

分散デジタルアイデンティティ技術の周辺動向

鈴木茂哉

慶應義塾大学大学院政策・メディア研究科 特任教授
慶應義塾大学SFC研究所ブロックチェーン・ラボ 副所長（技術統括）
WIDEプロジェクトボードメンバ

@ 第4回BASEアライアンス オンラインワークショップ "The 4th Workshop Basing Blockchain" 2021/10/8



本日のトピック

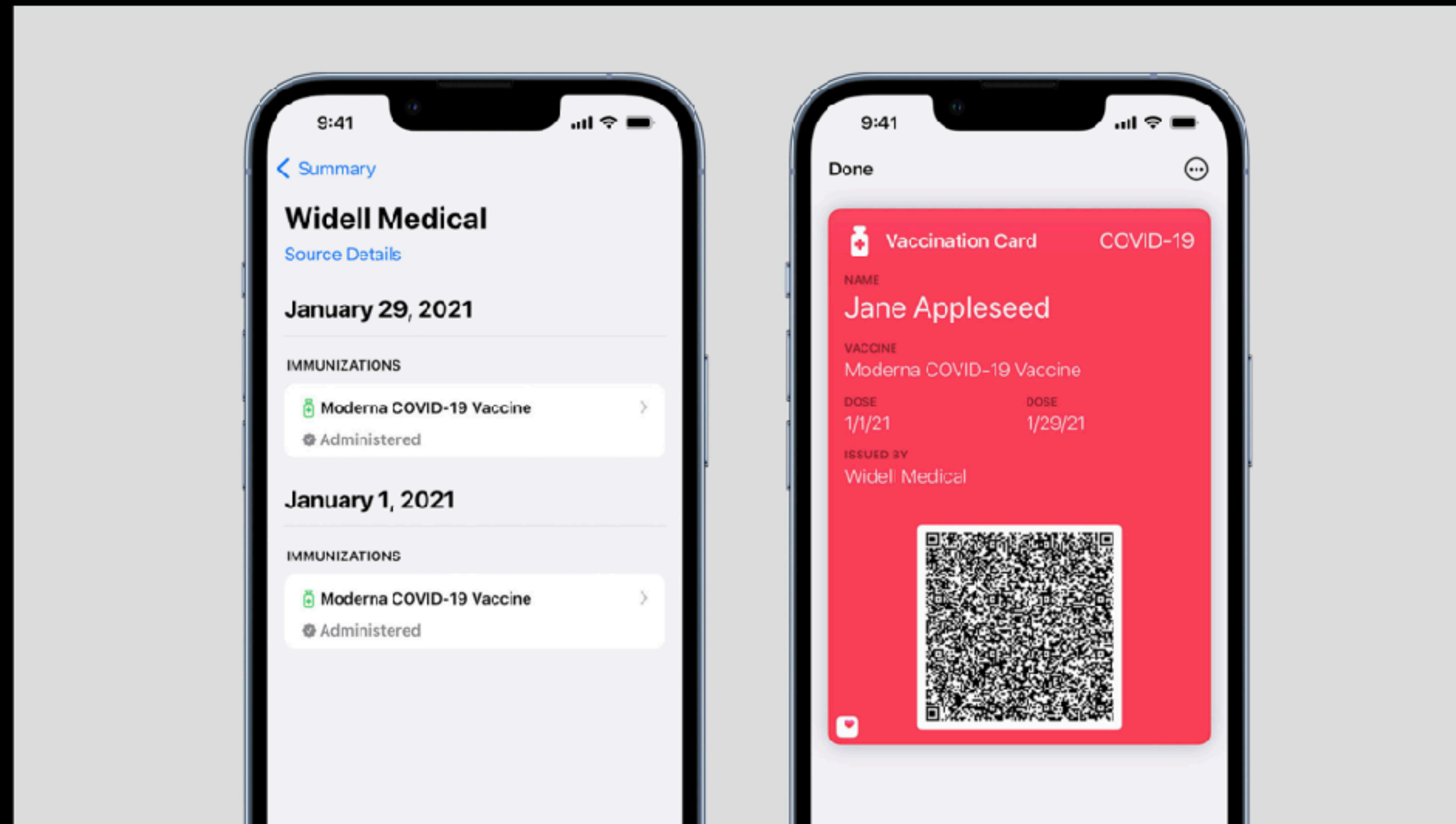
- ・ 検証可能なデジタル証明書とデジタルアイデンティティ
 - ・ Verifiable Credential
 - ・ ワクチン接種証明への応用
 - ・ 自己主権型デジタルアイデンティティとして適用可能な分散型アイデンティティ
 - ・ Decentralized Identifiers (DID)
 - ・ 課題と標準化動向
 - ・ 応用に向けた国内の取り組み
-
- ・ ブロックチェーンのアプリケーション(通貨的な応用**以外**)にはデジタルアイデンティティが必要
 - ・ 自己主権型デジタルアイデンティティにはブロックチェーンを使える
 - 課題: エネルギー消費の問題の解決が必要

■ 検証可能なデジタル証明書



Verifiable health records updates

September 21, 2021

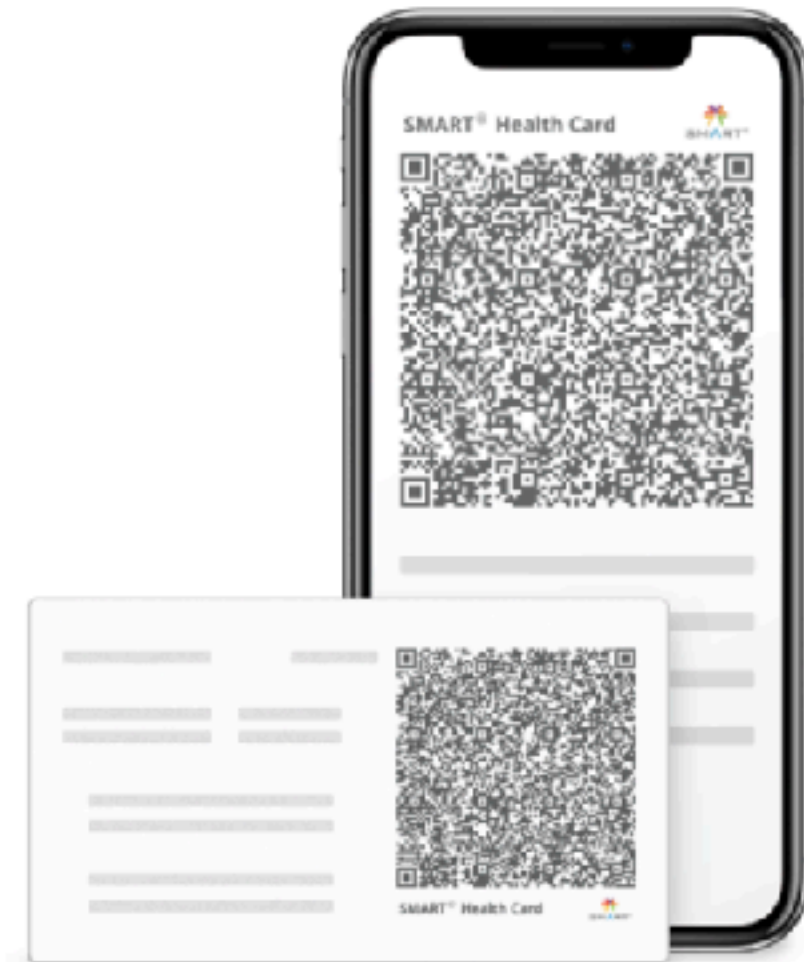


With iOS 15, users can download and store verifiable health records, including COVID-19 vaccinations and test results, in the Health app. Verifiable health records in the Health app are based on the SMART Health Cards specification. Users can choose to share verifiable health records stored in the Health app with approved third-party apps requesting this information, like airlines, event venues, and other businesses that facilitate in-person interactions. And in an upcoming software update, they can also choose to add verifiable COVID-19 vaccination records as a vaccination card in

<https://developer.apple.com/news/?id=7h3vwlh5>

What are SMART Health Cards?

SMART Health Cards are paper or digital versions of your clinical information, such as vaccination history or test results. They allow you to keep a copy of your records on hand and easily share this information with others if you choose.



SMART Health Cards may be printed on paper or digital.

<https://smarthealth.cards>

Protocol



Overview

Looking for a non-technical overview?

See the [SMART Health Cards public landing page](#). Otherwise, read on for the technical specifications.

Status

Stable first release authored with input from technology, lab, pharmacy, Electronic Health Record, and Immunization Information System vendors.

Contributing

To propose changes, please use GitHub [Issues](#) or create a [Pull Request](#).

Introduction

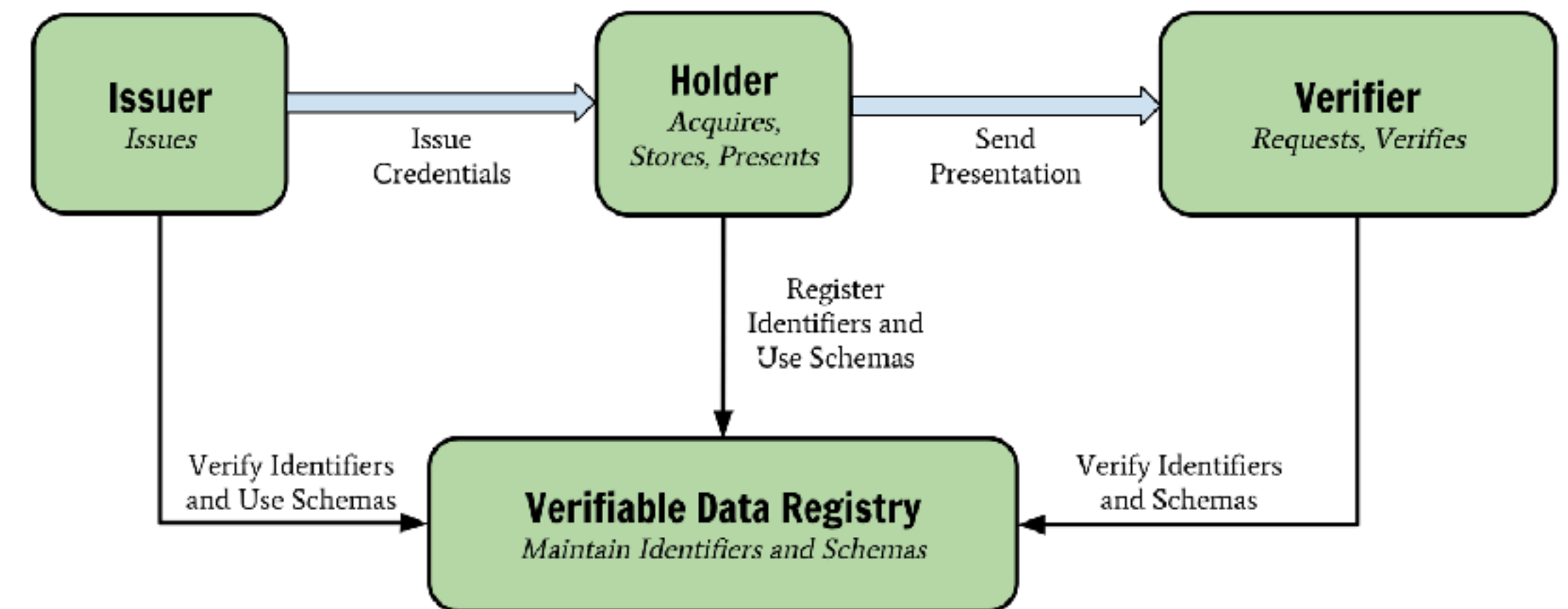
This implementation guide provides a framework for "Health Cards", with a short term goal to enable a consumer to receive COVID-19 Vaccination or Lab results and **present these results to another party in a**

Verifiable Credentials - 検証可能な資格証明書

- さまざまな「証明書」のデジタル化手段
- デジタル署名技術を用いた【発行者】(Issuer)により【対象者】(Subject)が特定の条件を満たしている事を【保持者】(Holder) が示すことができる
- W3C で標準化されている [1]

- Subject / Issuer / Holder を示すための手段が必要

→ デジタルアイデンティティ技術が必須



デジタル庁のパブコメ (2021/9/30締め切り)

- デジタル庁「コロナワクチンの接種証明書（電子交付）の仕様」パブコメ [1]
 - 渡航向けと国内向けの二案
 - 渡航向けは ICAO標準で、Verifiable Credentialでは無い
 - 国内向けは Smart Health Card [2] で、Verifiable Credentialベース

デジタル庁

[ホーム](#) > [お知らせ](#) > コロナワクチンの接種証明書(電子交付)の仕様に関するご意見を募集します

コロナワクチンの接種証明書(電子交付)の仕様に関するご意見を募集します

公開日：2021年9月17日 最終更新：2021年9月22日

デジタル庁ではコロナワクチンの接種証明書(電子交付)の活用を検討されている事業者、自治体、公共機関、医療機関等の皆様を対象に、仕様に関する意見募集を実施します。

背景・目的

現在デジタル庁では接種証明書の電子交付の検討を内閣官房とともに進めています。

組織情報

政策

法令

採用

資料


申請・届出

お知らせ

注目のトピック

デジタル庁発足式を行いました

平井大臣メッセージ



【国内向け】二次元コード付き証明書とAPIの仕様（案）

二次元コード付き証明書の仕様

【目視確認】 紙で出力する接種証明書と同等の内容がスマホのアプリ上で確認できるため、接種情報を目視確認することができます。

【情報読取】 アプリ上の二次元コードから以下の項目を読み取ることもできます。

二次元コード付き証明書の取得

以下の手順で取得することができます。

- (1) スマホで接種証明書アプリをダウンロード
- (2) マイナンバーカード + 4桁の暗証番号で申請
- (3) 接種情報を二次元コード付き証明書の形で交付



イメージ

姓名 [Surname Given name]
接種 証明

生年月日 [Date of Birth]
1991-02-05

二次元コードに含まれる項目(案)

- ・漢字氏名
- ・生年月日
- ・ワクチン名・メーカー名
- ・ロット番号
- ・接種日
- ・証明書ID
- ・発行日

規格： SMART Health Cards (想定)

接種情報取得APIの仕様

予約サイト等での利用を念頭に置き、ワクチン接種情報を取得するAPIも提供予定です。

- (1) 「接種券番号」「生年月日」の情報を入力する
- (2) 「最終接種回数」「最終接種日」等の情報を返す

[1] <https://www.digital.go.jp/posts/ckWVVAYa>
[2] <https://smarthealth.cards>

SMART Health Cardの仕様概要 [1]

- JSON Web Token^[2] 形式の Verifiable Credential^[3] として実装
- 証明対象(credentialSubject) は HL7^[4] のレコードとして表現
 - COVID-19 ワクチンの場合は Patient レコードとワクチン関連レコードをHL7 FHIR Bundleで指示
- 証明書発行者の指示はURL ("iss") → 例: <https://smarthealth.cards/examples/issuer>
 - 公開鍵は発行者URL指示先にある well-known URLの JSON Web Key Set^[5]で指示
→ 例: <https://smarthealth.cards/examples/issuer/.well-known/jwks.json>
 - JSON Web Key Set に X.509証明書チェーンを同梱できる
- SMART Health Card データ生成手順:
 - 圧縮 (minify + zip deflate)
 - JWSヘッダ追加
 - JSON Web Signature^[6] で署名
- 数値エンコード → QR Code (複数可)

[1] SMART Health Card <https://smarthealth.cards>

[2] RFC7519 JSON Web Token (JWT) <https://www.rfc-editor.org/rfc/rfc7519>

[3] Verifiable Credentials Data Model 1.0 <https://www.w3.org/TR/2019/REC-vc-data-model-20191119/>

[4] HL7 Standards <https://www.hl7.org>

[5] JSON Web Key (JWK) <https://www.rfc-editor.org/rfc/rfc7517>

[6] JSON Web Signature (JWS) <https://www.rfc-editor.org/rfc/rfc7515>

構造の概略

```
{
  "iss": "<<Issuer URL>>",
  "nbf": 1591037940, // nbf = Not Before - Time Stamp
  "vc": {
    "type": [
      "https://smarthealth.cards#health-card",
      "<<Additional Types>>",
    ],
    "credentialSubject": {
      "fhirVersion": "<<FHIR Version, e.g. '4.0.1'>>",
      "fhirBundle": {
        "resourceType": "Bundle",
        "type": "collection",
        "entry": [ "<<FHIR Resource>>", "<<FHIR Resource>>", "..."]
      }
    }
  }
}
```

Jupyter Notebook Walkthrough: <https://github.com/dvci/health-cards-walkthrough/blob/main/SMART%20Health%20Cards.ipynb>

Demo Portal: <https://demo-portals.smarthealth.cards>



Example Payload with FHIR Bundle

```
{
  "iss": "https://smarthealth.cards/examples/issuer",
  "nbf": 1620992383.218,
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1"
    ],
    "type": [
      "VerifiableCredential",
      "https://smarthealth.cards#health-card",
      "https://smarthealth.cards#immunization",
      "https://smarthealth.cards#covid19"
    ],
    "credentialSubject": {
      "fhirVersion": "4.0.1",
      "fhirBundle": {
        "resourceType": "Bundle",
        "type": "collection",
        "entry": [
          {
            "fullUrl": "resource:0",
            "resource": {
              "resourceType": "Patient",
              "name": [
                {
                  "family": "Anyperson",
                  "given": [
                    "John",
                    "B."
                  ]
                }
              ],
              "birthDate": "1951-01-20"
            }
          }
        ]
      }
    }
  }
},
```

Header and Patient Information

```
{
  "fullUrl": "resource:1",
  "resource": {
    "resourceType": "Immunization",
    "status": "completed",
    "vaccineCode": {
      "coding": [
        {
          "system": "http://hl7.org/fhir/sid/cvx",
          "code": "207"
        }
      ]
    },
    "patient": {
      "reference": "resource:0"
    },
    "occurrenceDateTime": "2021-01-01",
    "performer": [
      {
        "actor": {
          "display": "ABC General Hospital"
        }
      ]
    ],
    "lotNumber": "0000001"
  },
}
```

First Vaccination Record

```
{
  "fullUrl": "resource:2",
  "resource": {
    "resourceType": "Immunization",
    "status": "completed",
    "vaccineCode": {
      "coding": [
        {
          "system": "http://hl7.org/fhir/sid/cvx",
          "code": "207"
        }
      ]
    },
    "patient": {
      "reference": "resource:0"
    },
    "occurrenceDateTime": "2021-01-29",
    "performer": [
      {
        "actor": {
          "display": "ABC General Hospital"
        }
      ]
    ],
    "lotNumber": "0000007"
  },
}
```

Second Vaccination Record



Chain of Trust of SMART Health Card

JSON File: example.smart-health-card

JWS - Header

```
{
  alg: 'ES256',
  zip: 'DEF',
  kid: 'OBztBGRexV0me4ycPTBp-lAMWQmU1_OY1q8m4awW_34'
}
```

JWS - Payload

```
{
  "iss": "https://smarthealth.cards/examples/issuer",
  "nbf": 1620992383.218,
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1"
    ],
    "type": [
      "VerifiableCredential",
      "https://smarthealth.cards#health-card",
      "https://smarthealth.cards#immunization",
      "https://smarthealth.cards#covid19"
    ],
    "credentialSubject": {
      "fhirVersion": "4.0.1",
      "fhirBundle": {
        "resourceType": "Bundle",
        "type": "collection",
        "entry": [
          // ----- Snip -----
        ]
      }
    }
  }
}
```

JWS - Signature

```
RH5TVWB-
aYrPnbtb2LXU9gpC1WRra0gQHjZxSE_htNScq8NdIdgoUt5C1kvdiXbYq
D79W87si9x66fFCwmCmgw
```

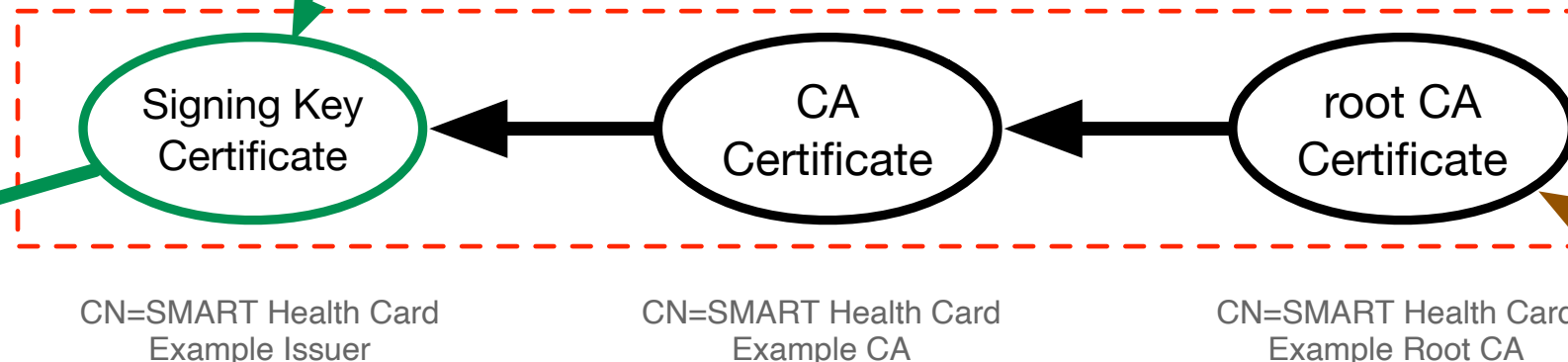
Web Server: https://smarthealth.cards/

JWKS file: in URL: https://smarthealth.cards/examples/issuer/.well-known/jwks.json

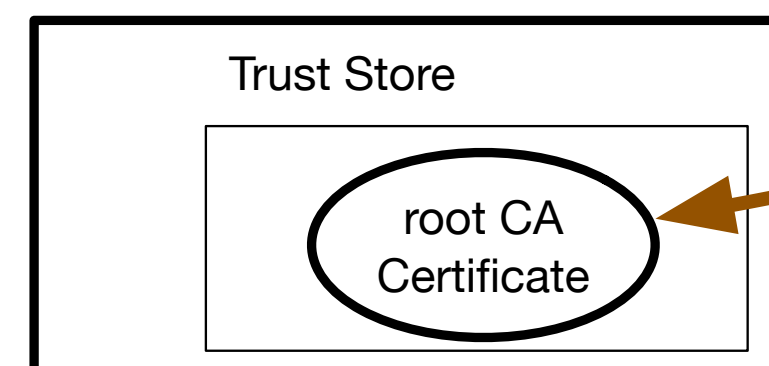
```
{
  "warning": "You should be using spec.smarthealth.cards. <snip>",
  "keys": [
    {
      "kty": "EC",
      "kid": "3Kfdg-XwP-7gXyywtUfUADwBumDOPKMqx-iELL11W9s",
      "use": "sig",
      "alg": "ES256",
      "crv": "P-256",
      "x": "11XvRWylI2S0EyJlyf_bWfw_TQ5CJJNLw78bHXNxcgw",
      "y": "eZXwxv01hvCY0KucrPfKo7yAyMT6Ajc3N7OkAB6VYy8"
    },
    {
      "kty": "EC",
      "kid": "OBztBGRexV0me4ycPTBp-lAMWQmU1_OY1q8m4awW_34",
      "use": "sig",
      "alg": "ES256",
      "x5c": [
        "MIICBjCCAYygAwIBAgIUgGxqplmagmOhhHUnRDUnQhTKaZUwCgYIKoZIz<snip>",
        "MIICBjCCAWigAwIBAgIUWgu3m7SToFGJKDerCOQcMK5AlbUwCgYIKoZIz<snip>",
        "MIICMTCCAZoGAwIBAgIUB-niLvaIdt13U3xO2i7miRk1thEQwCgYIKoZIz<snip>"
      ],
      "crv": "P-256",
      "x": "f6GJiCnbnBaIm2jDaH_3UPC7Y1-x5yBAi5ddZ8v3Y_w",
      "y": "jKcgirFw4G9v9gWTDcQAJvcCRQpbIK76bWqKBtseFzQ"
    }
  ]
}
```

X.509 CA Certificates for Issuer's Signing Key

Issuer's Signing Key

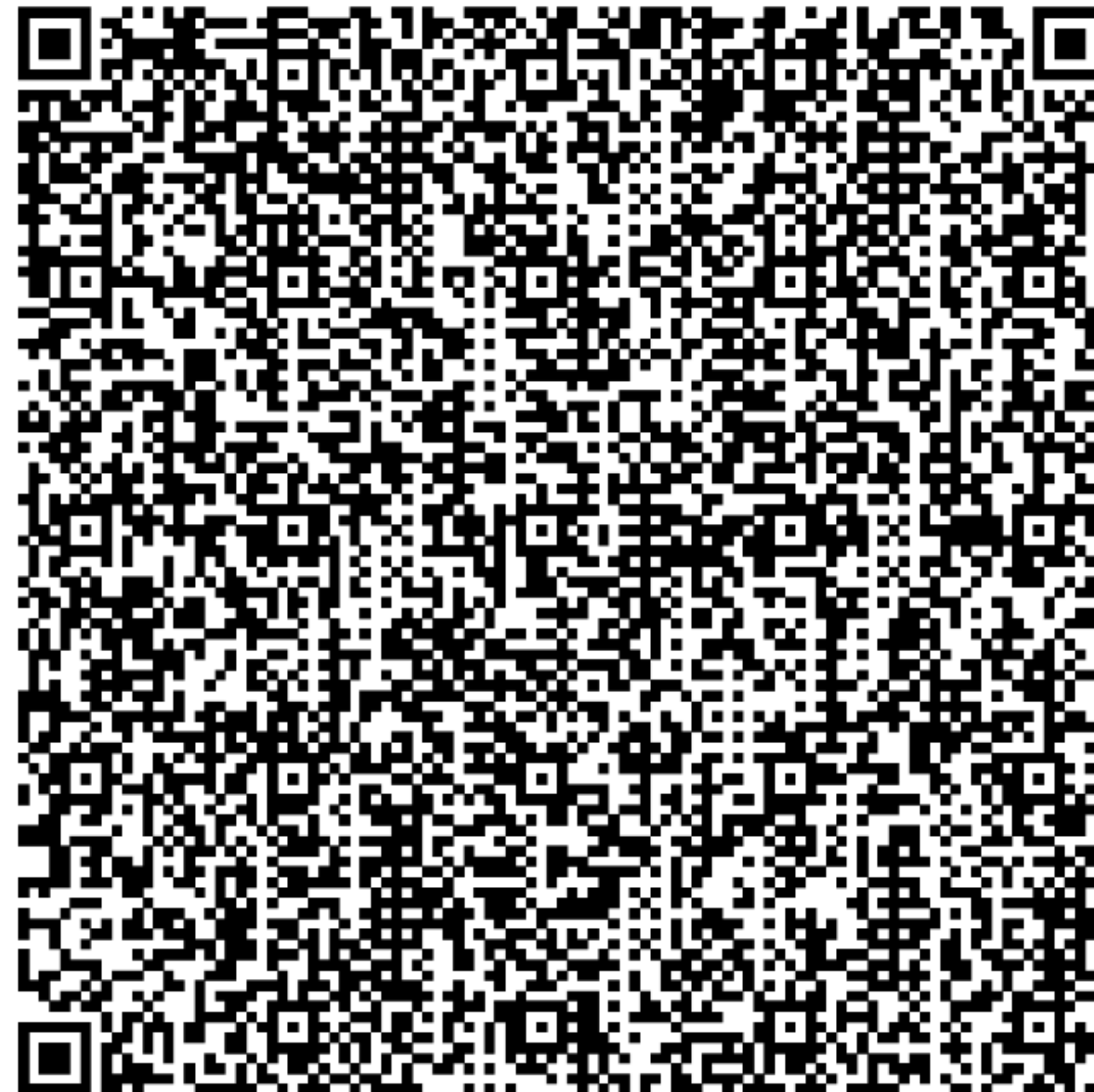


Verifying Device



Note: Part of this example is modified, and not from a real execution results due to the experimental environment

デモ QRコード



Jupyter Notebook Walkthrough: <https://github.com/dvci/health-cards-walkthrough/blob/main/SMART%20Health%20Cards.ipynb>
から借用



ワクチン接種証明書と身分証明書

- ・ パブコメで示されている資料^[1]では身分証明書とともに用いられることが前提
- ・ マイナンバーカードと接触アプリの組み合わせで発行
- ・ 海外用はパスポート番号が含まれる。国内用は氏名と生年月日

【渡航向け】二次元コード付き証明書（案）

二次元コード付き証明書の仕様

【目視確認】 紙で出力する接種証明書と同等の内容がスマホのアプリ上で確認できるため、接種情報を目視確認することができます。

【情報読取】 アプリ上の二次元コードから以下の項目を読み取ることもできます。

二次元コード付き証明書の取得

以下の手順で取得することができます。

- (1) スマホで接種証明書アプリをダウンロード
- (2) マイナンバーカード + 4桁の暗証番号で申請
- (3) パスポートのMachine Readable ZoneのOCR読取
- (4) 接種情報を二次元コード付き証明書の形で交付



二次元コードに含まれる項目(案)

- ・ローマ字氏名★
- ・国籍・地域★
- ・旅券番号★
- ・生年月日
- ・ワクチン名・メーカー名
- ・ロット番号
- ・接種日
- ・証明書ID
- ・発行日

★: パスポートから読み取る情報

規格: ICAO VDS-NC (想定)

【国内向け】二次元コード付き証明書とAPIの仕様（案）

二次元コード付き証明書の仕様

【目視確認】 紙で出力する接種証明書と同等の内容がスマホのアプリ上で確認できるため、接種情報を目視確認することができます。

【情報読取】 アプリ上の二次元コードから以下の項目を読み取ることもできます。

二次元コード付き証明書の取得

以下の手順で取得することができます。

- (1) スマホで接種証明書アプリをダウンロード
- (2) マイナンバーカード + 4桁の暗証番号で申請
- (3) 接種情報を二次元コード付き証明書の形で交付



二次元コードに含まれる項目(案)

- ・漢字氏名
- ・生年月日
- ・ワクチン名・メーカー名
- ・ロット番号
- ・接種日
- ・証明書ID
- ・発行日

規格: SMART Health Cards (想定)

接種情報取得APIの仕様

予約サイト等での利用を念頭に置き、ワクチン接種情報を取得するAPIも提供予定です。

- (1) 「接種券番号」「生年月日」の情報を入力する
- (2) 「最終接種回数」「最終接種日」等の情報を返す

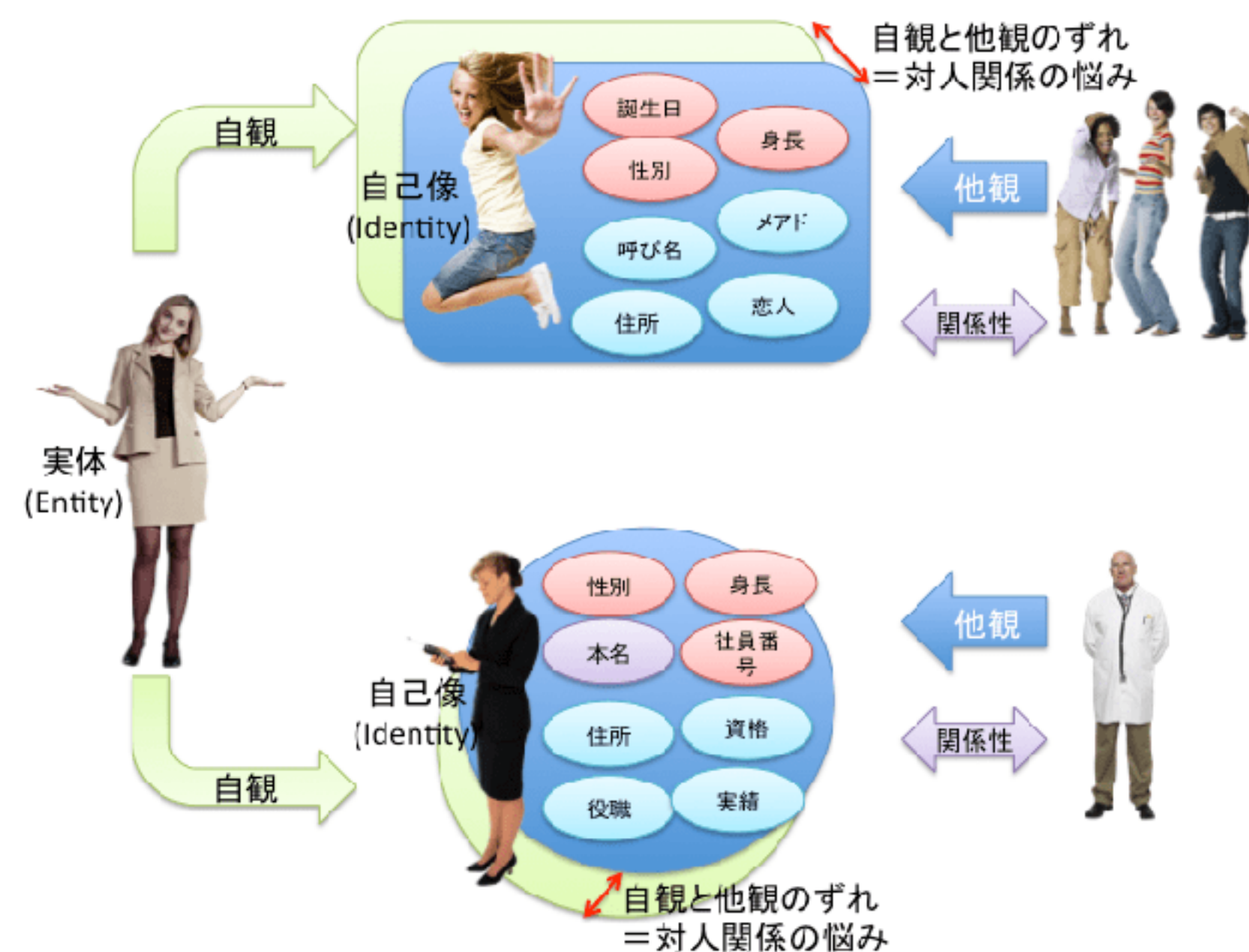
[1] <https://www.digital.go.jp/posts/ckWVVAYa>

デジタルアイデンティティ



デジタルアイデンティティ

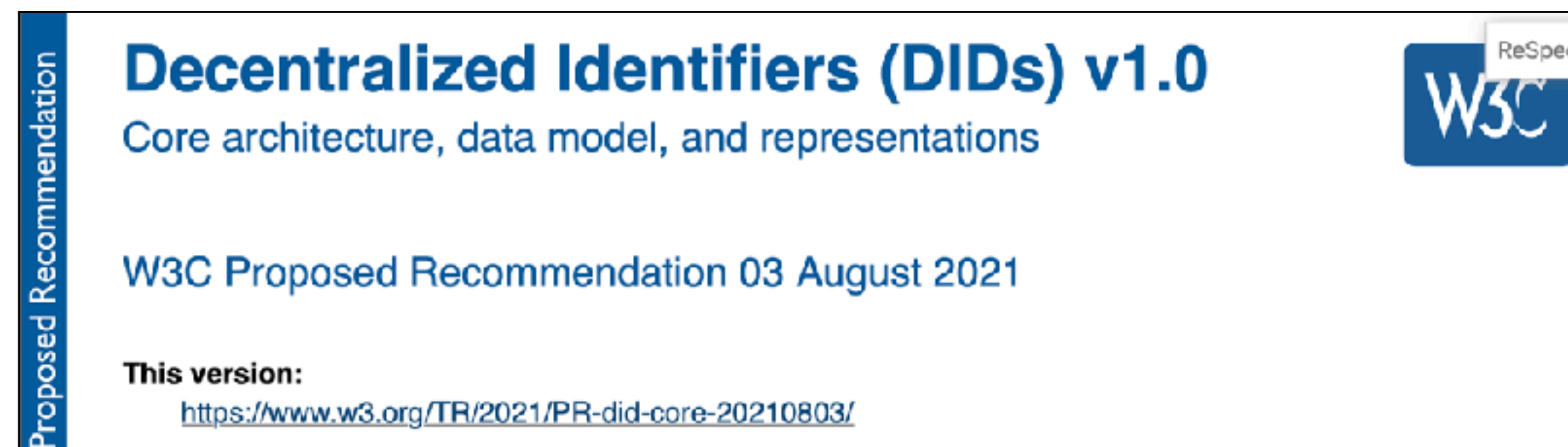
- ものすごく「丸めて」表現すると:
「ある人(= 実体: 一つ)に対応するサイバー空間中で識別可能な自己像(複数可)」
- 実体と自己像、自己像に対する自観、他人からみた他観や関係性など、厳密に説明するのは難しい。
[1]参照のこと (右図も同文書から)
- ISOの定義では
「実体を構成する属性の集合」
(ISO/IEC 24760-1)



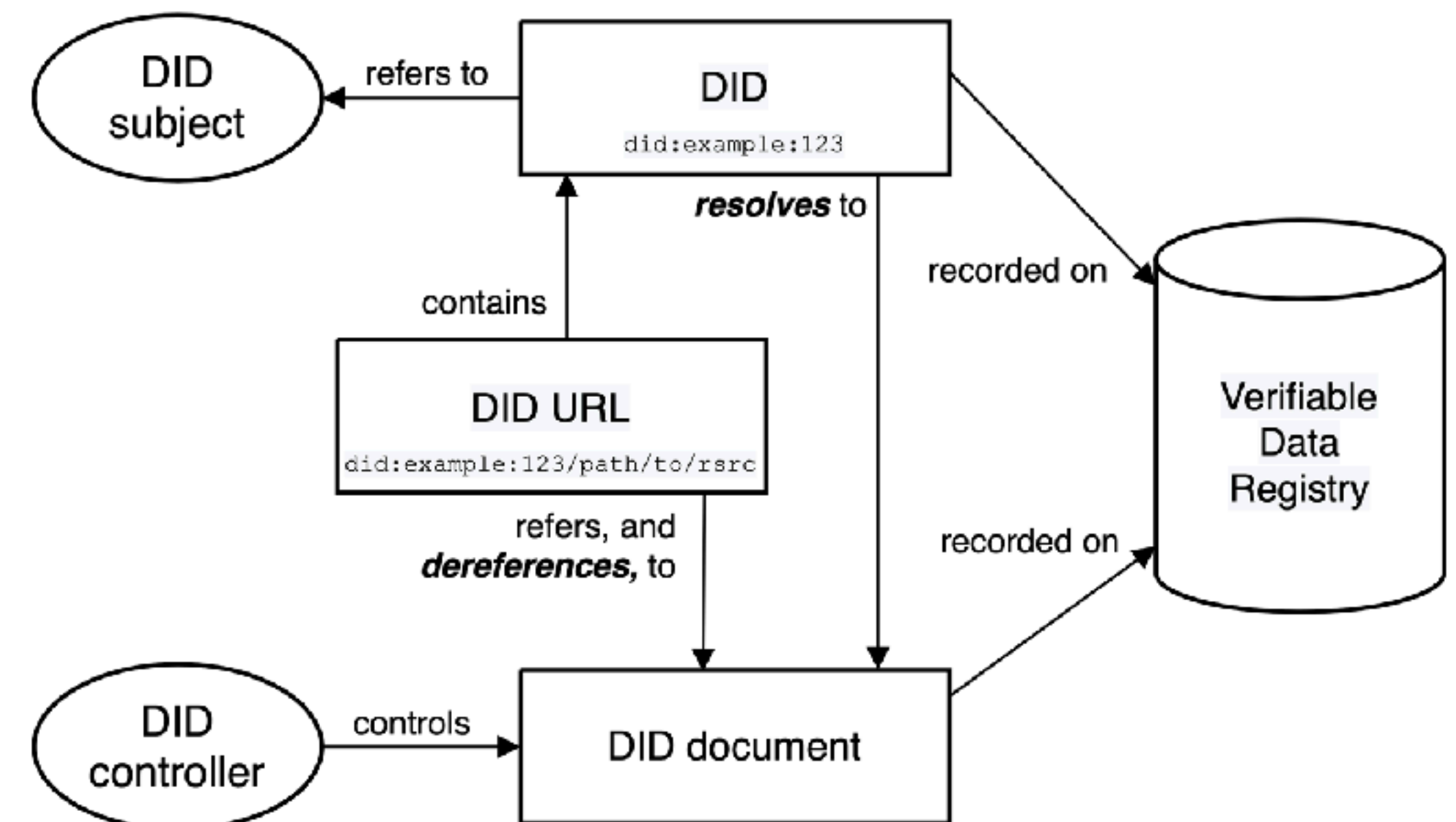
Decentralized Identifier (DIDs) v1.0 (Proposed Recommendation)

- 自己主権型の識別子にまつわるデータモデル標準
 - 周辺技術との組み合わせで自己主権型のアイデンティティを実現できる
 - 複数の方式(メソッド)で実装され、メソッドにより、ブロックチェーン技術を下支えにするものも、しないものもある

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



Decentralized Identifier (DIDs) v1.0 (Proposed Recommendation)
<https://www.w3.org/TR/2021/PR-did-core-20210803/>



DID Methodと実装状況

- DID Specification Registry に一覧がある。現在このリストには113個 (2021/10/8)
- コンフォーマンステストに提出された実装の数は47個

§ 12. DID Methods

This table summarizes the DID method specifications currently in development. The links will be updated as subsequent Implementer's Drafts are produced.

The normative requirements for DID method specifications can be found in [Decentralized Identifiers v1.0: Methods \[DID-CORE\]](#). DID methods that do not meet these requirements will not be accepted. We encourage DID method authors to provide an email address in the Author Links column, as this helps with maintenance.

ISSUE

How will we automate the update of the namespace reservations and keep them in sync with the reserved namespace in the Abstract Data Model? See [issue #152](#).

| Method Name | Status | DLT or Network | Author Links | Link |
|-------------|-------------|-----------------------|--|-------------------------------------|
| did:3: | PROVISIONAL | Ceramic Network | Joel Thorstensson | 3ID DID Method |
| did:abt: | PROVISIONAL | ABT Network | ArcBlock | ABT DID Method |
| did:aergo: | PROVISIONAL | Aergo | Blocko | Aergo DID Method |
| did:ala: | PROVISIONAL | Alastria | Alastria National Blockchain Ecosystem | Alastria DID Method |
| did:bba: | PROVISIONAL | Ardor | Attila Aldemir | BBA DID Method |
| did:bid: | PROVISIONAL | bif | teleinfo caict | BIF DID Method |
| did:bnb: | PROVISIONAL | Binance Smart Chain | Ontology Foundation | Binance DID Method |

DID Core Specification Test Suite and Implementation Report

30 July 2021

Latest editor's draft:

<https://w3c.github.io/did-test-suite/>

Editors:

[Orie Steele \(Transmute\)](#)

[Shigeya Suzuki \(Keio University\)](#)

[Manu Sporny \(Digital Bazaar\)](#)

[Markus Sabadello \(Danube Tech\)](#)

Participate:

[GitHub w3c/did-test-suite](#)

[File an issue](#)

[Commit history](#)

[Pull requests](#)

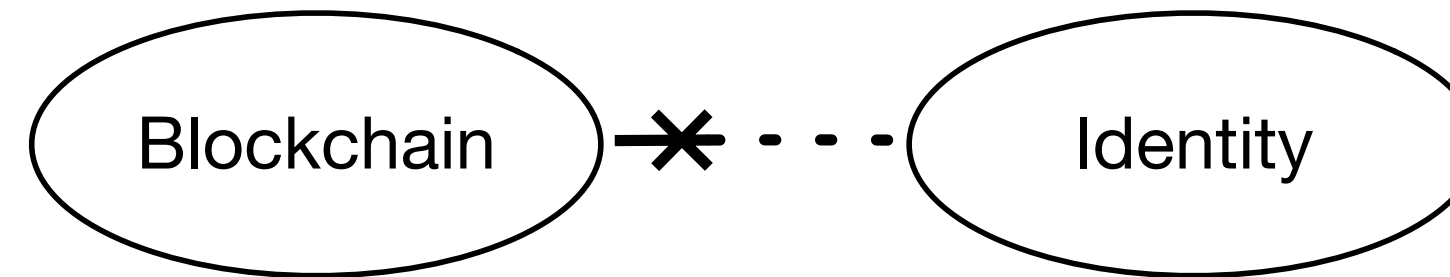
Copyright © 2021 W3C® (MIT, ERCIM, Keio, Beihang). W3C [liability](#), [trademark](#) and [permissive document license](#)

<https://w3c.github.io/did-spec-registries/#did-methods>

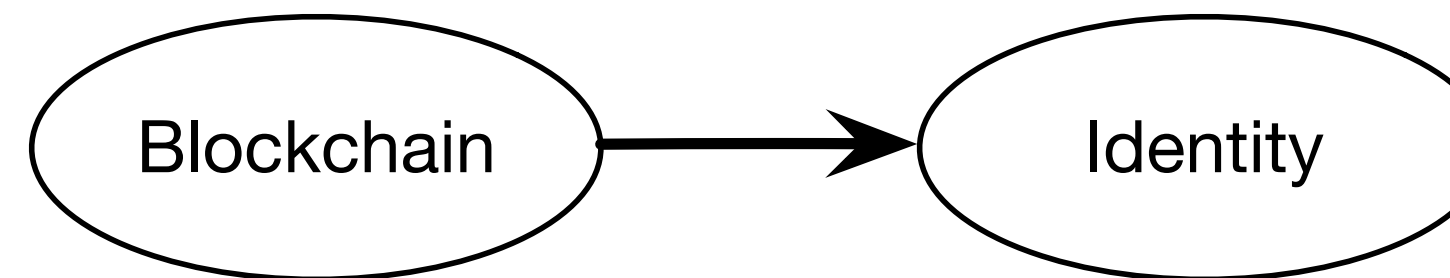
<https://w3c.github.io/did-test-suite/>

Dependency of Blockchain, Identity, and DNS

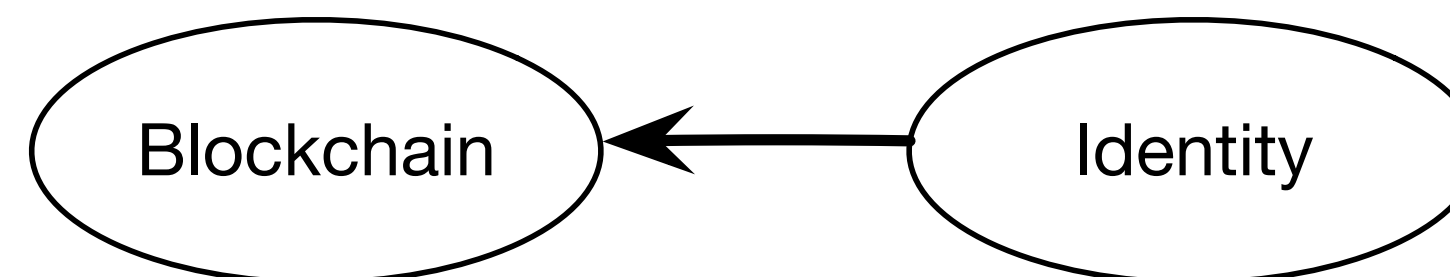
Blockchain-based Cryptocurrencies' requires Anonymity for Fungibility



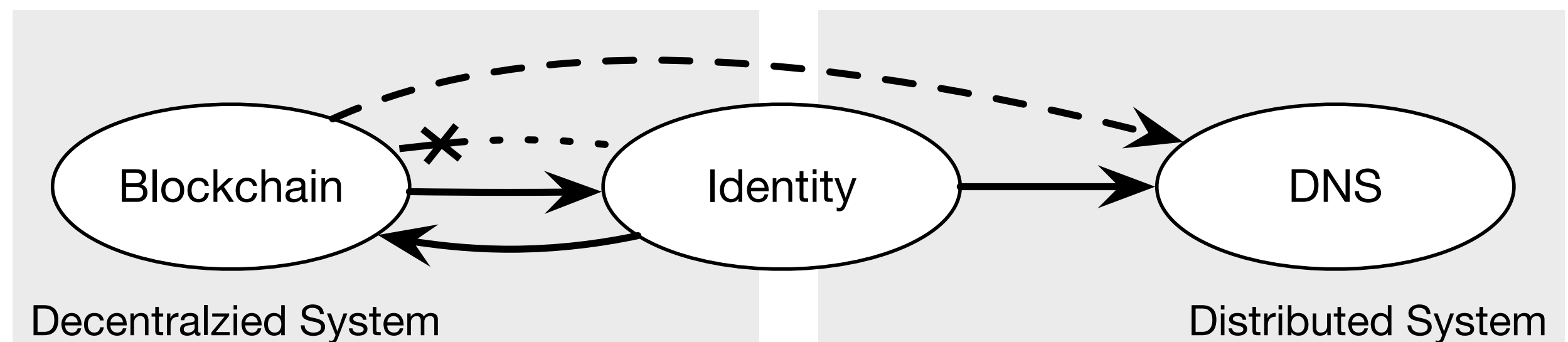
Blockchain Application depends on Identity System



Privacy-centric Identity System often needs Blockchain (i.e., Decentralized Identifier (DID))



A decentralized System does not work effectively without Distributed System, at least for now. This dependency is especially true for DNS



Key Points in Formal Objection

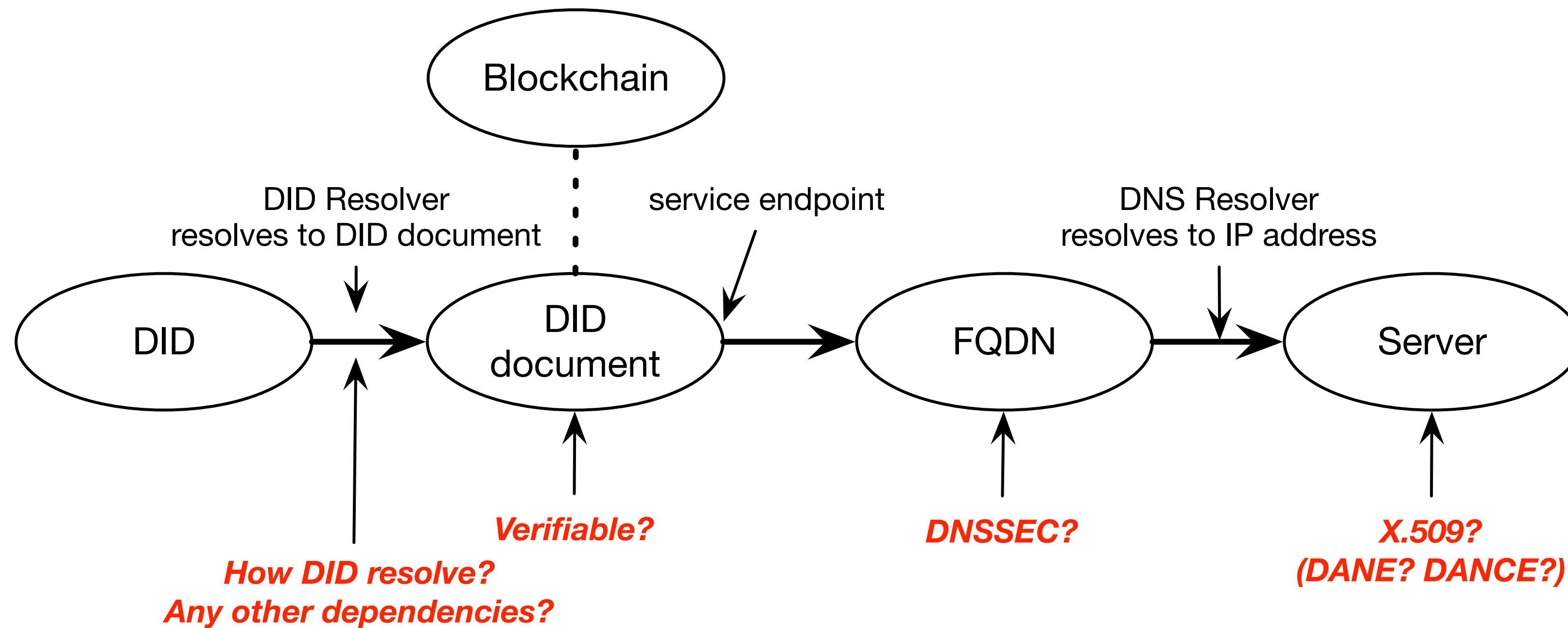
- Interoperability
 - beyond data model
 - no standardized specs for methods - did:key or did:web?
 - format compatibility
- Decentralization
 - did:web decentralized ?
- Energy Requirement
 - ... on public blockchain based methods

Minutes on meeting on the topic (public)

| W3C | | DiD 1.0 Comments | | 21 September 2021 | |   | |
|---|---|------------------|--|-------------------|--|---|--|
| Attendees | | | | Contents | | | |
| Present | Tartek Çelik, Chris Wilson, Philippe Le Hégaré, Ivan Herman, Daniel Burnett, Travis Leithead, Theresa O'Connor, Manu Sporny, Annette Greiner, Jeffrey Yasskin, Brent Zundel, Pamela Dingle, Eric Rescorla | | | 1. | DiD methods status & interop. standardization | | |
| | | | | 2. | Did we achieve to make DiD decentralized, given centralized methods? | | |
| | | | | 3. | DiD methods and energy requirements | | |
| | | | | 4. | JSON, JSON-LD | | |
| | | | | 5. | Next steps | | |
| Regrets | none | | | | | | |
| Chair | plh | | | | | | |
| Scribe | Dan | | | | | | |
| <h2>Meeting minutes</h2> | | | | | | | |
| <p>plh: sent agenda in advance</p> <p>... want to see if we can find common ground without forcing common ground on broader community</p> | | | | | | | |

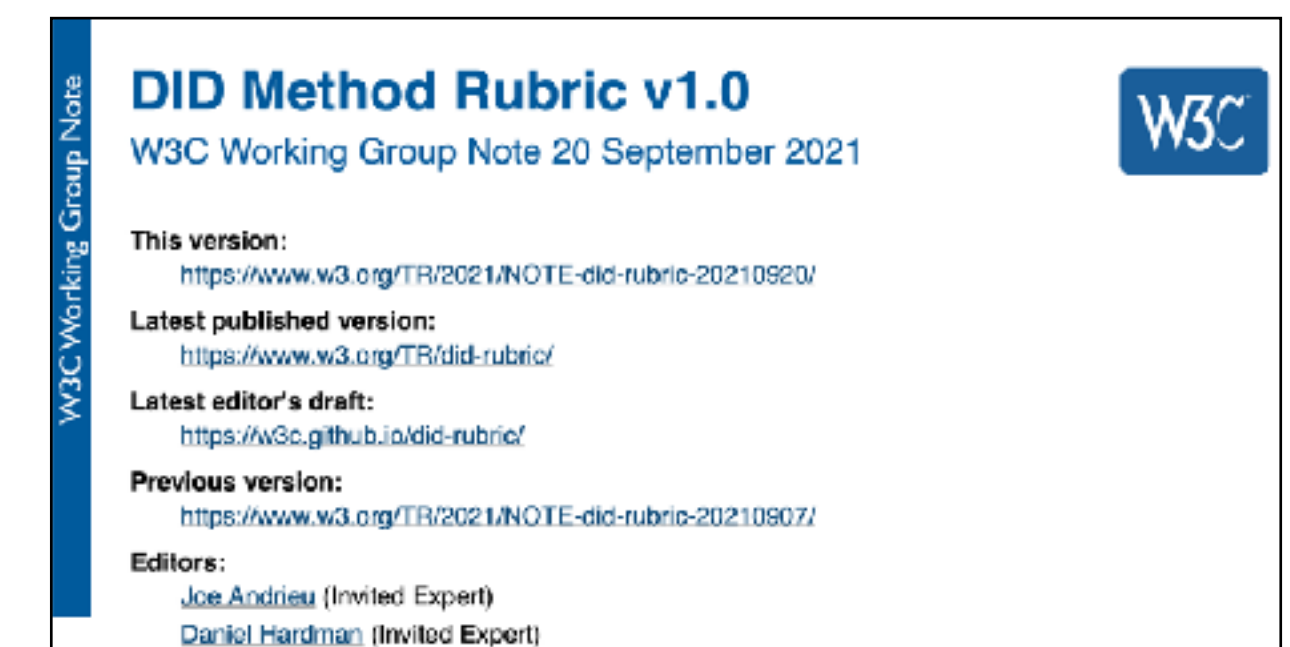
[1] <https://www.w3.org/2021/09/21-did10-minutes.html>

Example: DID and related services



DID Method Rubric v1.0 (W3C Working Group Note)

- DIDは、自己主権型の識別子にまつわるデータモデル標準であり、周辺技術との組み合わせで自己主権型のアイデンティティを実現できる。DIDの具体的な実装仕様は DID Method 毎に規定される
- たとえば、どのように「Decentralize(d)」されるのかは、Methodのデザイン毎に異なる。さらに、"decentralization" という概念の共通した定義さえ困難であることが明らかになった
- そのため、DID Methodの様々な特性の比較をするための文書として、本文書が整備されつつある



DID Rubric の Criteria 例 (1)

3.1.1 Open contribution (participation) §

<https://www.w3.org/TR/did-rubric#criteria-1> v1.0.0

3.1.1.1 Question §

How open is participation in governance decisions?

3.1.1.2 Responses §

- A. Anyone can participate in an open, fair process where all participants have equal opportunity to be heard and influence decisions.
- B. Anyone can comment and contribute to open debate, but decisions are ultimately made by a closed group.
- C. Debate is restricted to a selected but known group.
- D. Debate is conducted in secret by an unknown group.

3.1.1.3 Relevance §

Governance determines how the rules of the underlying network are set and maintained. The more parties that are able to contribute to governance debates, the more decentralized the governance.

3.1.1.4 Examples §

| Method | Spec. | Net. | Reg. | Notes |
|----------|-------|------|------|---|
| did:peer | B | C | C | did:peer has no intrinsic network. It can use any communications channel between parties. Only those two parties are privy to the decisions made about communications and recordation. The spec is openly developed on github by a listed set of contributors and issues may be raised by anyone. |
| did:git | B | C | D | The git network is the git source code, which is controlled (currently) by 16 people. They do not have a public issues process. The spec is openly developed on github by a listed set of contributors and issues may be raised by anyone. Each registry is controlled by potentially unknown parties as negotiated in "meatspace". |
| did:btcr | B | D | D | Changes to the bitcoin protocol are chaotic and uncertain. They use BIPs, but the path to adoption is uncertain and the relative power of developers, miners, and users is open to debate. The spec is openly developed on github by a listed set of contributors and issues may be raised by anyone. |

DID Rubric の Criteria 例 (2)

§ 3.4.1 Auditability

<https://www.w3.org/TR/did-rubric#criteria-12>

§ 3.4.1.1 Question

Who can retrieve cryptographic proof of the history of changes to a given DID Document?

§ 3.4.1.2 Responses

- A. Anyone
- B. Only a select group, including parties not involved in a given DID transaction
- C. Only parties to the transaction
- D. Not available

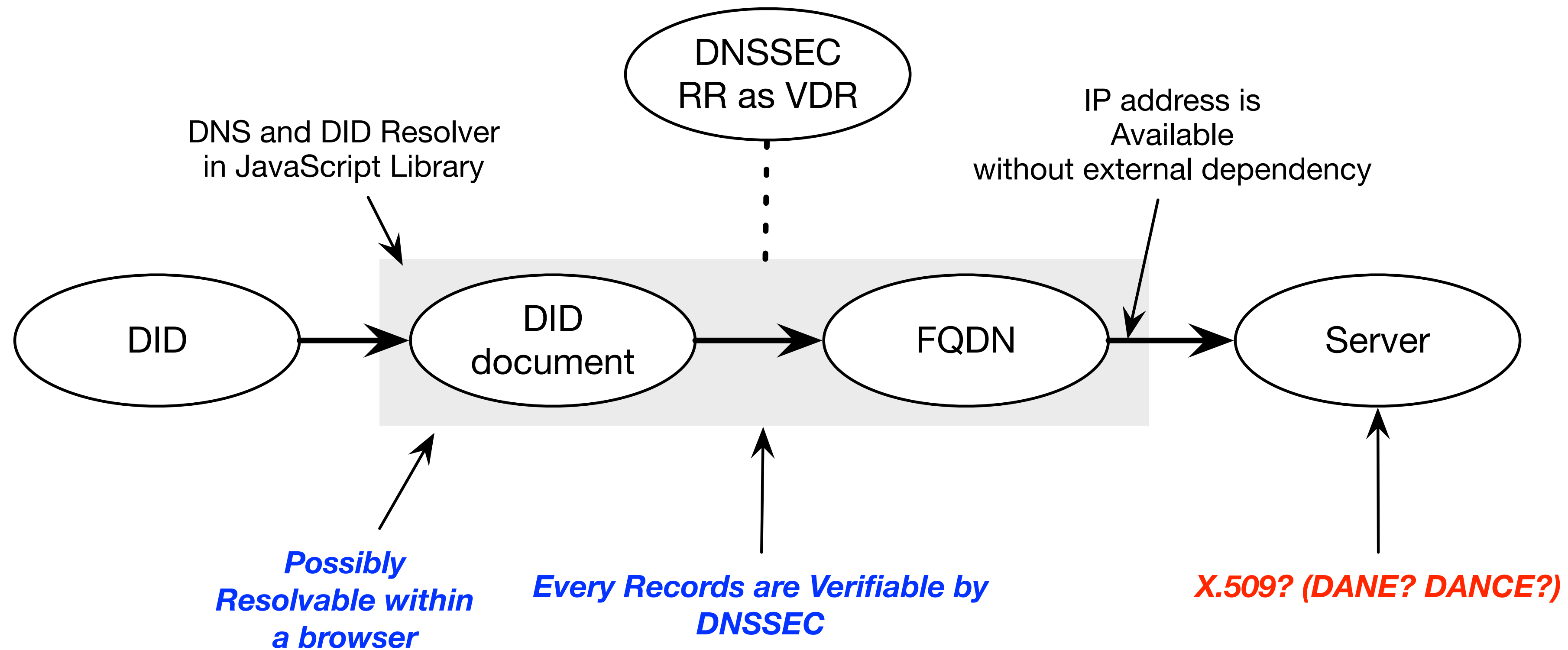
§ 3.4.1.3 Relevance

Trustlessness is a prerequisite of a decentralized system. If you have to trust the source of a DID Document (i.e., if you can't verify cryptographically a DID Document that is returned from resolution), then you are at the mercy of a potentially centralized authority. If, instead you have a cryptographic audit trail, then the current state of a DID cannot be compromised by an intermediary or central party.

3.4.1.4 Examples §

| Method | Reg. | Notes |
|----------|------|--|
| did:peer | C- | DID:peer maintains a cryptographic journal, but it is only available to the peers and, technically, can be refused (each peer may suspend interactions at any time). |
| did:git | B- | If you have access to the authoritative git repo, you can see the cryptographic journal. However, within the method specification, there is no way to know if the repo you are inspecting is, in fact, definitive. |
| did:btcr | A | Anyone can see everything. |
| did:sov | A | Anyone can see everything—the Sovrin ledger is completely public. |
| did:ethr | A | Anyone can see updates and deletes. Creation is private. |
| did:jolo | A | Anyone can see updates and deletes. Creation is private. |

On-going work: did:dnsssec [1]



[1] Proposal on the Design and Implementation of a DID method over DNSSEC (`did:dnsssec`)

<https://shigeya.github.io/did-dnssec-proposal/main/draft-suzuki-did-dnssec-proposal.html>

[2] RFC7671: The DNS-Based Authentication of Named Entities (DANE) Protocol - Updates and Operational Guidance

<https://datatracker.ietf.org/doc/html/rfc7671>

[3] WG Charter: DANE Authentication for Network Clients Everywhere (DANCE)

<https://datatracker.ietf.org/doc/charter-ietf-dance/>

| DID/VC の応用



ニューノーマル時代における人間の社会活動を支える情報基盤の在り方とデジタルアイデンティティの位置づけ

Version 0.1 (2020/8/3)

慶應義塾大学SFC研究所 ブロックチェーン・ラボ

村井 純

慶應義塾大学 教授

鈴木 茂哉

慶應義塾大学大学院政策・メディア研究科 特任教授

松尾 真一郎

慶應義塾大学大学院政策・メディア研究科 特任教授(非常勤)

ジョージタウン大学研究教授

クロサカタツヤ

慶應義塾大学大学院政策・メディア研究科 特任准教授(非常勤)

ニューノーマルと新たなインターネット文明の調和

新型コロナウイルス感染症（COVID-19）の感染拡大は、人間社会に新しい生活様式を要求しはじめている。我が国をはじめ、世界中の多くで、人間との接触（フィジカル・コンタクト）への制限が求められる中、デジタル・テクノロジーの活用は、従来のような付加価値向上という水準を超えて、すでに生命や健康の安全にとって重要な手段として位置づけられはじめている。こうした現状を、マイクロソフトのサテニア・ナデラCEOは、同社の決算発表において「この2ヶ月間で2年分に匹敵するほどのデジ



Trusted Web 推進協議会

- 内閣官房デジタル市場競争本部内でデジタル市場競争会議が令和2年6月に取りまとめた「中期展望レポート」に基づき設立された協議会
- 趣旨[1]:
 - 「デジタル市場競争に係る中期展望レポート」（令和2年6月16日デジタル市場競争会議）に基づき、将来の競争構造の変化を睨み、データ・ガバナンスのあり方をテクノロジーで変える分散型の“Trusted Web”の構築を進める。推進にあたっては、官民の連携体制の下で、データ・ガバナンスの構造設計、その際に必要となる要素やそれを実現する技術の抽出・課題検証、移行のためのロードマップの策定、具体的なユースケースに即した検証、必要な政策面での対応、国際的な発信等の具体化を進めていく必要がある。
 - このため、これらを実行する官民の連携体制として、専門家・関係者から成る「Trusted Web 推進協議会」（以下「協議会」という。）を設立し、上記の事項について検討を行う。
 - 協議会での検討の成果は、デジタル市場競争会議等に適宜報告し、必要に応じてルール整備、技術開発支援や国際的な発信等に反映させる。

首相官邸 Prime Minister of Japan and His Cabinet

政策会議

トップ > 会議等一覧 > デジタル市場競争本部

デジタル市場競争本部
Headquarters for Digital Market Competition

グローバルで変化が激しいデジタル市場における競争やイノベーションを促進するため、競争政策の迅速かつ効果的な実施を目的としてデジタル市場競争本部を設置しています。

設置根拠

- 設置根拠
- 名簿 (PDF/54KB)
- 開催状況
- English

会議情報

- デジタル市場競争会議
- デジタル市場競争会議ワーキンググループ
- Trusted Web推進協議会

※デジタル市場競争会議が令和2年6月に取りまとめた「中期展望レポート」に基づき設立された協議会

首相官邸 Prime Minister of Japan and His Cabinet

政策会議

トップ > 会議等一覧 > デジタル市場競争本部 > Trusted Web推進協議会

Trusted Web推進協議会

| 回数 | 開催日 | 議題・会議関係資料 |
|-----|--------------------|--|
| — | (公表中) 令和3年4月5日 | 1. Trusted Web White Paper ver1.0 Executive Summary 会議資料等については、下記の外部リンクにて公開しています(※)。 https://github.com/TrustedWebPromotionCouncil/Documents |
| — | (公表中) 令和3年3月31日 | 資料 1. Trusted Web ホワイトペーパー ver1.0 エグゼクティブサマリー (PDF/210KB) 2. Trusted Web ホワイトペーパー ver1.0 (PDF/941KB) 3. Trusted Web ホワイトペーパー ver1.0 修正案 (PDF/799KB) 会議資料等については、下記の外部リンクにて公開しています(※)。 最新版はこちらでご確認をお願いいたします。 https://github.com/TrustedWebPromotionCouncil/Documents |
| 第3回 | 令和3年3月12日 | 1. 意見交換 ○ Trusted Web ホワイトペーパー（案）について 2. その他 会議資料等については、下記の外部リンクにて公開しています(※)。 https://github.com/TrustedWebPromotionCouncil/Documents |

まとめ

- ・ 検証可能なデジタル証明書とデジタルアイデンティティ
 - ・ Verifiable Credential
 - ・ ワクチン接種証明への応用
 - ・ 自己主権型デジタルアイデンティティとして適用可能な分散型アイデンティティ
 - ・ Decentralized Identifiers (DID)
 - ・ 課題と標準化動向
 - ・ 応用に向けた国内の取り組み
-
- ・ ブロックチェーンのアプリケーション(通貨的な応用**以外**)にはデジタルアイデンティティが必要
 - ・ 自己主権型デジタルアイデンティティにはブロックチェーンを使える
 - 課題: エネルギー消費の問題の解決が必要