain!



CA’s public key

CA’s public key

CA’s public key

CA’s public key

[redacted]

CA’s sig

[redacted]

Nationality: Japan

CA’s sig

[redacted]

Graduated from Waseda

CA’s sig

Secret key

[redacted]

Resident of Tokyo

CA’s sig

Service1

Service2

Service3

選択開示

European Union Agency for Cybersecurity(enisa) レポート 2022.1.20

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Search for resources, tools, publications and more

English (en)

TOPICS PUBLICATIONS TOOLS NEWS EVENTS ABOUT WORK WITH ENISA CONTACT

Home › Publications › Digital Identity: Leveraging the SSI Concept to Build Trust

Topic

› Trust Services

Keywords

Identity & Trust

Digital Identity: Leveraging the SSI Concept to Build Trust

The maintenance of continuity in social life, businesses and administration has accelerated the reflection on the possibility of a need for such decentralised electronic identity. This report explores the potential of self-sovereign identity (SSI) technologies to ensure secure electronic identification and authentication to access cross-

Recommended publications

Remote Identity Proofing - Attacks & Countermeasures

Remote identity proofing is a crucial element in creating trust for digital services. The present study analyses the collection and validation of...

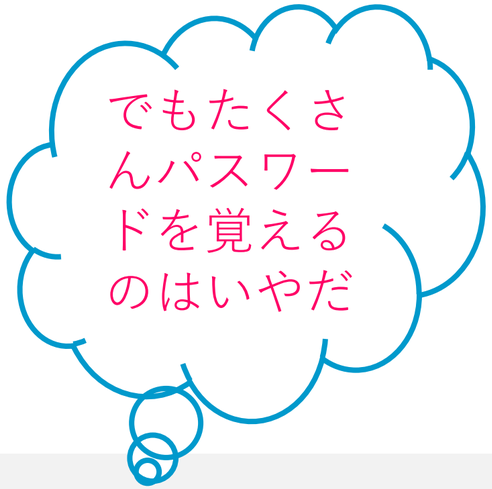
Published on January 20, 2022

https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust

黒歴史の言い訳

言い訳

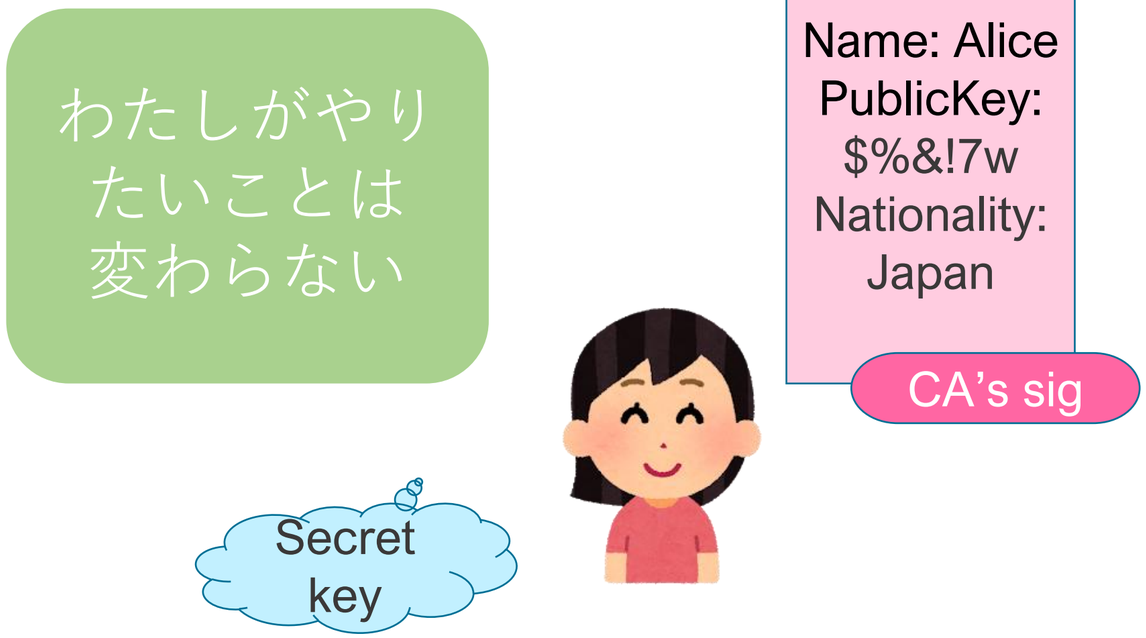
- 2022年当時、Self-sovereign Identityという言葉がかっこいいと思っていた
- Self-sovereign でないIdentityとはGoogle, Facebook, Twitter（現X）の「ID/パスワード」（認証技術）でソーシャルログインすることだと思っていた。
    - いつアカウントを使ったかを把握される
    - いつでもアカウントをバンされる
    - パスワードを知られているのでなりすまされる



~~Self-sovereign Identityの実現方法 DID+VC~~

自分の公開鍵＋秘密鍵 ~~(Distributed Identifier)~~

に、保証された属性(Verifiable Credentials)をそれぞれ付与して、必要に応じて必要なだけの属性を開示する。



じゃあ Self-Sovereignってなんなの？

Discloaimer:　私見です。

Self-Sovereign

- 「自己主権」というけど、何に対する主権？
- ネットでググるとさまざまな解釈がされている
- 「*Self-Sovereign Identity* (SSI) describes an **approach in which the individual should be able to control and manage his or her digital identity, without the intervention of a third-party administrative authority.**」

  https://en.archipels.io/post/self-sovereign-identity-everything-you-need-to-know

  自分の名前も自由に変えられるということ？マイナンバーカードは政府管理だからNG？
- 自分が自分のID Providerになればそれは自己主権かも。

  例：Self-Issued OpenID Provider （SIOP)

  自分の名前も自由に変えられる点で信頼されにくくなる

Self-Sovereign（私見です）

- 「自己主権」が必要なのは政府に迫害されているような難民の人。（多少の文句はありつつも政府にぬくぬく守られているわが国でのシステムを言うのはどうよ？）
- 自分は自由に決めたいけど相手が自由に決めたり変えたりするのは困るユースケースもよく扱っていない？
- 「主権」が暗黙のうちに限定されているユースケースなのであれば、誤解を防ぐためにもSSIっていうのはやめませんか、という提案
  - NFTも「限られたお皿」の上では「唯一無二」かもしれないけど、まったく「唯一無二」じゃなかったよね。

DID

Decentralized Identifier (W3C)

Decentralized Identity??

DID： Decentralized Identifier

- 一体何がDecentralizedなんだろう。。。
- 好き勝手にIdentifierとその属性を定義できる権利？
- W3CではDID method が112(2022年当時）→184(2023年当時）→??
- Bitcoinのように、公開鍵＝Identifierとするのが、認証方式とも融合できて、やりたかったことなのでは？
- did:key, did:webくらいを公開鍵のフォーマット（参照手段）として標準化しておけば十分なのでは。

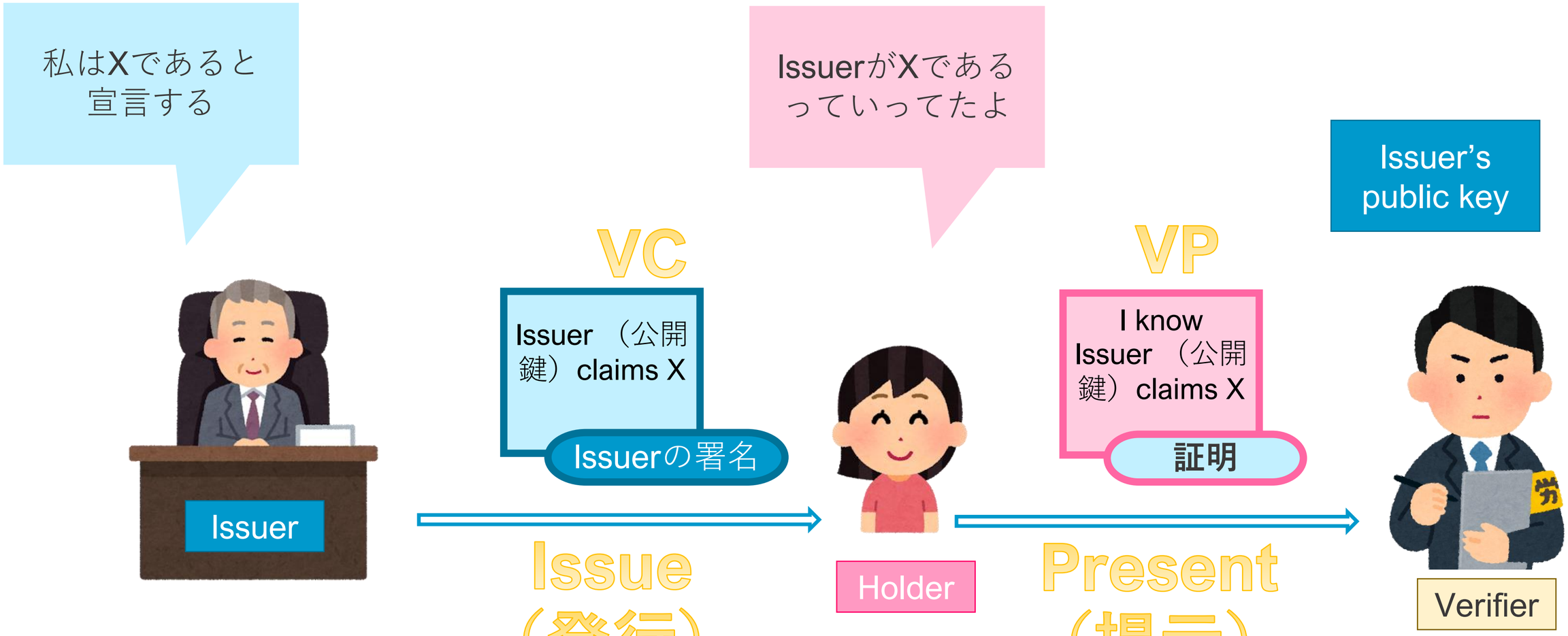
VC (Verifiable Credentials)

そもそも普通、Credentials (証明書）はVerifiable なものでは？

VC (Verifiable Credentials)

- 結局、署名フォーマット！

VCって？VPって？（Verifiable Credential, Verifiable Presentation)



VCって？VPって？（Verifiable Credential, Verifiable Presentation)

私はXであると
宣言する

VC

Issuer （公開鍵）claims X

Issuerの署名

IssuerがXであるっていってたよ

Holder

VP

I know
Issuer （公開鍵）claims X

証明

VCをそのままみせてもいい。
でもそれだけじゃ、芸がないよね

Verifier

Issue
（発行）

Present
（提示）

VCって？VPって？（Verifiable Credential, Verifiable Presentation)

私はXとYを
宣言する

VC

Issuer （公開鍵）claims
X and Y

Issuerの署名

Issue
（発行）

IssuerがXである
っていってたよ

Holder

選択的開示

VP

I know
Issuer （公開鍵）claims X

証明

Present
（提示）

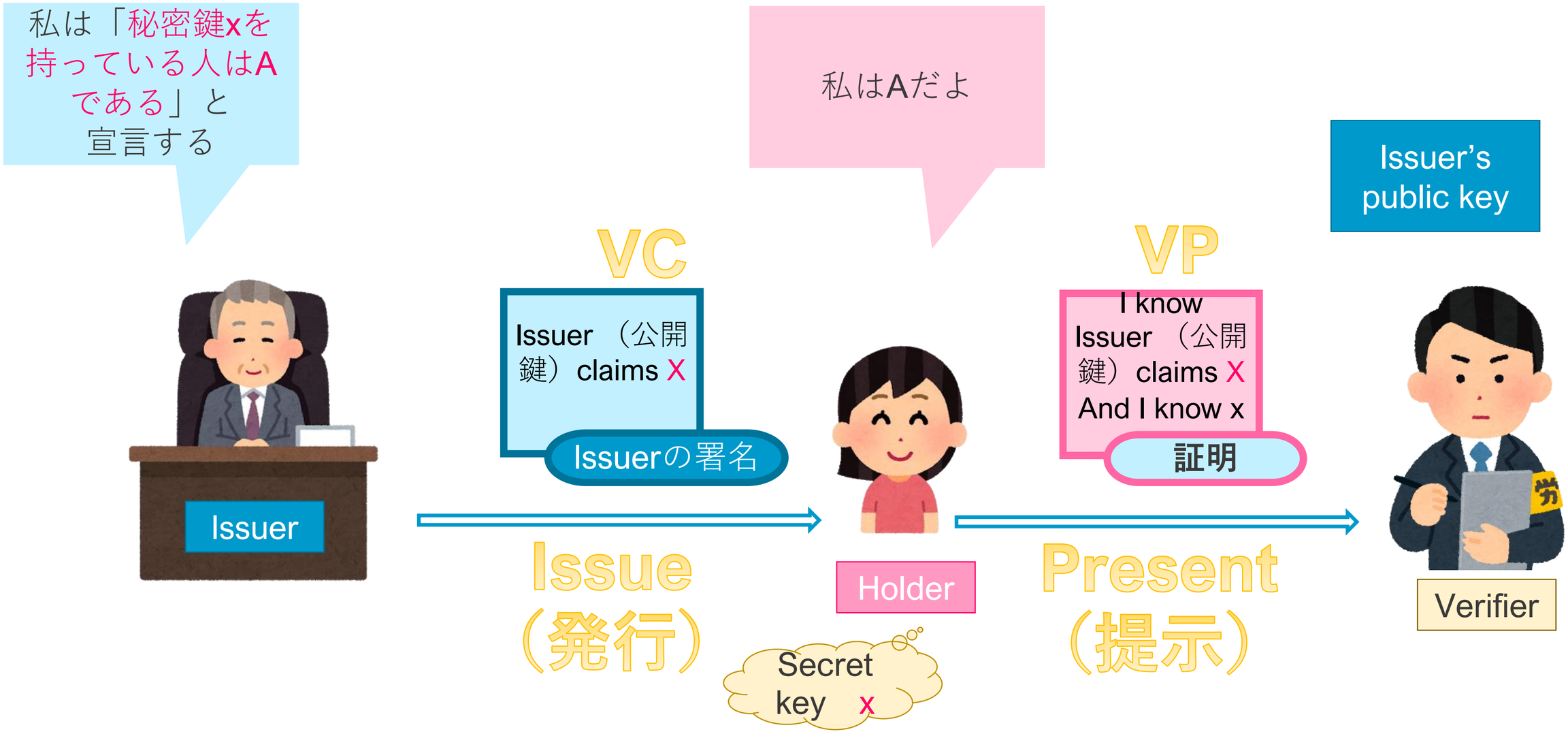
Issuer’s
public key

Verifier

日本のワクチンパスポートもVC仕様

https://idmlab.eidentity.jp/2021/12/verifiable-credentials.html

Binding VCって？



Binding VCって？

私は「秘密鍵xを持っている人はAである」と宣言する

私はAだよ

VC

Issuer （公開鍵）claims X

Issuerの署名

Issue（発行）

Holder

Secret key x

VP

I know
Issuer （公開鍵）claims X
And I know x

証明

Present（提示）

VCをそのままみせた上で、自分がxを知っていることの証明

Public key

Verifier

Binding VCって？VPって？

私は「秘密鍵xを持っている人はAである」と宣言する

秘密鍵をそのまま書けないので、秘密鍵のコミットメント（公開鍵）を書く

私はAだよ

VCをそのままみせた上で、自分がxを知っていることの証明

VC

Issuer （公開鍵）claims X

Issuerの署名

Issue（発行）

Secret key x

VP

I know Issuer （公開鍵）claims X And I know x

証明

Present（提示）

Binding VCって？

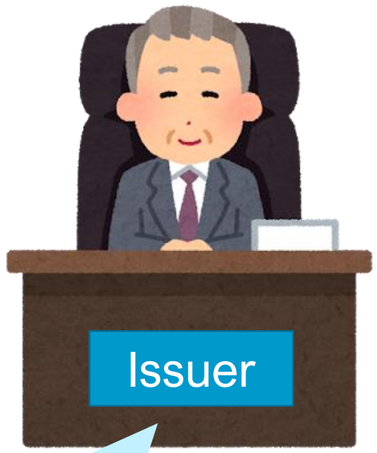
公開鍵証明書

私は「秘密鍵xを持っている人はAである」と宣言する

秘密鍵をそのまま書けないので、秘密鍵のコミットメントCx（公開鍵）を書く

私はAだよ

VCをそのままみせた上で、自分がxを知っていることの証明



VC

Issuer （公開鍵）claims X

Issuerの署名

VP

I know
Issuer （公開鍵）claims X
And I know x

証明

Holder

Verifier

Issue（発行）

Present（提示）

Secret key x

私は「Aさんの公開鍵はCxである」と宣言する

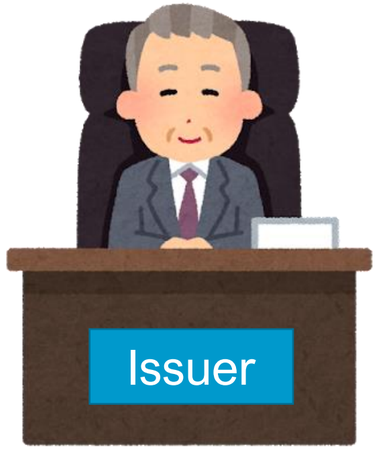
学生証の例

VC

Waseda Univ. Student Card

Name: Alice
Birthday: 2002.1.1
Entrance Year: 2020
Campus: Tokyo

OK



Issuerの署名

Holder

Issue
（発行）

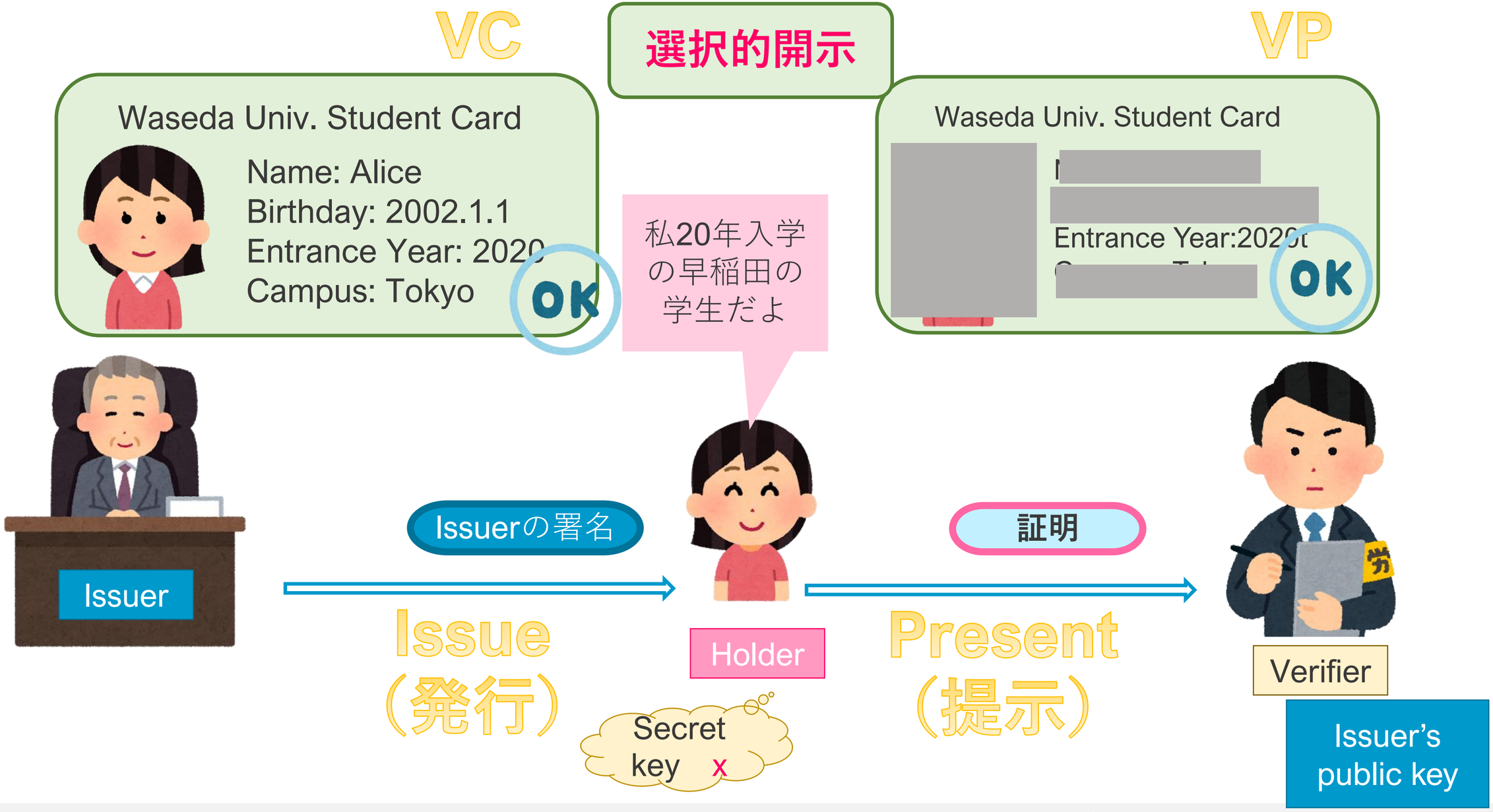
Present
（提示）

Verifier

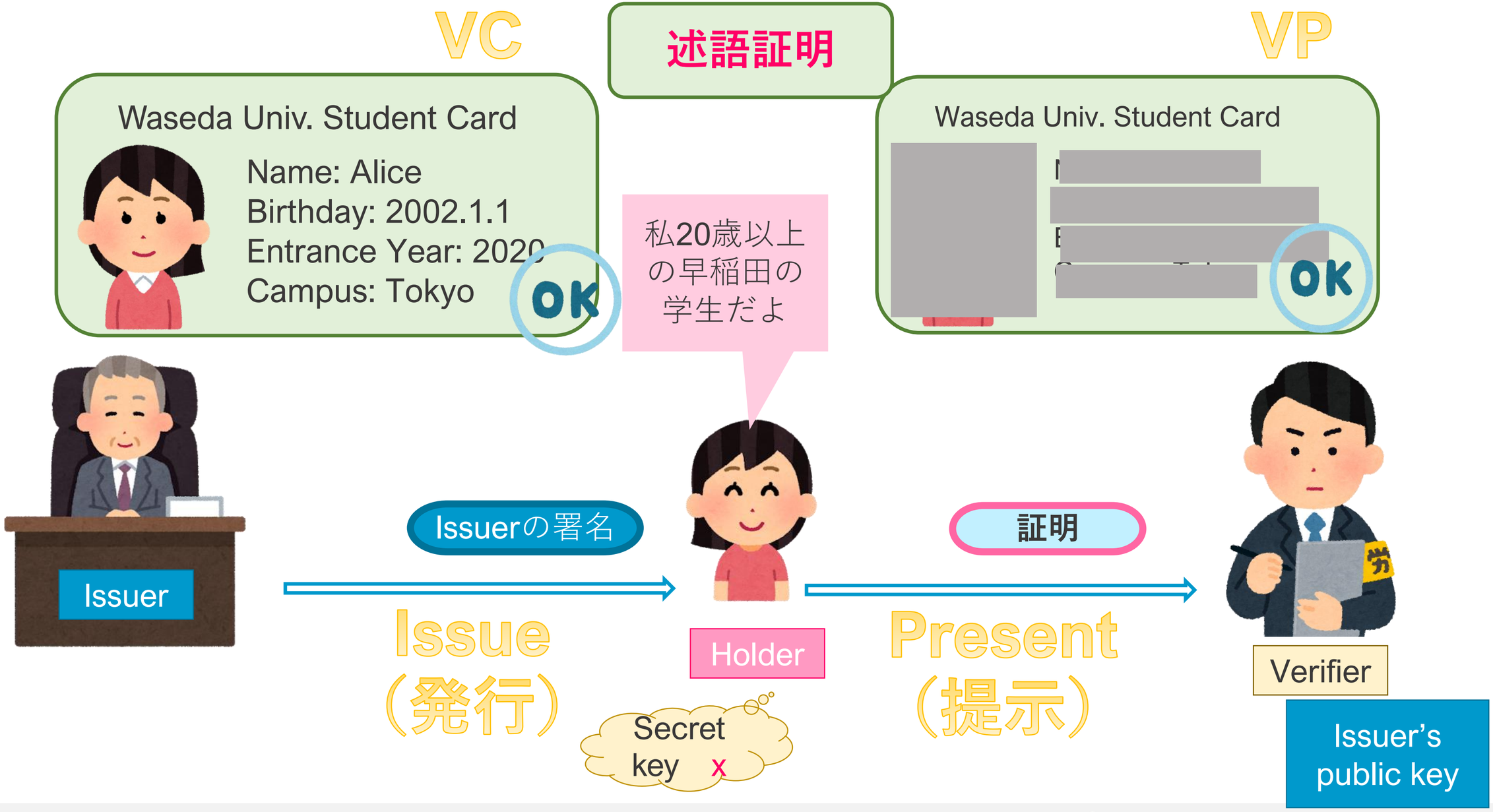
Secret key x

Issuer's public key

学生証の例


VC
選択的開示
VP
Waseda Univ. Student Card
Name: Alice
Birthday: 2002.1.1
Entrance Year: 2020
Campus: Tokyo
OK
Waseda Univ. Student Card
Entrance Year:2020
OK
私20年入学の早稲田の学生だよ
Issuer
Issuerの署名
Issue
（発行）
Holder
Secret key x
証明
Present
（提示）
Verifier
Issuer's public key

学生証の例


VC
述語証明
VP
Waseda Univ. Student Card
Name: Alice
Birthday: 2002.1.1
Entrance Year: 2020
Campus: Tokyo
OK
私20歳以上の早稲田の学生だよ
Waseda Univ. Student Card
OK
Issuer
Issuerの署名
Issue
（発行）
Holder
Secret key x
証明
Present
（提示）
Verifier
Issuer's public key

VC (Verifiable Credentials)

- 結局、署名フォーマット！
- デジタル署名がついていれば検証可能、検証可能なものはすべて証明書！
- あらゆるデータをVC化して、誰がそれを述べたのか、言質を明確にしよう！（データの一人歩きをやめよう！）
- 偽情報の責任を取らせよう！
- 入力を簡単にしよう！
- VCの活用を広めよう！！

VC (Verifiable Credentials)の課題

- 鍵管理
- 失効
- BBS署名の標準化
- 選択開示のネゴシエーション（必要なのは何か）の標準化
- 述語証明のバリエーションの標準化
- 効率性：VP生成の速度、VPの長さ
- 耐量子。。。。

- それでもVCの活用を広めよう！！

VC (Verifiable Credentials)の課題

- 鍵管理
- 失効
- BBS署名の標準化
- 選択開示のネゴシエーション（必要なのは何か）の標準化
- 述語証明のバリエーションの標準化
- 効率性：VP生成の速度、VPの長さ
- 耐量子。。。。

- それでもVCの活用を広めよう！！

佐古研究室では使い勝手のよいオープンソースライブラリを構築しようとしています！

賛同いただける方はご連絡ください。

今日のメッセージ

SSI、DIDはなんだと思っていますか？

概念だとしたらどんな概念？
技術だとしたらどんな技術？
マーケティングワードになっていませんか？

公開鍵暗号技術のメリットを社会に普及させるとしたら、
標準的なVC（＆VP）のフォーマットを普及させるべきでは？

Back up

IETFで標準化中の選択的開示手法: SD-JWT

IETF
Internet Engineering Task Force

Alice の
属性情報
(a1, a2, ..., an)

M=(hash(a1), hash (a2)..hash(an))
Sig = sign(M)

Alice は
(a1, a2, a3)
だけを示したい

Alice

M, Sig, (a1,a2,a3)

Bob

Bob は正しく
確認できる。

Bobはそれ以
外の情報は
得られない

Linkability in Selective Disclosure

Selectively disclose (a1,a2,a3)

Alice has
Attributes
(a1, a2, ..., an)

OK

Alice

M, Sig, (a1,a2,a3)

M, Sig, (a4,a5,a6)

Bob

Same
person!

linkable

David

Selectively disclose (a4,a5,a6)

EU Digital Identity Wallet

POLICY AND LEGISLATION | Publication 10 February 2023

The European Digital Identity Wallet Architecture and Reference Framework

The purpose of the document is to provide a set of the specifications needed to develop an interoperable European Digital Identity (EUDI) Wallet Solution based on common standards and practices.

Downloads

ARF v1.0.0 for publication — Download

Related topics

- Creating a digital society
- eGovernment, Trust services and eID
- Trust services and eIdentification
- Strengthening trust and security

Only linkable
Selective Disclosure

https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework

異議を示す研究者たちのOpenLetter 2023.11.2

Joint statement of scientists and NGOs on the EU's proposed eIDAS reform

2nd November 2023

Dear Members of the European Parliament,
Dear Member States of the Council of the European Union,

We the undersigned are cybersecurity experts, researchers, and civil society organisations from across the globe.

We have read the near-final text of the eIDAS digital identity reform which has been agreed on a technical level in the trilogue between representatives from the European Parliament, Council and Commission. We appreciate your efforts to improve the digital security of European citizens; it is of utmost importance that the digital interactions of citizens with government institutions and industry can be secure while protecting citizens' privacy. Indeed, having common technical standards and enabling secure cross-border electronic identity solutions is a solid step in this direction. However, we are extremely concerned that, as proposed in its current form, this legislation will not result in adequate technological safeguards for citizens and businesses, as intended. In fact, it will very likely result in less security for all.

39か国504名の研究者と
40のNPO団体が署名

Japan

Prof. Masayuki Hatta	Surugadai University
Dr. Octavio Perez Kempner	NTT Social Informatics Laboratories
Prof. Toshimaru Ogura	JCA-NET
Prof. Kazue Sako	Waseda University
Dr. Mehdi Tibouchi	NTT Social Informatics Laboratories

https://epicenter.works/fileadmin/user_upload/eIDAS_Open_Letter-2023-11-01-Academics_NGOs.pdf